EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PANORAMA DELLE MINACCE SOTTO FORMA DI ATTACCHI ALLA CATENA DI APPROVIGIONAMENTO TRACCIATO DALL'ENISA

LUGLIO 2021

INFORMAZIONI SULL'ENISA

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento dell'UE sulla cibersicurezza, l'ENISA contribuisce alla politica dell'UE in materia di sicurezza nel settore informatico, migliora l'affidabilità dei prodotti, dei servizi e dei processi TIC con programmi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sul suo lavoro sono disponibili al seguente indirizzo: www.enisa.europa.eu.

CONTATTI

Per contattare gli autori, inviare un messaggio di posta elettronica a etl@enisa.europa.eu.
Per maggiori informazioni sul presente documento, si prega di scrivere a press@enisa.europa.eu.

REDATTORI

Ifigeneia Lella, Marianthi Theocaridou, Eleni Tsekmezoglou, Apostolos Malatras — Agenzia dell'Unione europea per la cibersicurezza
Sebastian Garcia, Veronica Valeros — Università tecnica ceca di Praga

RINGRAZIAMENTI

Desideriamo ringraziare i membri e gli osservatori del gruppo di lavoro ad hoc dell'ENISA sui paesaggi della minaccia informatica per il loro prezioso riscontro e le loro osservazioni nella convalida della presente relazione. Desideriamo inoltre ringraziare Volker Distelrath (Siemens) e Konstantinos Moulinos (ENISA) per il loro feedback.

NOTE LEGALI

Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) 2019/881. L'ENISA può aggiornare periodicamente tale pubblicazione.

Secondo necessità, sono citate anche fonti di terze parti. L'ENISA non è responsabile del contenuto delle fonti esterne, quali i siti web esterni riportati nella presente pubblicazione.

La presente pubblicazione è unicamente a scopo informativo. Deve essere accessibile gratuitamente. L'ENISA, o chiunque agisca in suo nome, declina ogni responsabilità per l'uso che può essere fatto delle informazioni di cui alla presente pubblicazione.

AVVISO SUL COPYRIGHT

ISBN: 978-92-9204-509-8 – DOI: 10.2824/168593

INDICE

SINTESI

Gli attacchi alla catena di approvvigionamento sono fonte di preoccupazione per la sicurezza da molti anni. Tuttavia, dagli inizi del 2020, la comunità si trova a doversi confrontare con un maggior numero di attacchi meglio organizzati. È possibile che, in conseguenza della più solida protezione della sicurezza attuata dalle organizzazioni, gli autori degli attacchi abbiano deciso di rivolgersi ai fornitori. Sono peraltro riusciti a produrre impatti significativi in termini di tempi di inattività dei sistemi, perdite finanziarie e danni alla reputazione. L'importanza delle catene di approvvigionamento è attribuita al fatto che attacchi riusciti possono avere ripercussioni su un gran numero di clienti che si avvalgono del fornitore colpito. Pertanto, gli effetti a cascata di un singolo attacco possono avere un impatto ampiamente diffuso.

La presente relazione mira a mappare e studiare gli attacchi alla catena di approvvigionamento rilevati dal gennaio 2020 all'inizio di luglio 2021. Sulla base delle tendenze e dei modelli osservati, gli attacchi alla catena di approvvigionamento sono aumentati in numero e in sofisticazione nel 2020 e tale tendenza continua nel 2021, con un rischio crescente per le organizzazioni. Si stima che nel 2021 gli attacchi alla catena di approvvigionamento saranno quattro volte superiori rispetto al 2020. Poiché la metà degli attacchi è stata attribuita ad attori di minacce persistenti avanzate (APT), la loro complessità e le loro risorse superano di gran lunga gli attacchi non mirati più comuni e, pertanto, vi è una crescente necessità di nuovi metodi di protezione in grado di includere i fornitori e garantire la sicurezza delle organizzazioni.

La presente relazione presenta il panorama della minaccia rappresentata dagli attacchi della catena di approvvigionamento dell'Agenzia, elaborato con il sostegno del gruppo di lavoro ad hoc sui paesaggi della minaccia informatica[1].

Tra i punti principali della relazione figurano i seguenti:

- Una **tassonomia** per classificare gli attacchi della catena di approvvigionamento al fine di analizzarli meglio in modo sistematico e comprendere il modo in cui si manifestano.
- Dal gennaio 2020 all'inizio di luglio 2021 sono stati segnalati **24 attacchi alla catena di approvvigionamento**, che sono stati esaminati nella presente relazione.
- Circa il **50 % degli attacchi è stato attribuito dalla comunità della sicurezza a noti gruppi APT**.
- Circa il **42 % degli attacchi analizzati non è** ancora stato **attribuito a un particolare gruppo**.
- Circa il **62 % degli attacchi contro i clienti** ha approfittato della **fiducia nel proprio fornitore**.
- Nel **62 % dei casi**, i **malware erano la tecnica di attacco** utilizzata.
- Per quanto riguarda di attacchi che prendono di mira beni specifici, nel **66% degli incidenti** gli autori degli attacchi **si sono concentrati sul codice dei fornitori** per compromettere ulteriormente i clienti interessati.
- Circa il **58 % degli attacchi della catena di approvvigionamento mirava** ad ottenere l'accesso ai **dati** (prevalentemente i dati dei clienti, compresi i dati personali e la proprietà intellettuale) e circa il **16 %** a ottenere l'accesso alle **persone**.
- **Non tutti gli attacchi dovrebbero essere considerati attacchi alla catena di approvvigionamento**, ma molti di essi sono, per loro natura, vettori potenziali di nuovi attacchi nella catena di approvvigionamento in futuro.
- Le **organizzazioni devono aggiornare la loro metodologia di cibersicurezza tenendo conto degli attacchi alla catena di approvvigionamento** e integrare tutti i loro fornitori nella loro protezione e verifica della sicurezza.

[1] Cfr. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

1. INTRODUZIONE

Gli attacchi alla catena di approvvigionamento sono fonte di preoccupazione per la sicurezza da molti anni. Tuttavia, dagli inizi del 2020, la comunità si trova a doversi confrontare con un maggior numero di attacchi più organizzati. È possibile che, a causa della più solida protezione della sicurezza attuata dalle organizzazioni, gli autori degli attacchi si siano spostati verso i fornitori e siano riusciti a causare un impatto significativo in termini di tempi di inattività dei sistemi, perdite finanziarie e danni alla reputazione, per citarne solo alcuni. La presente relazione mira a mappare e studiare gli attacchi alla catena di approvvigionamento rilevati dal gennaio 2020 all'inizio di luglio 2021.

L'effetto devastante e collaterale degli attacchi della catena di approvvigionamento è stato osservato pienamente con l'attacco di SolarWinds[2]. Quello di Solarwinds è considerato uno dei più grandi attacchi alla catena di approvvigionamento degli ultimi anni, in particolare per quanto riguarda le entità colpite, tra cui organizzazioni governative e grandi imprese. Ha ricevuto grande attenzione da parte dei media e ha portato a iniziative politiche in tutto il mondo[3]. Più di recente, nel luglio 2021, si è verificato l'attacco a Kaseya[4] che ha sollevato la necessità di un'ulteriore e specifica attenzione agli attacchi alla catena di approvvigionamento che colpiscono i fornitori di servizi gestiti. Purtroppo, questi due esempi non sono casi isolati e il numero di attacchi alla catena di approvvigionamento è aumentato costantemente nel corso dell'ultimo anno. Questa tendenza sottolinea inoltre la necessità che i responsabili politici e la comunità della sicurezza elaborino e introducano nuove misure protettive per affrontare i potenziali attacchi alla catena di approvvigionamento in futuro e per attenuarne l'impatto.

Attraverso un'attenta indagine e analisi, la presente relazione traccia una mappatura degli attacchi alla catena di approvvigionamento sulla base di incidenti individuati dal gennaio 2020 all'inizio di luglio 2021. Ogni incidente è stato suddiviso nei suoi elementi chiave, quali le tecniche di attacco e i beni sia dei fornitori che dei clienti interessati dagli avversari. L'introduzione di una tassonomia per gli attacchi alla catena di approvvigionamento ne faciliterà la classificazione e potrebbe costituire il punto di partenza per un approccio più strutturato nell'analisi di tali attacchi e nell'introduzione di controlli di sicurezza specifici per attenuarli. La tassonomia proposta contribuisce inoltre a classificare, confrontare e discutere questi attacchi utilizzando un terreno comune. Vengono discusse le analogie tra la tassonomia proposta e altri quadri ben noti.

La presente relazione analizza inoltre le analogie tra il ciclo di vita degli attacchi alla catena di approvvigionamento e gli attacchi più noti da parte di minacce persistenti avanzate (APT). Nell'allegato figura una sintesi degli incidenti più rilevanti verificatisi nella catena di approvvigionamento dal 2020, ciascuno dei quali è stato decomposto conformemente alla tassonomia di cui sopra.

Il fulcro della relazione è un'analisi di tutti gli incidenti segnalati nella catena di approvvigionamento per identificarne le caratteristiche e le tecniche principali. L'analisi risponde a domande su quali sono le tecniche di attacco più comuni utilizzate negli attacchi alla catena di approvvigionamento, quali sono i beni principali dei clienti presi di mira e quali sono i rapporti tra attacchi e beni presi in considerazione.

Con l'aumento dell'attenzione prestata agli attacchi alla catena di approvvigionamento, molti altri incidenti correlati alla sicurezza sono stati anch'essi segnalati come connessi alla catena di approvvigionamento, e considerati anch'essi attacchi alla catena di approvvigionamento. Viene quindi spiegato quale attacco costituisca un attacco alla catena di approvvigionamento e perché molti attacchi non siano realmente attacchi alla catena di approvvigionamento, mostrando alcuni casi come esempi. Comprendere il panorama delle minacce relative agli attacchi della catena di

[2] Russian SolarWinds hackers launch email attack on government agencies, The Guardian. https://www.theguardian.com/technology/2021/may/28/russian-solarwinds-hackers-launch-assault-government-agencies. Accessed on 08/07/2021.
[3] Cfr. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html
[4] Ransomware Attack Affecting Likely Thousands of Targets Drags On, WSJ, https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071. Consultato il 03/12/2021.

approvvigionamento è importante in quanto un'errata classificazione degli incidenti può portare a un'analisi e a conclusioni erronee delle tendenze.

La relazione contiene inoltre una serie di raccomandazioni rivolte ai responsabili politici e alle organizzazioni, in particolare ai fornitori, e la sua adozione può aumentare la sicurezza globale in caso di attacchi alla catena di approvvigionamento.

La presente relazione è strutturata come segue:

- Il **capitolo 1** fornisce una breve introduzione al tema della catena di approvvigionamento e al panorama dedicato alle minacce dell'ENISA.
- Il **capitolo 2** tratta di ciò che costituisce un attacco alla catena di approvvigionamento e introduce una tassonomia strutturata per classificare gli incidenti rilevanti che riguardano anche quadri consolidati di intelligence sulle minacce informatiche.
- Il **capitolo 3** fornisce una panoramica del ciclo di vita di un tipico attacco alla catena di approvvigionamento.
- Il **capitolo 4** descrive i principali attacchi alla catena di approvvigionamento verificatisi tra la fine del 2020 e l'inizio del 2021.
- Il **capitolo 5** fornisce un calendario degli incidenti pertinenti e un'analisi approfondita degli incidenti.
- Il **capitolo 6** affronta la questione dell'errata classificazione degli incidenti come attacchi alla catena di approvvigionamento.
- Il **capitolo 7** introduce raccomandazioni tecniche e di alto livello per migliorare la sicurezza della catena di approvvigionamento e attenuare l'impatto degli attacchi della catena di approvvigionamento.
- L'**allegato A** riassume 24 incidenti della catena di approvvigionamento individuati e analizzati nella presente relazione.

2. CHE COS'È UN ATTACCO ALLA CATENA DI APPROVVIGIONAMENTO?

Il termine *catena di approvvigionamento* si riferisce all'ecosistema di processi, persone, organizzazioni e distributori coinvolti nella creazione e nella fornitura di una soluzione o di un prodotto finale[5]. Nella cibersicurezza, la catena di approvvigionamento comprende un'ampia gamma di risorse (hardware e software), archiviazione (cloud o locale), meccanismi di distribuzione (applicazioni web, negozi online) e software di gestione.

In una catena di approvvigionamento, sono presenti quattro elementi chiave:

- *Fornitore*: un'entità che fornisce un prodotto o un servizio a un'altra entità.
- *Beni del fornitore*: elementi preziosi utilizzati dal fornitore per produrre il prodotto o il servizio.
- *Cliente*: l'entità che consuma il prodotto o il servizio prodotto dal fornitore.
- *Beni del cliente*: elementi preziosi di proprietà dell'obiettivo.

Un'entità può essere un individuo, un gruppo di individui o un'organizzazione. I beni possono essere: persone, software, documenti, finanze, hardware o altro.

Un attacco alla catena logistica è una combinazione di almeno due attacchi. Il primo attacco riguarda un fornitore che viene poi utilizzato per attaccare l'obiettivo per avere accesso ai suoi beni. L'obiettivo può essere il cliente finale o un altro fornitore. Pertanto, affinché un attacco possa essere classificato come una catena di approvvigionamento, sia il fornitore che il cliente devono essere obiettivi.

2.1. TASSONOMIA DEGLI ATTACCHI ALLA CATENA DI APPROVVIGIONAMENTO

La presente relazione propone una tassonomia per caratterizzare gli attacchi alla catena di approvvigionamento e strutturarne la successiva analisi. Questa tassonomia tiene conto di tutti e quattro gli elementi chiave di una catena di approvvigionamento, nonché delle tecniche utilizzate dagli autori degli attacchi. La tassonomia può aiutare le organizzazioni a comprendere le varie parti di un attacco alla catena di approvvigionamento, confrontandole con altri attacchi informatici simili e soprattutto identificando gli incidenti come attacchi alla catena di approvvigionamento.

La tassonomia dovrebbe essere utilizzata come modello guida in cui, a seguito di un nuovo potenziale attacco alla catena di approvvigionamento, la comunità potrebbe cercare di analizzarla individuando e classificando ciascuno dei quattro distinti elementi della tassonomia. Se nessun cliente viene attaccato o nessun fornitore è attaccato, è possibile che non si tratti di un attacco alla catena di approvvigionamento[6].

La tassonomia, come presentata nella tabella 1, comprende una sezione per il fornitore e una per il cliente. Per il fornitore, la prima parte è chiamata "tecnica di attacco utilizzata per compromettere la catena di approvvigionamento" e identifica **come** il fornitore è stato attaccato. La seconda parte per il fornitore è chiamata "beni del fornitore presi di mira dall'attacco alla catena di approvvigionamento" e identifica **quale** è l'obiettivo dell'attacco al fornitore.

Per il cliente, la prima parte è chiamata "tecniche di attacco utilizzate per compromettere il cliente" e identifica **come** il cliente è stato attaccato. La seconda parte per il cliente è chiamata "beni del cliente presi di mira dall'attacco alla catena di approvvigionamento" e identifica **quale** è l'obiettivo dell'attacco al cliente.

[5] Beamon, B. M. (1998). Supply chain design and analysis: Models and methods. International journal of production economics, 55(3), 281-294.
[6] Per ulteriori esempi, è possibile consultare la sezione "Non tutti gli attacchi sono attacchi alla catena di approvvigionamento".

Per ciascuno di questi quattro elementi distintivi nella tassonomia sono stati definiti gli elementi che meglio caratterizzano un attacco alla catena di approvvigionamento. Selezionando gli elementi corrispondenti è possibile avere una migliore comprensione di ciò che è noto o non noto in merito a un attacco. La tassonomia è concettualmente diversa dalla knowledge base di MITRE ATT&CK® e non intende sostituirla, bensì completarla. Le tecniche di attacco definite nella tassonomia proposta e illustrate nella tabella 1 sono in alcuni casi connesse alle tecniche di attacco pertinenti individuate nel quadro MITRE ATT&CK® e sono pertanto contrassegnate con il rispettivo identificativo MITRE ATT&CK® tra parentesi quadre, ad esempio [T1189]. Le sottosezioni che seguono chiariscono ciascuna delle quattro parti della tassonomia e come identificarne gli elementi.

Tabella 1. Tassonomia proposta per gli attacchi alla catena di approvvigionamento. Si articola in quattro parti: (i) tecniche di attacco utilizzate verso il fornitore, (ii) beni del fornitore attaccati, (iii) tecniche di attacco utilizzate verso il cliente, (iv) beni del cliente attaccati.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Infezione da malware	Software preesistente	Rapporto di fiducia [T1199]	Dati
Ingegneria sociale	Librerie software	Compromissione "drive-by" [T1189]	Dati personali
Attacco "brute force"	Codice	Phishing [T1566]	Proprietà intellettuale
Sfruttamento della vulnerabilità del software	Formazioni	Infezione da malware	Software
Sfruttamento della vulnerabilità della configurazione	Dati	Attacco fisico o modifica	Processi
Intelligence open source (OSINT)	Processi	Contraffazione	Larghezza di banda
	Hardware		Ambito finanziario
	Persone		Persone
	Fornitore		

Per le attività di coordinamento delle risposte agli incidenti, e per la condivisione delle informazioni al livello dell'Unione, viene utilizzata una tassonomia degli incidenti di sicurezza informatica dell'UE[7]. Poiché la tassonomia è concettualmente diversa e non consente un'analisi dettagliata degli incidenti alla catena di approvvigionamento, viene consigliato l'uso complementare di entrambe le tassonomie.

2.2. TECNICHE DI ATTACCO UTILIZZATE PER COMPROMETTERE UNA CATENA DI APPROVVIGIONAMENTO

Le tecniche di attacco si riferiscono a "come" è avvenuto l'attacco, e non a "cosa" è stato usato per attaccare. Ad esempio, questa categoria distingue se il fornitore è stato attaccato con una password trovata online (OSINT) o se la password è stata ottenuta attraverso un attacco di tipo "brute-Force". Tuttavia, non è rilevante per la tassonomia se la password trovata online sia stata trapelata, fosse una password predefinita oppure se sia stata venduta in un mercato nero. Le categorie delle tecniche di attacco riportate di seguito coprono le tecniche di attacco più comunemente

[7] Cybersecurity incident taxonomy, Publications of the NIS Cooperation Group, July 2018. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. consultato il 03/12/2021.

utilizzate negli attacchi alla catena di approvvigionamento analizzati nella presente relazione. È evidente che, in un determinato attacco, possono essere utilizzate più tecniche e, in molti casi, le entità potrebbero non essere in grado di scoprire come gli autori degli attacchi abbiano ottenuto l'accesso alla loro infrastruttura, oppure queste informazioni non sono state divulgate o debitamente segnalate.

Tabella 2. Tecniche di attacco utilizzate per compromettere il fornitore nella catena. Ogni tecnica identifica il modo in cui l'attacco si è verificato e non ciò che è stato attaccato. Nello stesso attacco possono essere utilizzate diverse tecniche.

TECNICHE DI ATTACCO UTILIZZATE PER COMPROMETTERE UNA CATENA DI APPROVVIGIONAMENTO	
Infezione da malware	ad esempio, lo spyware utilizzato per rubare le credenziali ai dipendenti.
Ingegneria sociale	Ad esempio, phishing, applicazioni false, typo-squatting, impersonificazione Wi-Fi, raggiri che portano il fornitore a compiere un'azione.
Attacco "brute-force"	Ad esempio, indovinare una password SSH, indovinare un login Web.
Sfruttamento della vulnerabilità del software,	Ad esempio, SQL injection od overflow del buffer in un'applicazione.
Sfruttamento della vulnerabilità della configurazione	Ad esempio, sfruttare un problema di configurazione.
Attacco fisico o modifica	Ad esempio, modificare l'hardware, l'intrusione fisica.
Intelligence open source (OSINT)	Ad esempio, cercare in linea credenziali, chiavi API, nomi utente.
Contraffazione	Ad esempio, imitazione di USB con scopi dannosi.

2.3. BENI DEI FORNITORI INTERESSATI DA UN ATTACCO ALLA CATENA DI APPROVVIGIONAMENTO

I beni dei fornitori presi di mira dagli autori degli attacchi fanno riferimento a "quale" era l'obiettivo dell'attacco al fornitore, che ha consentito di sferrare ulteriori attacchi. Normalmente, i beni presi di mira sono caratterizzati da una relazione diretta con l'obiettivo finale; è, quindi, solitamente possibile comprendere le intenzioni finali dell'autore dell'attacco analizzando l'elenco dei beni interessati. In alcuni casi, a causa della mancanza di informazioni divulgate o segnalate dal fornitore, le informazioni sui beni presi di mira dagli attacchi non sono disponibili. Ciò potrebbe verificarsi anche quando i fornitori non dispongono delle conoscenze o delle competenze necessarie per identificare quali beni sono stati compromessi dagli autori degli attacchi.

Tabella 3. Beni del fornitore presi di mira dagli autori degli attacchi. Ogni elemento identifica "cosa" è stato attaccato nel fornitore. Nello stesso attacco possono essere utilizzate diverse tecniche che potrebbero influire su più beni.

BENI DEL FORNITORE INTERESSATI DA UN ATTACCO ALLA CATENA DI APPROVVIGIONAMENTO	
Software preesistente	Ad esempio, software utilizzato dal fornitore, server Web, applicazioni, database, sistemi di monitoraggio, applicazioni cloud, firmware. Non include le librerie software.
Librerie software	Ad esempio, librerie di terze parti, pacchetti software installati da terze parti come npm, ruby, ecc.
Codice	Ad esempio, il codice sorgente o il software prodotto dal fornitore.
Formazioni	Ad esempio, password, chiavi API, regole firewall, URL.
Dati	Ad esempio, informazioni sul fornitore, valori dei sensori, certificati, dati personali dei clienti o dei fornitori stessi, dati personali.
Processi	Ad esempio aggiornamenti, backup o processi di convalida, firma dei processi di certificazione.
Articoli di ferro	Ad esempio hardware prodotto dal fornitore, chip, valvole, UDB.
Persone	Ad esempio persone mirate che hanno accesso a dati, infrastrutture o altre persone.

2.4. TECNICHE DI ATTACCO UTILIZZATE PER RAGGIUNGERE UN COMPROMESSO

Questo elemento della tassonomia si riferisce alle tecniche di attacco utilizzate per compromettere il cliente attraverso il suo fornitore. Nell'ambito di questo elemento della tassonomia, identifichiamo "come" il cliente è stato attaccato e non con "cosa". Si tratta di una tecnica e non di un tipo specifico di attacco. Ad esempio, se il cliente aggiorna il proprio software dal fornitore e riceve un tipo di malware, l'attacco riguarda sia una "relazione di fiducia" sia una "infezione da malware". È evidente, in molti casi, possono essere applicate più tecniche. I clienti potrebbero non conoscere la tecnica utilizzata dagli autori degli attacchi per accedere alle loro risorse tramite i fornitori, ma possono disporre dei mezzi per identificare che la tecnica utilizzata non rientrava nel loro perimetro.

Tabella 4. Tecniche di attacco utilizzate per compromettere il cliente. Ogni tecnica identifica il modo in cui l'attacco si è verificato e non ciò che è stato attaccato. Nello stesso attacco possono essere utilizzate diverse tecniche.

TECNICHE DI ATTACCO UTILIZZATE PER COMPROMETTERE UN CLIENTE	
Relazione di fiducia [T1199]	Ad esempio, attendibilità di un certificato, attendibilità di un aggiornamento automatico, attendibilità di un backup automatico.
Compromissione "drive-by" [T1189]	Ad esempio, script dannosi in un sito Web per infettare gli utenti con malware.

TECNICHE DI ATTACCO UTILIZZATE PER COMPROMETTERE UN CLIENTE	
Phishing [T1566]	Ad esempio, messaggi che rappresentano il fornitore, false notifiche di aggiornamento.
Infezione da malware	Ad esempio, RAT (Remote Access Trojan), backdoor, ransomware.
Attacco fisico o modifica	Ad esempio, modificare l'hardware, l'intrusione fisica.
Contraffazione	Ad esempio, creare un falso USB, modificare una scheda madre, impersonare il personale del fornitore.

2.5. BENI DI CLIENTI OGGETTO DELL'ATTACCO DELLA CATENA DI APPROVVIGIONAMENTO

I beni dei clienti sono l'obiettivo principale e finale degli autori degli attacchi e di solito la *raison d'être* alla base di un attacco alla catena di approvvigionamento. Tali attività possono variare a seconda del settore industriale e del tipo di servizio offerto. L'elemento particolare della tassonomia è inteso a facilitare la comprensione dell'impatto dell'attacco e a consentire confronti sugli obiettivi degli autori dell'attacco. Alcuni beni potrebbero essere stati direttamente presi di mira dagli autori degli attacchi, mentre altri potrebbero essere stati inavvertitamente colpiti. In genere, gli attacchi tipici alle catene di approvvigionamento colpiscono più di un cliente. È possibile che il cliente non sia a conoscenza dell'obiettivo dell'avversario (ad esempio, l'attacco non è riuscito o è stato rilevato rapidamente).

Tabella 5. Beni del cliente presi di mira dagli autori degli attacchi. Ogni elemento identifica cosa è stato attaccato nel cliente. Nello stesso attacco possono essere utilizzate diverse tecniche. Solitamente questo è l'obiettivo finale dell'attacco.

BENI DEL CLIENTE INTERESSATI DA UN ATTACCO ALLA CATENA DI APPROVVIGIONAMENTO	
Dati	Ad esempio, dati di pagamento, feed video, documenti, e-mail, piani di volo, dati di vendita e dati finanziari, proprietà intellettuale.
Dati personali	Ad esempio, dati dei clienti, record dei dipendenti, credenziali.
Software	Ad esempio, accesso al codice sorgente del prodotto del cliente, modifica del software del cliente.
Processi	Ad esempio, documentazione di processi interni di funzionamento e configurazione, inserimento di nuovi processi dannosi, documenti di schemi.
Larghezza di banda	Ad esempio, utilizzo della larghezza di banda per attacchi DDoS (Distributed Denial of Service), invio di SPAM o infezione di utenti su larga scala.
Ambito finanziario	Ad esempio, furto di criptovaluta, dirottamento di conti bancari, trasferimento di denaro.

Persone	Ad esempio, individui presi di mira per la posizione ricoperta o le conoscenze possedute.

2.6. COME UTILIZZARE LA TASSONOMIA

Di seguito è riportato un esempio di come l'applicazione della tassonomia a un caso reale possa contribuire a identificarne le caratteristiche particolari e a facilitare la comprensione delle caratteristiche dell'attacco.

Codecov è un'azienda che fornisce software per la copertura di codice e strumenti di test. L'azienda fornisce strumenti ad altre aziende come IBM e Hewlett Packard Enterprise. Nell'aprile 2021, Codecov ha riferito che utenti malintenzionati hanno ottenuto alcune loro credenziali valide attraverso un'immagine Docker[8] a causa di un errore nella creazione di tali immagini Docker. Dopo avere ottenuto queste credenziali, gli autori degli attacchi le hanno utilizzate per compromettere uno "script bash di upload" utilizzato dai clienti Codecov[9]. Quando i clienti scaricavano ed eseguivano lo script, gli autori degli attacchi riuscivano ad esfiltrare i dati dai clienti di Codecov, incluse informazioni riservate che hanno consentito loro di accedere alle risorse dei clienti[10]. Più clienti Codecov hanno riferito che gli autori degli attacchi erano in grado di accedere al codice sorgente utilizzando informazioni rubate dalla violazione di Codecov[11]. L'attacco non è stato attribuito a avversari specifici. Nella figura 1 (di seguito) sono illustrati i passaggi interessati da questo particolare attacco.

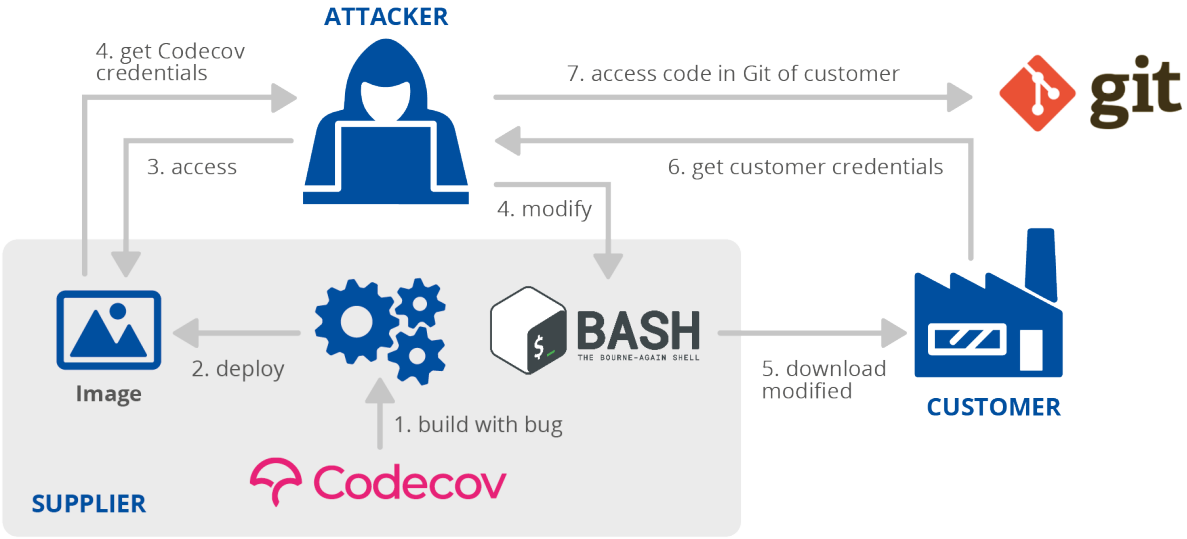
Utilizzando queste informazioni, è possibile identificare i quattro elementi della tassonomia proposta. L'attacco al fornitore indica che gli autori degli attacchi hanno avuto accesso al fornitore e, in questo caso, è stato possibile eseguirlo sfruttando una vulnerabilità di configurazione. Attraverso questo attacco, gli autori degli attacchi prendono di mira il bene del "codice" nel fornitore. Dopo avere identificato gli elementi per il fornitore nella tassonomia, è possibile definire come il cliente è stato attaccato. Nel caso Codecov si tratta di un "rapporto di fiducia" con il fornitore che non è stato protetto e verificato. Il bene finale destinato al cliente è stato segnalato come codice sorgente, quindi "Software".

Tabella 6. La tassonomia di attacco alla catena di approvvigionamento applicata all'attacco a Codecov Company. Gli aggressori hanno sfruttato una vulnerabilità di configurazione a Codecov utilizzata per modificare il codice del fornitore. Gli autori degli attacchi hanno abusato della relazione di fiducia tra Codecov e i suoi clienti per esfiltrare i dati necessari e accedere al codice sorgente del software del cliente.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Sfruttamento della vulnerabilità della configurazione	Codice	Rapporto di fiducia [T1199]	Software

[8] Codecov supply chain attack breakdown, GitGuardian, https://blog.gitguardian.com/codecov-supply-chain-breach/. consultato il 03/12/2021.
[9] Bash Uploader Security Update, Codecov, https://about.codecov.io/security-update/. consultato il 03/12/2021.
[10] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. consultato il 03/12/2021.
[11] Rapid7 Source Code Breached in Codecov Supply-Chain Attack, The Hacker News, https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html. consultato il 03/12/2021.

Figura 1. Schema del funzionamento dell'attacco alla catena di approvvigionamento di Codecov. Il processo di creazione del container Codecov presentava un bug nei container distribuiti online (1). Gli autori dell'attacco hanno effettuato l'accesso al container e ottenuto le credenziali di Codecov (2). Quindi, hanno modificato lo script bash di Codecov (3) che era stato aggiornato nei clienti (4). Lo script bash dannoso ha esfiltrato le credenziali del cliente trasmettendole all'autore dell'attacco (5), che le ha utilizzate per accedere ai dati dei clienti (6).



2.7. TASSONOMIA DELLA CATENA DI APPROVVIGIONAMENTO E ALTRE STRUTTURE

2.7.1. Knowledge Base di MITRE ATT&CK®

MITER ATT&CK® è un'accurata knowledge base e un modello che descrive il funzionamento degli avversari cibernetici. La tassonomia proposta nella relazione differisce da quella di MITER ATT&CK®[12] perché differiscono i rispettivi scopi. Pertanto, non è possibile utilizzare MITER ATT&CK® nella tassonomia della catena di approvvigionamento, in quanto in questa sede si è scelto di porre l'accento sui quattro aspetti che normalmente caratterizzano un attacco alla catena di approvvigionamento, ed in particolare sul rapporto fornitore-cliente. Mentre MITER ATT&CK® mappa completamente le opzioni e le fasi del ciclo di vita di tutti gli attacchi, la sua copertura dei dettagli di una catena di approvvigionamento non è ancora quella sviluppata.

Ad esempio, nella categoria "Initial Access" (Accesso iniziale) di MITER ATT&CK® esiste una tecnica chiamata "Supply Chain Compromise" (Compromissione della catena di approvvigionamento)[13]. Si tratta di elementi molto utili per consentire alle aziende di identificare i rischi in una catena di approvvigionamento, ma risultano troppo generici quando occorre focalizzarsi esplicitamente sugli attacchi alla catena di approvvigionamento stessa. La tassonomia proposta mappa tutti i dettagli dell'attacco alla catena di approvvigionamento stessa e quindi potrebbe potenzialmente integrare la knowledge base MITER ATT&CK®.

2.7.2. Framework Cyber Kill Chain® di Lockheed Martin

La tassonomia proposta ha anche uno scopo diverso dal noto framework Cyber Kill Chain® sviluppato da Lockheed Martin[14]. La cyber kill chain è un framework progettato per identificare le misure adottate dagli aggressori per raggiungere i loro obiettivi. Sebbene possono essere considerati come parte di un attacco alla catena di approvvigionamento, questi passaggi sono troppo generici per consentire di classificare, comprendere e confrontare tali attacchi. La tassonomia qui presentata propone un'analisi più dettagliata di questi attacchi e, cosa più importante, contribuisce a mappare entrambi gli attacchi coinvolti in un unico attacco alla catena di approvvigionamento, uno al fornitore e uno al cliente.

[12] MITRE ATT&CK®, MITRE, https://attack.mitre.org/. consultato il 03/12/2021.
[13] Supply Chain Compromise, Technique T1195 – Enterprise, MITRE ATT&CK®, https://attack.mitre.org/techniques/T1195/. consultato il 03/12/2021.
[14] Cyber Kill Chain®, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. consultato il 03/12/2021.

3. IL CICLO DI VITA DI UN ATTACCO ALLA CATENA DI APPROVVIGIONAMENTO

Si può osservare che un attacco alla catena di approvvigionamento è solitamente costituito da un attacco a uno o più fornitori e, quindi, da un attacco successivo all'obiettivo finale, ossia il cliente. Ciascuno di questi attacchi può risultare molto simile al ciclo di vita degli attacchi APT.

Sebbene sia difficile concordare su una definizione univoca di un attacco APT, in questa relazione un attacco APT viene considerato come un attacco mirato volto a ottenere l'accesso non autorizzato a un'organizzazione (solitamente l'esecuzione di codice), che diffonde per un lungo periodo di tempo e il cui obiettivo finale è in una relazione specifica con l'obiettivo (diversamente, ad esempio, dalla criptominazione). Naturalmente, si tratta di una definizione non completa e ne esistono altre altrettanto valide. Tuttavia, una definizione è importante per comprendere che gli attacchi alla catena di approvvigionamento sono solitamente mirati, complessi, costosi e probabilmente pianificati a lungo termine dai loro autori. Il semplice fatto che almeno due tipi di attacchi riusciti rientrino in tipici incidenti nella catena di approvvigionamento è indicativo del grado di sofisticazione degli avversari oltre che della loro persistenza e intenzione di successo.

Vale la pena notare che molti attacchi APT sono stati considerati non "avanzati" dalla comunità in relazione alla qualità del loro codice, exploit e malware. Tuttavia, si può ritenere che la definizione di "avanzato" faccia riferimento all'intera operazione e non necessariamente al solo codice. Infine, il processo che ingloba la pianificazione, lo staging, lo sviluppo e l'esecuzione di due attacchi in due organizzazioni è un'attività complessa.

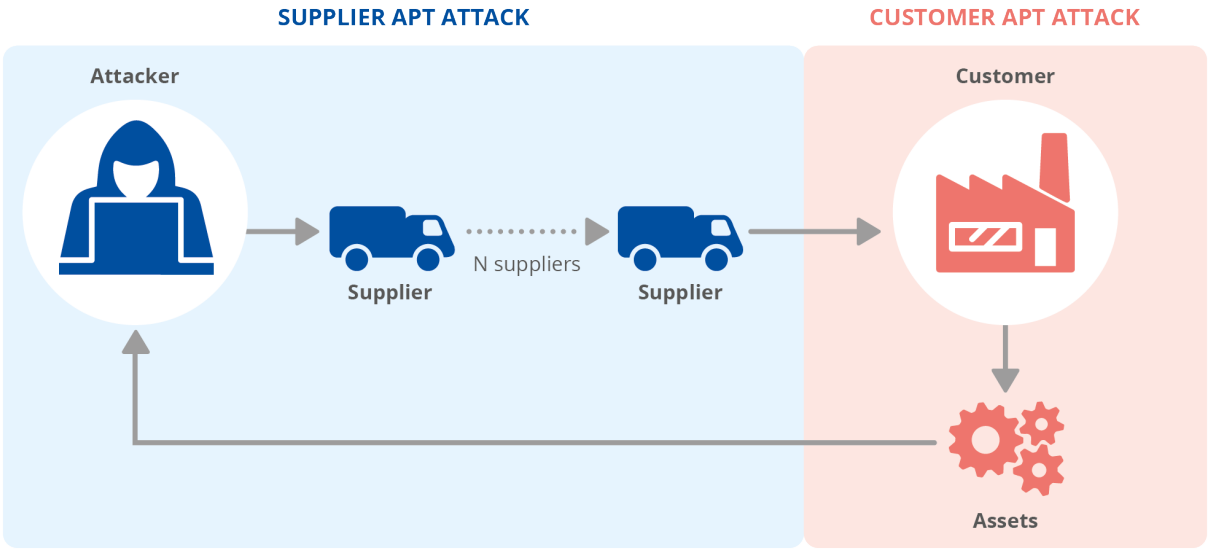
Queste distinzioni sono fondamentali per comprendere **che un'organizzazione potrebbe essere vulnerabile a un attacco alla catena di approvvigionamento anche quando le sue difese sono abbastanza buone** e, quindi, che gli autori degli attacchi stanno cercando di esplorare nuovi potenziali percorsi per infiltrarsi passando ai fornitori per farne un obiettivo. Inoltre, l'impatto potenziale degli attacchi alla catena di approvvigionamento che colpiscono numerosi clienti dello stesso fornitore è probabilmente immenso. Questo è un altro motivo per cui questi tipi di attacchi stanno diventando sempre più comuni: forniscono agli avversari mezzi per aumentare potenzialmente la loro reputazione, e possibilmente ne ricavano grandi guadagni finanziari.

Un'ulteriore caratteristica degli attacchi alla catena di approvvigionamento comporta la complessità del gestirli e gli sforzi necessari per mitigare e affrontare tali attacchi. Il semplice fatto che almeno due entità organizzative siano interessate e l'uso, molto probabilmente, di sofisticati vettori di attacco complicano la gestione di un incidente, l'analisi forense e la gestione complessiva dell'incidente. Il fatto che il rapporto fornitore-consumatore sia in continua evoluzione e che sia i fornitori sia i clienti aggiornino costantemente i propri sistemi, introduce la necessità di una sicurezza continua nella catena di approvvigionamento e di una valutazione e gestione attiva dei rischi.

Il ciclo di vita di un attacco alla catena di approvvigionamento è costituito da due parti principali: l'attacco al fornitore e l'attacco al cliente. Ciascuno di questi attacchi è solitamente complesso, in quanto richiede un vettore di attacco, un piano d'azione e un'attenta esecuzione. Questi attacchi possono richiedere mesi per riuscire e, in molti casi, possono rimanere inosservati per un lungo periodo di tempo. Il ciclo di vita di un attacco alla catena di approvvigionamento è illustrato nella Figura 2.

Il primo attacco del ciclo di vita è denominato "attacco APT al fornitore" e si concentra sulla compromissione di uno o più fornitori. Il secondo attacco del ciclo di vita è denominato "attacco APT al cliente" e si concentra sull'obiettivo finale dell'attacco. Queste due parti sono collegate dall'accesso al fornitore ma, in caso contrario, potrebbero presentare differenze nelle tecniche utilizzate, nei vettori di attacco sfruttati e nel tempo dedicato all'attacco.

Figura 2. Il ciclo di vita degli attacchi alla catena di approvvigionamento può essere visto come due attacchi APT intrecciati. Il primo attacco riguarda uno o più fornitori, mentre il secondo attacco riguarda i clienti. Questi attacchi richiedono un'attenta pianificazione ed esecuzione.



In almeno undici attacchi su tutti i casi studiati in questa relazione, le indagini hanno confermato che gli attacchi alla catena di approvvigionamento sono stati condotti da gruppi noti di APT. Queste attribuzioni sono state effettuate dalle società di sicurezza responsabili delle relazioni di cui all'allegato A. Negli altri tredici casi gli incidenti non sono stati oggetto di indagini complete o l'attribuzione non è stata possibile. Tali attribuzioni supportano l'idea che entrambe le parti del ciclo di vita di un attacco alla catena di approvvigionamento possano assomigliare alle attività degli attacchi APT. Vale la pena notare che l'attribuzione degli autori degli attacchi è molto difficile, incline all'errore, imprecisa e politicamente impegnativa, ma non impossibile.

Poiché ogni parte dell'attacco alla catena logistica può essere considerata come un attacco APT, il suo ciclo di vita individuale generalmente seguirebbe le stesse fasi degli altri attacchi APT. Tali stadi sono descritti in dettagli, ad esempio, nel MITRE ATT&CK® Tactics for Enterprises[15].

[15] MITRE ATT&CK® Tactics - Enterprise Version 9, MITRE, https://attack.mitre.org/tactics/enterprise/. consultato il 03/12/2021.

4. ATTACCHI PRINCIPALI ALLA CATENA DI APPROVVIGIONAMENTO

In questa sezione è presentata una sintesi degli attacchi più importanti alla catena di approvvigionamento dal gennaio 2020 all'inizio di luglio 2021, con una classificazione che segue la tassonomia proposta. Questi casi sono stati selezionati per il grande impatto prodotto nella comunità o perché evidenziano alcune caratteristiche importanti (come indicato negli elementi della tassonomia). L'elenco completo e la descrizione di tutti gli attacchi alla catena di approvvigionamento dal gennaio 2020 fino all'inizio di luglio 2021 sono disponibili nell'allegato A.

4.1. SOLARWINDS ORION. GESTIONE IT E MONITORAGGIO REMOTO

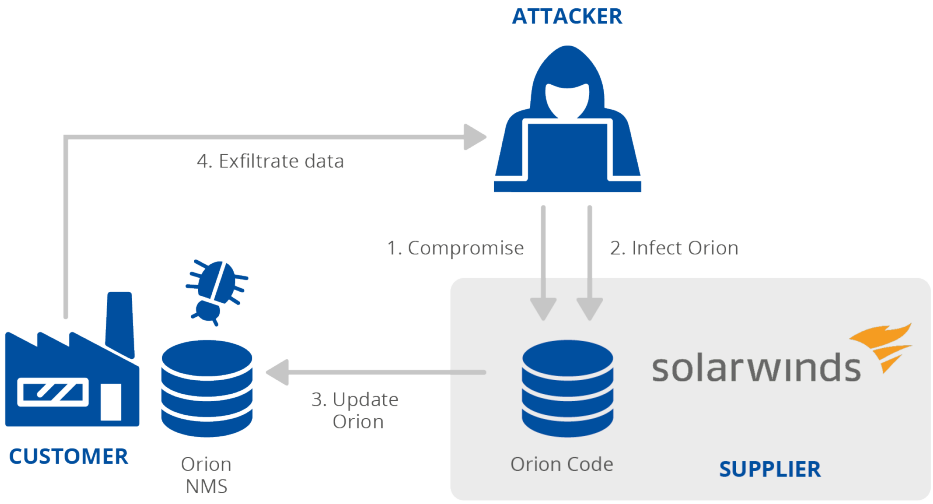
SolarWinds è un'azienda che fornisce software di gestione e monitoraggio[16]. Orion è il prodotto del sistema di gestione della rete SolarWinds (NMS)[17]. Nel dicembre 2020 è stata riscontrata una compromissione in Orion. Un'indagine approfondita ha dimostrato che gli autori degli attacchi hanno ottenuto l'accesso alla rete SolarWinds, possibilmente sfruttando una vulnerabilità zero-day in un'applicazione o dispositivo di terze parti, un attacco di forza bruta o attraverso l'ingegneria sociale. Una volta compromessi, gli autori degli attacchi hanno raccolto informazioni per un periodo di tempo prolungato. Il software dannoso è stato iniettato in Orion durante il processo di creazione[18,19]. Il software compromesso è stato scaricato direttamente dai clienti, quindi è stato utilizzato per raccogliere e rubare informazioni[20]. L'attacco è stato attribuito al gruppo APT29[21,22].

Tabella 7. La tassonomia di attacco alla catena di approvvigionamento applicata all'attacco a SolarWinds. Gli autori degli attacchi hanno utilizzato più tecniche di attacco per compromettere il software SolarWinds Orion. Hanno modificato il codice nel fornitore e abusato del rapporto di fiducia dei clienti in SolarWinds per aggiornare i clienti con malware. L'obiettivo finale degli autori degli attacchi era costituito dai dati dei clienti.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Sfruttamento della vulnerabilità del software, Attacco "brute-force", Ingegneria sociale	Processi, codice	Rapporto di fiducia [T1199], Infezione da malware	Dati

[16] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. consultato il 03/12/2021.
[17] Orion Platform - Scalable IT Monitoring, SolarWinds, https://www.solarwinds.com/solutions/orion. consultato il 03/12/2021.
[18] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. consultato il 03/12/2021.
[19] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. consultato il 03/12/2021.
[20] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. consultato il 03/12/2021.
[21] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. consultato il 03/12/2021.
[22] Russian hacker group 'Cozy Bear' behind Treasury and Commerce breaches, The Washington Post, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html. consultato il 08/07/2021.

Figura 3. Diagramma dell'attacco alla catena di approvvigionamento di SolarWinds. Gli autori degli attacchi hanno compromesso SolarWinds e modificato il codice del software ORION. Le istanze ORION nei clienti sono state aggiornate con malware, consentendo agli autori degli attacchi di accedere ai dati dei clienti.



4.2. MIMECAST. SERVIZI DI CIBERSICUREZZA CLOUD

Mimecast è un fornitore di servizi di cibersicurezza basati su cloud. Tra i servizi forniti rientrano quelli relativi alla sicurezza della posta elettronica, che richiedono ai clienti di collegarsi in modo sicuro ai server Mimecast per utilizzare i propri account Microsoft 365. Nel gennaio 2021 è stato scoperto che utenti malintenzionati avevano compromesso Mimecast (tramite il fornitore SolarWinds). La compromissione ha fatto sì che tali utenti malintenzionati ottenessero un certificato rilasciato da Mimecast, utilizzato dai clienti per accedere ai servizi Microsoft 365; gli autori degli attacchi hanno potuto così intercettare le connessioni di rete e connettersi agli account Microsoft 365 per rubare informazioni[23,24]. L'attacco è stato attribuito al gruppo APT29[25]. La compromissione del fornitore è stata collegata a SolarWinds, ma non vi sono informazioni concrete che confermino tale collegamento.

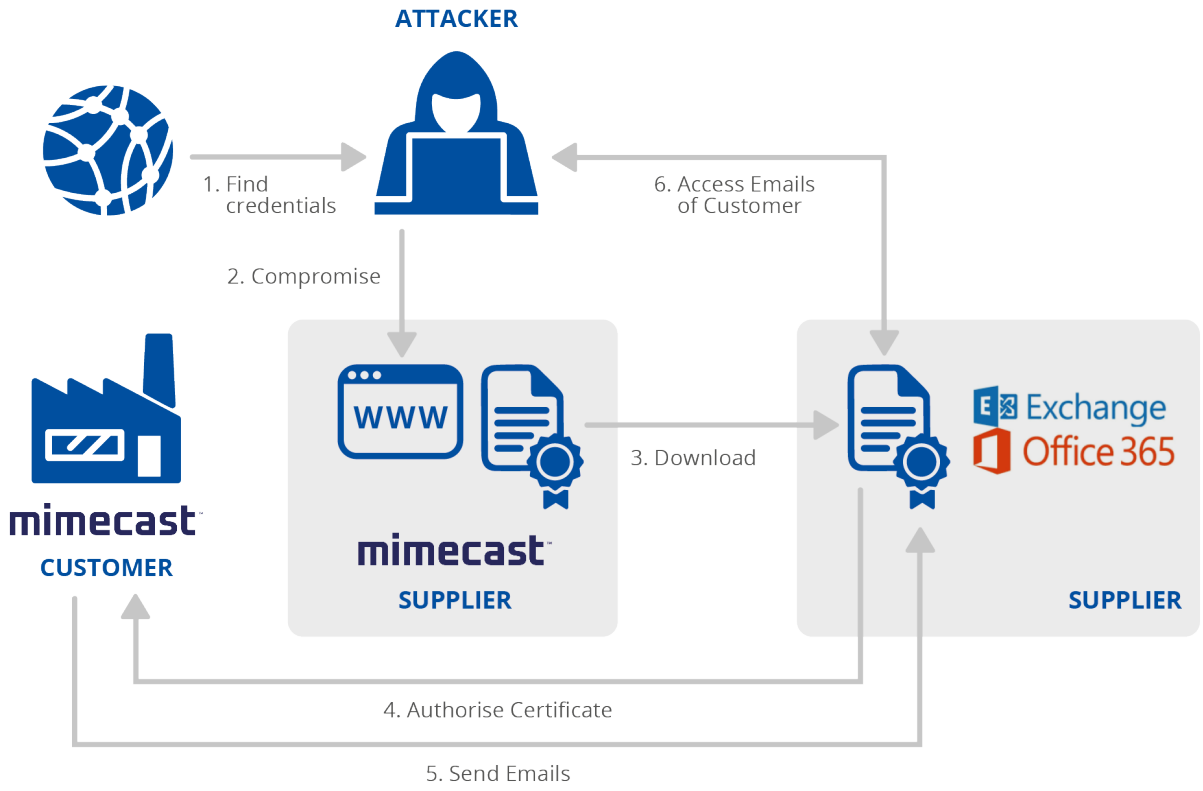
Tabella 8. La tassonomia degli attacchi alla catena di approvvigionamento applicata all'attacco di Mimecast. Non è noto in che modo gli aggressori abbiano preso di mira i dati dei fornitori, in particolare un certificato rilasciato da Mimecast-issued. Gli aggressori hanno abusato del rapporto di fiducia tra la società e i suoi clienti, i quali caricavano i propri dati su Mimecast. Gli autori degli attacchi hanno avuto accesso ai dati dei clienti a Mimecast.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Dati

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199]	Dati

[23] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. consultato il 03/12/2021.
[24] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. consultato il 03/12/2021.
[25] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. consultato il 03/12/2021.

Figura 4. Schema dell'attacco alla catena di approvvigionamento Mimecast. Gli autori degli attacchi hanno trovato credenziali utili per compromettere il fornitore e accedere ai suoi certificati, utilizzati a loro volta per accedere ai dati dei clienti dopo che questi ultimi convalidavano e rendevano accessibili i certificati.



4.3. LEDGER. PORTAFOGLI HARDWARE

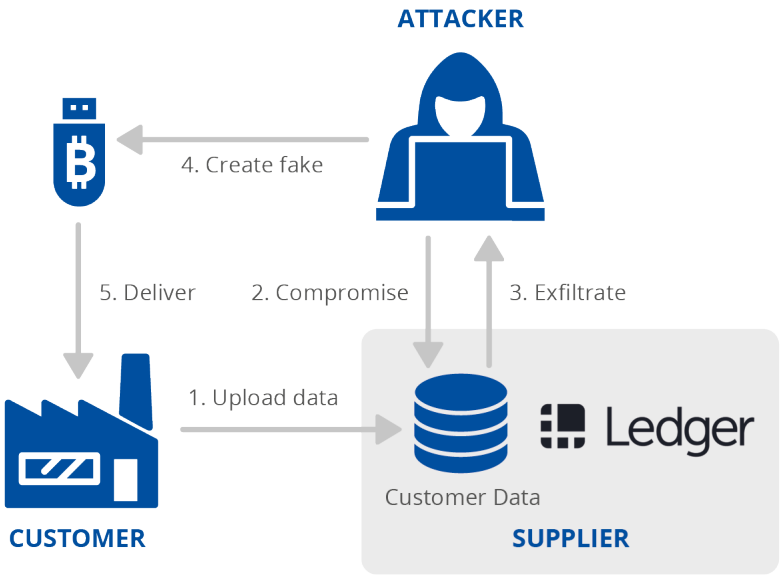
Ledger è un'impresa che fornisce tecnologia hardware per portafogli per criptovalute. Nel luglio 2020, gli aggressori hanno ottenuto valide credenziali per accedere alla banca dati di commercio elettronico di Ledger[26]. I dati rubati sono stati resi pubblici in un forum online[27]. Gli autori degli attacchi hanno utilizzato i dati rubati per phishing e estorsione online degli utenti[28,29]e per rubare denaro degli utenti attraverso un attacco fisico, dopo aver fornito agli utenti portafogli Ledger contraffatti che, se collegati a un computer che richiede le chiavi di sicurezza, potrebbero infettare il computer con malware e rinviare le informazioni rubate agli autori degli attacchi[30]. Gli autori dell'attacco sono sconosciuti.

Tabella 9. La tassonomia degli attacchi alla catena di approvvigionamento applicata all'attacco di Ledger. Gli autori degli attacchi hanno utilizzato tecniche di intelligence open source per trovare credenziali valide per accedere ai registri di registro e rubare i dati dei clienti. Con tali dati, hanno sfruttato il rapporto di fiducia dei clienti verso Ledger inviando messaggi di phishing e false cripto-portafogli su unità USB per rubare criptovalute ai clienti.

[26] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership, Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. consultato il 03/12/2021.
[27] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. consultato il 03/12/2021.
[28] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. consultato il 03/12/2021.
[29] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, Bitdefender HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html, consultato il 03/12/2021.
[30] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. consultato il 08/07/2021.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
OSINT	Dati	Rapporto di fiducia [T1199], Phishing [T1566], Contraffazione	Ambito finanziario

Figura 5. Schema dell'attacco alla catena di approvvigionamento Ledger. Gli autori degli attacchi hanno trovato le credenziali di Ledger online, hanno eseguito l'accesso alla banca dati dei clienti e utilizzato le informazioni per attaccare i clienti.



4.4. KASEYA. SERVIZI DI GESTIONE IT COMPROMESSI CON RANSOMWARE

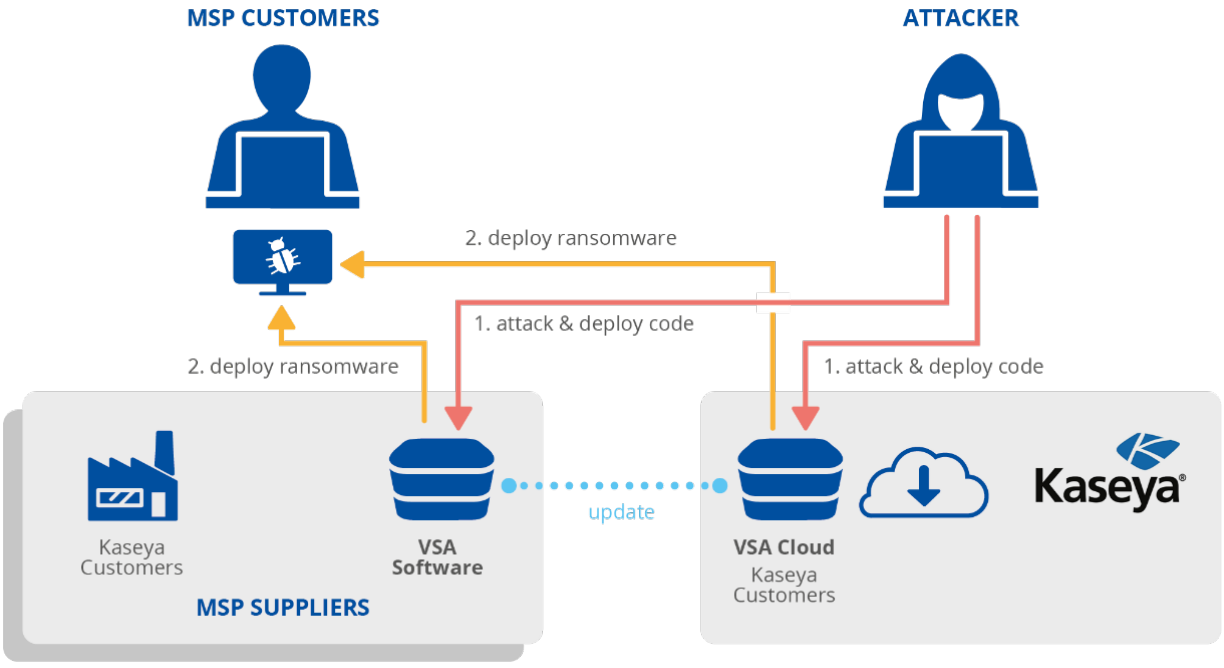
Kaseya è un fornitore di servizi software specializzato in strumenti di monitoraggio e gestione in remoto. Offre ai propri clienti software VSA (Virtual System/Server Administrator) da scaricare e da utilizzare anche attraverso i suoi server cloud. I provider di servizi gestiti (MSP) possono utilizzare il software VSA in sede oppure possono operare con licenza sui server cloud VSA di Kaseya. Gli MSP, a loro volta, offrono vari servizi IT ad altri client[31]. Nel luglio 2021, utenti malintenzionati hanno sfruttato una vulnerabilità a zero giorni nei sistemi di Kaseya (CVE-2021-30116[32]) che ha consentito loro di eseguire comandi in modalità remota sui dispositivi VSA dei clienti di Kaseya. Kaseya è in grado di inviare aggiornamenti remoti a tutti i server VSA. Venerdì 2 luglio 2021, è stato distribuito un aggiornamento al sistema VSA dei client Kaseya che ha eseguito codice proveniente dagli autori degli attacchi. Questo codice dannoso ha, a sua volta, distribuito ransomware[33,34] ai clienti gestiti da tale VSA.

[31] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. consultato il 03/12/2021.
[32] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116 consultato il 03/12/2021.
[33] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/. consultato il 03/12/2021.
[34] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. consultato il 03/12/2021.

Tabella 10. La tassonomia di attacco alla catena di approvvigionamento applicata all'attacco a Kaseya. Sfruttando una vulnerabilità del software, utenti malintenzionati hanno ottenuto l'accesso al software Kaseya. Hanno sfruttato questo accesso per installare ransomware nell'infrastruttura dei clienti. L'attacco ha preso di mira dati e risorse finanziarie dei clienti Kaseya attraverso richieste di riscatto.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Sfruttamento della vulnerabilità del software	Software preesistente	Rapporto di fiducia [T1199], Infezione da malware	Dati, aspetti finanziari

Figura 6. Schema dell'attacco alla catena di approvvigionamento di Kaseya. Gli autori degli attacchi hanno distribuito il codice alle istanze VSA dei fornitori MSP (sia nel cloud che in sede, è ancora sotto esame). Alcuni MSP, a loro volta, sono stati sfruttati per distribuire malware e ransomware ai rispettivi client.



4.5. UN ESEMPIO CON MOLTE INCOGNITE: SISTEMA DI ASSISTENZA PASSEGGERI SITA

Il caso di SITA è importante per i molti componenti degli attacchi alla catena di approvvigionamento che restano **sconosciuti** e per le possibili implicazioni del loro impatto. Dimostra che possono esservi molte circostanze in cui i dettagli degli attacchi non vengono mai pubblicati, a causa di impossibilità tecniche o di decisioni politiche e di marketing da parte delle aziende. Esiste un compromesso tra un vantaggio per la comunità, che può migliorare la propria sicurezza attraverso i dettagli appresi dalle compromissioni subite da altri, e i benefici per le singole aziende, ad esempio finanziarie, in termini di reputazione e di mercato[35].

[35] Investors in SolarWinds sold millions in stock before Russia breach revealed, The Washington Post, https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/. consultato il 05/12/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

SITA è un'azienda specializzata in tecnologia di informazione aerea e informazioni di trasporto. Il sistema di servizio passeggeri SITA è utilizzato per fornire alle compagnie aeree informazioni sui passeggeri al momento dell'imbarco, compreso il rischio che i passeggeri potrebbero rappresentare per un paese[36].

Nel marzo 2021, è stato rivelato che utenti malintenzionati avevano compromesso i server SITA per ottenere l'accesso ai dati dei passeggeri dai clienti di SITA. Alcuni clienti di SITA hanno segnalato anche violazioni dei dati, come Air India, Singapore Airlines e Malaysia Airlines[36].

A seguito di segnalazioni di dati trapelati su Internet, Air India ha anche riferito che le sue reti erano state compromesse e i dati rubati.[37] La compromissione delle reti interne di Air India era presumibilmente legata all'incidente SITA, perché una società di sicurezza ha scoperto che il nome di un computer interno di Air India era "SITASERVER4". Ad oggi, non è ancora noto come gli autori degli attacchi abbiano ottenuto l'accesso ai server SITA e non è noto come abbiano avuto accesso a Air India o se vi siano effettivamente riusciti. L'attacco interno alle reti di Air India è stato attribuito al gruppo APT41[37].

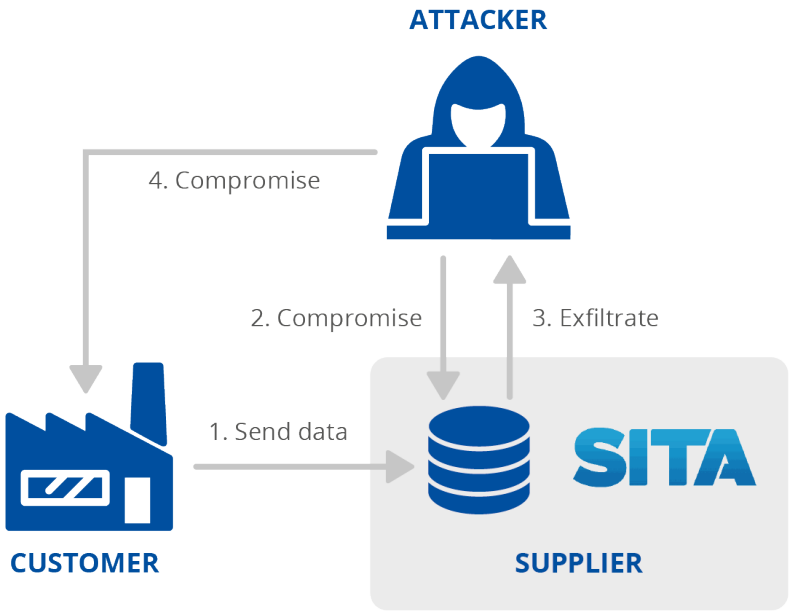
Il numero di variabili sconosciute in questo incidente è un esempio del panorama delle minacce che si presentano in caso di attacchi alla catena di approvvigionamento. Il livello di maturità delle indagini cibernetiche e di preparazione di molte organizzazioni dovrebbe estendersi anche ai rispettivi fornitori, in considerazione delle complesse relazioni intrecciate.

Tabella 11. La tassonomia di attacco alla catena di approvvigionamento applicata all'attacco a SITA. Non è noto come gli autori degli attacchi hanno effettuato l'accesso al fornitore. Sono riusciti ad accedere ai dati del fornitore relativi ai suoi clienti. Non è noto come siano riusciti a infiltrarsi in Air India. Le informazioni disponibili indicano che l'obiettivo principale degli autori degli attacchi era costituito dai dati dei clienti.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Dati	Tecnica sconosciuta	Dati personali

[36] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. consultato il 03/12/2021.
[37] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. consultato il 03/12/2021.

Figura 7. Schema dell'attacco alla catena di approvvigionamento di SITA. Gli autori degli attacchi hanno rubato i dati dei passeggeri dalle aziende clienti di SITA. Ad oggi, non è ancora noto come gli autori degli attacchi abbiano ottenuto l'accesso ai server SITA e non è noto come abbiano avuto accesso a Air India o se vi siano effettivamente riusciti.



5. ANALISI DEGLI INCIDENTI DELLA CATENA DI APPROVVIGIONAMENTO

In questa sezione, è presentata un'analisi degli attacchi alla catena di approvvigionamento basata sugli attacchi segnalati dall'inizio del 2020 fino all'inizio di luglio 2021. L'analisi si concentra sugli attacchi alla catena di approvvigionamento resi pubblici e riporta, nell'allegato A, una panoramica dettagliata. Come descritto più avanti, alcuni attacchi che sembravano essere attacchi alla catena di approvvigionamento, in realtà non lo erano e, quindi, sono stati omessi dall'analisi. Un riepilogo di tutti gli incidenti analizzati nella relazione è riportato nella tabella 12.

Tabella 12. Riepilogo degli attacchi alla catena di approvvigionamento identificati, analizzati e convalidati da gennaio 2020 all'inizio di luglio 2021.

FORNITORE	CATEGORIA DI FORNITORI	ANNO	IMPATTO	GRUPPI ATTRIBUITI
Mimecast	Software di sicurezza	2021	Globale	APT29
SITA	Aviazione	2021	Globale	APT41
Ledger	Blockchain	2021	Globale	-
Verkada	Sicurezza fisica	2021	Globale	Gruppo hacktivist
BigNox NoxPlayer	Software	2021	Regionale	-
Shipper Investment Messenger	Software finanziario	2021	Regionale	Thallium APT
ClickStudios	Software di sicurezza	2021	Regionale	-
Apple Xcode	Software di sviluppo	2021	Globale	-
Sito del presidente del Myanmar	Pubblica amministrazione	2021	Regionale	PAT Mustang Panda
Ucraina SEI EB	Pubblica amministrazione	2021	Regionale	-
Codecov	Software per imprese	2021	Globale	-
Fujitsu ProjectWEB	Collaborazione cloud	2021	Regionale	-
Kaseya	Gestione dei sistemi informatici	2021	Globale	Gruppo REVIL
MonPass	Autorità di certificazione	2021	Regionale	Winnti APT Group
SYNNEX	Distributore di tecnologia	2021	Regionale	APT 29
Microsoft Windows HCP	Software	2021	Globale	-
SolarWinds	Gestione del cloud	2020	Globale	APT29
Accellion	Software di sicurezza	2020	Globale	UNC2546
Wizvera Veraport	Gestione identità	2020	Regionale	PAT Lazarus
Able Desktop	Software per imprese	2020	Regionale	TA428
Aisino	Software finanziario	2020	Regionale	-

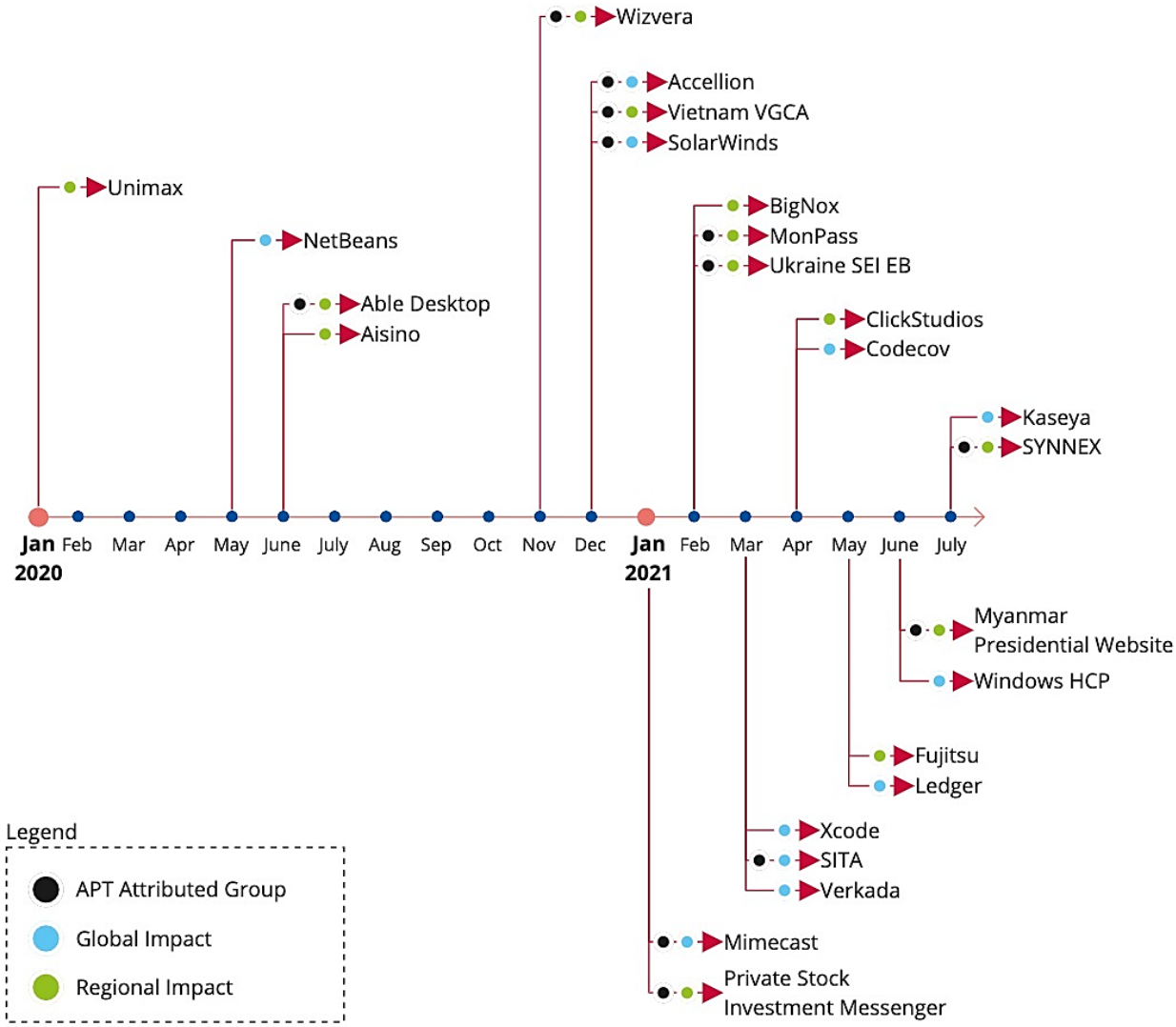
Vietnam VGCA	Autorità di certificazione	2020	Regionale	TA413, TA428
NetBeans	Software di sviluppo	2020	Globale	-
Unimax	Telecomunicazione	2020	Regionale	-

5.1. SEQUENZA TEMPORALE DEGLI ATTACCHI ALLA CATENA DI APPROVVIGIONAMENTO

L'analisi mostra che su 24 attacchi confermati alla catena di approvvigionamento, 8 (33 %) sono stati segnalati nel 2020, mentre 16 (66 %) riguardano il periodo da gennaio 2021 all'inizio di luglio 2021. **Sulla base di questi dati, il trend prevede per il 2021 un numero di attacchi alla catena di approvvigionamento di 4 volte superiore rispetto al 2020.**

La figura 8 mostra una sequenza temporale degli attacchi analizzati in questa relazione, evidenziando gli incidenti attribuiti ai gruppi APT e se hanno avuto un impatto globale o regionale. Per ogni attacco l'impatto può essere classificato come globale o regionale. Gli attacchi sono considerati di impatto globale se la base clienti è globale oppure se il numero di utenti finali potenzialmente interessati è in milioni. In alternativa, gli attacchi che hanno un impatto sugli utenti in una regione o in un paese specifico oppure che interessano solo pochi utenti sono considerati attacchi di portata regionale.

Figura 8. Sequenza temporale di attacchi alla catena di approvvigionamento segnalati da gennaio 2020 all'inizio di luglio 2021. Il mese indicato nella figura si riferisce al mese in cui è stato segnalato l'incidente, non al mese in cui è avvenuto l'attacco. Gli incidenti attribuiti ai gruppi APT sono contrassegnati con punti neri, gli incidenti con impatto globale sono contrassegnati con punti viola e gli incidenti con impatto regionale sono contrassegnati con punti verdi. Un riepilogo dettagliato di ciascun incidente è disponibile nell'allegato A.



5.2. COMPRENDERE IL FLUSSO DEGLI ATTACCHI

Ciascuno degli incidenti mostrati nella figura 7 è stato analizzato, riassunto e classificato secondo la tassonomia proposta. La tassonomia supporta e facilita lo studio degli attacchi alla catena di approvvigionamento nel suo complesso in modo strutturato.

La figura 8 è un diagramma di Sankey[38], che illustra il flusso delle tecniche di attacco e delle risorse più comuni osservate negli attacchi alla catena di approvvigionamento studiati in questa relazione. **Le tecniche di attacco [ST] sono usate contro i beni dei fornitori [SA], che a loro volta vengono usati nelle tecniche di attacco [CT] per compromettere i beni dei clienti [CA].**

Nella figura 8 viene descritto in modo chiaro che la maggior parte delle tecniche di attacco utilizzate per compromettere il fornitore (prima colonna [ST]) sono:

- **Tecnica sconosciuta (66%)**, seguita da
- **Sfruttamento della vulnerabilità del software (16%)**.

[38] I diagrammi Sankey sono un tipo specifico di diagramma di flusso, in cui la larghezza delle frecce è mostrata proporzionalmente alla quantità di flusso.

In termini di risorse destinate ai fornitori (seconda colonna [SA]), la maggior parte degli attacchi mirava a compromettere:

- **codice (66%)**;
- **dati (20%);**
- **processi (12%)**.

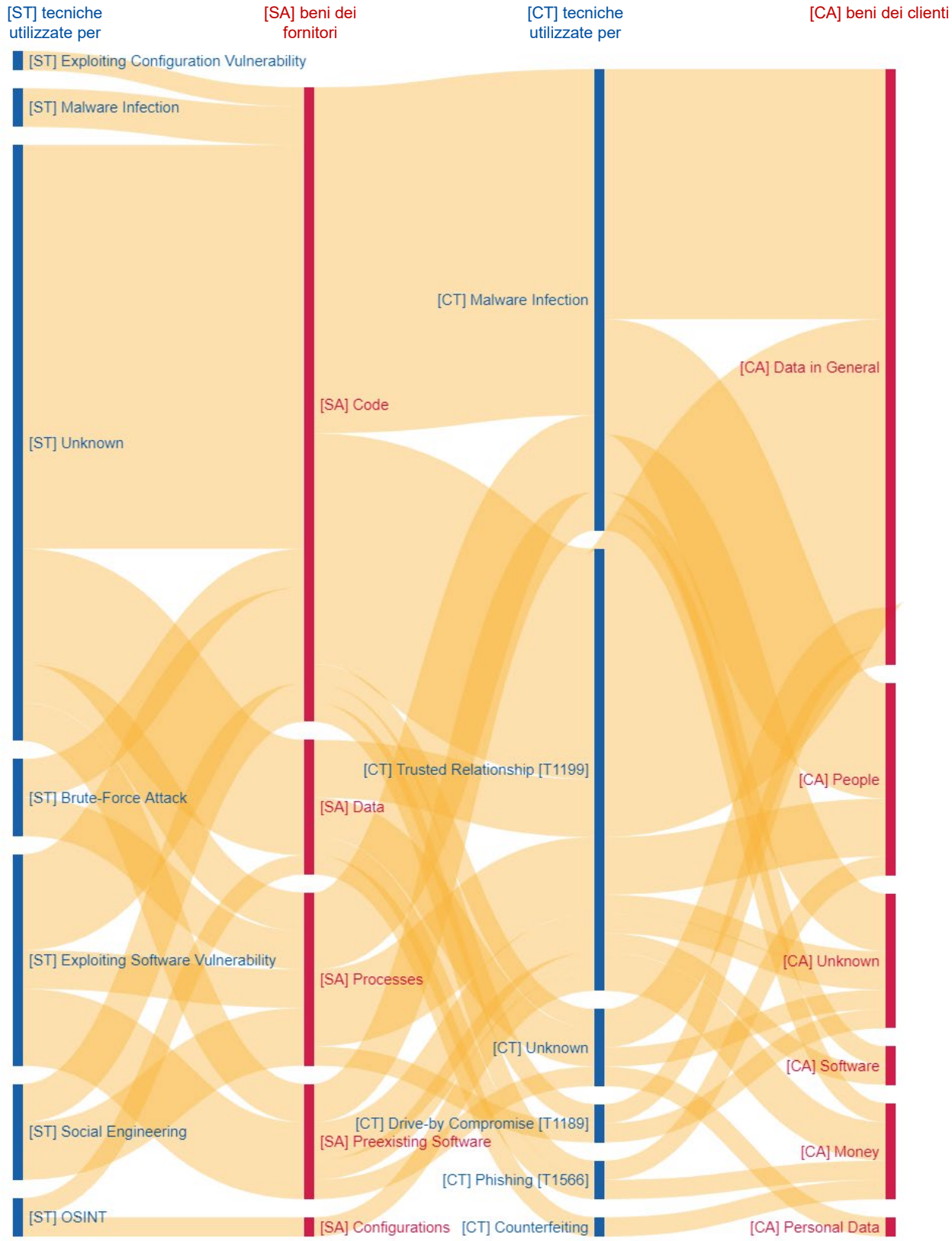
I beni dei fornitori compromessi vengono utilizzati come vettore di attacco per compromettere i clienti. Tali attacchi sono principalmente eseguiti (terza colonna [CT]) con le azioni seguenti:

- **abuso della fiducia del client (62%)** nel fornitore; oppure,
- **malware (62%)**.

Indipendentemente dalla tecnica utilizzata, la maggior parte degli attacchi alla catena di approvvigionamento mira a ottenere l'accesso a (quarta colonna [CA]):

- **dati (58%)** del cliente;
- **persone (16%)** importanti; e,
- **risorse finanziarie (8%)**.

Figura 9. Analisi degli incidenti della catena di approvvigionamento in base alla tassonomia proposta. Il diagramma Sankey descrive il flusso di tecniche di attacco [ST] usate contro i beni dei fornitori [SA], che a loro volta vengono usate nelle tecniche di attacco [CT] per compromettere i beni dei clienti [CA]. La larghezza delle connessioni tra i vari elementi aumenta quando la relazione viene osservata in un numero maggiore di attacchi alla catena di approvvigionamento.



5.3. ATTACCHI MIRATI A OBIETTIVI

Per quanto riguarda di attacchi che prendono di mira beni specifici, nel **66%** di questi gli autori degli attacchi si sono concentrati sul codice dei fornitori per compromettere ulteriormente i clienti interessati. Nel **20%** degli incidenti analizzati, l'obiettivo degli autori degli attacchi era costituito da **dati**, mentre nel **12%** dei casi gli obiettivi dell'attacco al fornitore erano **processi interni**. Queste informazioni sono fondamentali per comprendere dove concentrare gli sforzi in termini di protezione e cibersicurezza. Le organizzazioni devono concentrare i propri sforzi sulla convalida di codice e software di terze parti in modo da garantire che non siano stati manomessi o alterati.

I beni dei clienti finali presi di mira da questi attacchi alla catena di approvvigionamento sembrano essere prevalentemente dati dei clienti, inclusi i dati personali e relativi alla proprietà intellettuale. Così è stato nel 58 % degli incidenti analizzati nella catena di approvvigionamento. Gli autori degli attacchi hanno anche preso di mira in misura minore altre risorse, tra cui persone, software e risorse finanziarie.

5.4. LA MAGGIOR PARTE DEI VETTORI DI ATTACCO PER COMPROMETTERE I FORNITORI RIMANE SCONOSCIUTA

Le ricerche effettuate dimostrano che nel **66%** degli attacchi alla catena di approvvigionamento analizzati, **i fornitori non sapevano** come fossero stati compromessi, o non sono stati chiari in merito. Al contrario, meno del **9%** dei clienti compromessi dagli attacchi alla catena di approvvigionamento non sapeva come si fossero verificati gli attacchi. **Questi dati evidenziano il divario in termini di maturità nella segnalazione di incidenti alla cibersicurezza tra fornitori e aziende a contatto con utenti finali.**

Considerando che l'**83 %** dei fornitori opera nel settore della **tecnologia**, la mancanza di conoscenze sul modo in cui sono accaduti gli attacchi potrebbe indicare un **livello di maturità scarso** in materia di cyber-difesa nelle infrastrutture dei fornitori, oppure una certa riluttanza a condividere le informazioni pertinenti. Altri fattori possono contribuire a una mancanza di comprensione del modo in cui i fornitori vengono compromessi: la complessità e la sofisticazione degli attacchi e la lentezza nella scoperta degli attacchi, che a loro volta possono ostacolare le indagini.

5.5. ATTACCHI SOFISTICATI ATTRIBUITI AI GRUPPI APT

Oltre il **50% degli attacchi alla catena di approvvigionamento sono stati attribuiti a**gruppi di criminalità informatica ben noti, tra cui APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413 e TA428. L'analisi mostra che i gruppi APT sembrano propendere leggermente per obiettivi con impatto regionale e che un numero significativo di tali attacchi abbia come scopo l'accesso ai dati dei clienti.

Dei 24 incidenti analizzati, 10 non sono stati attribuiti ad alcun gruppo specifico. Il motivo principale della mancanza di attribuzione può essere che 7 di questi attacchi sono avvenuti negli ultimi 7 mesi. Incidenti di questo tipo possono necessitare di indagini più lunghe e, anche dopo del tempo, in alcuni casi, non è ancora possibile individuare gli autori. Tuttavia, data la complessità di questi attacchi, i fornitori dovrebbero prevedere che potrebbero essere presi di mira da gruppi organizzati di criminalità informativa e prepararsi di conseguenza.

6. NON TUTTI GLI ATTACCHI SONO ATTACCHI ALLA CATENA DI APPROVVIGIONAMENTO

Dal gennaio 2020 all'inizio di luglio 2021 si sono verificati molti incidenti che inizialmente **sembravano** attacchi alla catena di approvvigionamento o erano considerati parte di un probabile attacco futuro alla catena di approvvigionamento. Molte vulnerabilità del software tradizionali riscontrate sono state segnalate come "rischio" per futuri attacchi alla catena di approvvigionamento. Alcuni casi riguardavano vulnerabilità ritenute inserite intenzionalmente nel software o nell'hardware; successivamente, però, sono state riscontrate come bug o errori involontari. Molti di questi casi non erano attacchi alla catena di approvvigionamento in quanto non hanno comportato la compromissione di un fornitore.

In almeno tre occasioni gli autori hanno preso di mira biblioteche di software o dipendenze. In uno di questi casi, segnalato nel dicembre 2020, gli aggressori hanno caricato pacchetti dolosi nell'archivio RubyGems[39]. Un caso molto simile è stato segnalato nel marzo 2021, quando un ricercatore nel settore della sicurezza è riuscito a caricare pacchetti NPM pericolosi utilizzando nomi noti come nomi di componenti o infrastrutture utilizzati da società note[40]. Un terzo caso è stato segnalato nell'aprile 2021, quando gli autori di attacchi hanno caricato un pacchetto NPM doloso tentando di impersonare deliberatamente un pacchetto conosciuto in un attacco di tipo "dubbed brandjacking"[41]. In tutti questi casi, gli autori degli attacchi non hanno compromesso i pacchetti esistenti né gli archivi di software stessi; pertanto, non essendovi un chiaro attacco ai beni dei fornitori, non possono essere considerati attacchi alla catena di approvvigionamento.

In molti casi, le vulnerabilità del software sono state scoperte ma non utilizzate in attacchi oppure sono state individuate come errori e non introdotte intenzionalmente. Il primo esempio di questo caso è stato segnalato nel febbraio 2020, quando un ricercatore nel settore della sicurezza ha rivelato una vulnerabilità a 0 giorni nel firmware elaborati dalla società Xiaongmai e utilizzato per DVR, NVR e videocamere IP[42]. Tra gli altri esempi figurano le vulnerabilità segnalate nelle estensioni del codice dello Studio Visual Studio nel maggio 2021[43] e quelle relative ai mercati di software libero e open source (FOSS) basati su Pling nel giugno 2021[44]. In tutti questi casi, al momento della redazione della presente relazione sono emerse vulnerabilità ma non sono stati segnalati attacchi attivi derivanti da tali vulnerabilità. Come indicato nelle sezioni precedenti, un attacco alla catena di approvvigionamento comporta almeno due attacchi: uno nei confronti di un fornitore e uno nei confronti di un cliente. In assenza di un attacco contro un cliente o un fornitore, l'attacco non è considerato un attacco alla catena di approvvigionamento.

Inoltre, si sono verificati altri attacchi alla cibersicurezza e vulnerabilità che non si sono trasformate in attacchi alla catena di approvvigionamento. Uno di questi è l'attacco ai sistemi di Centreon. Centreon è un'impresa che fornisce servizi di monitoraggio informatico e offre uno strumento di monitoraggio informatico open source. Nel gennaio 2021, è stato scoperto che utenti malintenzionati avevano sfruttato vecchi casi pubblici di Centreon per compromettere le

[39] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. consultato il 03/12/2021.
[40] Malicious NPM packages target Amazon, Slack with new dependency attacks, Bleeping Computer, https://www.bleepingcomputer.com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/. consultato il 03/12/2021.
[41] Damaging Linux \& Mac Malware Bundled within Browserify npm Brandjack Attempt, Sonatype, https://blog.sonatype.com/damaging-linux-mac-malware-bundled-within-browserify-npm-brandjack-attempt. consultato il 03/12/2021.
[42] Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras, Habr, https://habr.com/en/post/486856/. consultato il 03/12/2021.
[43] Newly Discovered Bugs in VSCode Extensions Could Lead to Supply Chain Attacks, The Hacker News, https://thehackernews.com/2021/05/newly-discovered-bugs-in-vscode.html. consultato il 03/12/2021.
[44] Unpatched Flaw in Linux Pling Store Apps Could Lead to Supply-Chain Attacks, The Hacker News, https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.html. consultato il 03/12/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

infrastrutture dei clienti[45,46,47]. Gli autori degli attacchi, ritenuti essere il gruppo APT Sandworm, hanno condotto la campagna per tre anni, fino alla scoperta. L'attacco mirava a esfiltrare informazioni dai clienti interessati, era rivolto ai fornitori francesi di tecnologie dell'informazione. Si tratta di un caso in cui una particolare vulnerabilità del software è stata sfruttata in un software installato dai clienti. Tuttavia, il fornitore stesso non è stato compromesso e le vulnerabilità non sono state intenzionali.

[45] Sandworm Intrusion Set Campaign Targeting Centreon Systems, CERT-FR, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf. consultato il 03/12/2021.
[46] France Reveals 3-Year Long Supply Chain Attack, Secure World Expo, https://www.secureworldexpo.com/industry-news/france-supply-chain-attack-centreon-software. consultato il 03/12/2021.
[47] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. consultato il 03/12/2021.

7. RACCOMANDAZIONI

Gli attacchi alla catena di approvvigionamento **sfruttano l'interconnessione dei mercati globali**. Quando più clienti fanno affidamento sullo stesso fornitore, le conseguenze di un attacco informatico contro tale fornitore sono amplificate, con potenziali conseguenze a livello nazionale o persino transfrontaliero. Per alcuni prodotti, quali software e codici eseguibili, l'esistenza di una catena di approvvigionamento è "velata" o addirittura completamente nascosta all'utente finale. Il software dell'utente finale dipende, direttamente o indirettamente, dal software fornito dal fornitore. Tali dipendenze comprendono pacchetti, biblioteche e moduli, tutti utilizzati in modo pervasivo per ridurre i costi di sviluppo e accelerare i tempi di spedizione.

Maggiore è la protezione dalle organizzazioni che si occupano di attacchi informatici, maggiore è l'attenzione trasferita ai fornitori. Il risultato è ovvio: i fornitori stanno diventando l'anello più debole della catena di approvvigionamento. Allo stesso tempo, i clienti chiedono prodotti più sicuri dal punto di vista informatico, ma a basso costo: due esigenze che non sempre è possibile conciliare.

Come osservato in numerosi episodi di attacchi alla catena di approvvigionamento, le organizzazioni stanno diventando sempre più consapevoli della necessità di **valutare la maturità dei propri fornitori in termini di cibersicurezza** e di **livello di esposizione al rischio derivante da tale rapporto cliente-fornitore**. I clienti devono valutare e tenere conto della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei fornitori, inclusa l'eventuale applicazione di procedure di sviluppo sicure. Inoltre, dovrebbero esercitare una maggiore diligenza nella selezione e nel controllo dei propri fornitori e nella gestione del rischio derivante da tali relazioni.

Per **gestire il rischio di cibersicurezza della catena di approvvigionamento**, i clienti devono[48]:

- identificare e documentare i tipi di fornitori e prestatori di servizi;
- definire criteri di rischio per i diversi tipi di fornitori e servizi (ad esempio, dipendenze importanti da fornitori e clienti, dipendenze essenziali dal software, singoli punti di guasto);
- valutare i rischi legati alla catena di approvvigionamento in base alle proprie valutazioni d'impatto e ai requisiti in materia di continuità operativa;
- definire misure per il trattamento dei rischi sulla base delle buone pratiche;
- monitorare i rischi e le minacce alla catena di approvvigionamento, sulla base di fonti di informazione interne ed esterne e dei risultati del monitoraggio e dei riesami delle prestazioni dei fornitori;
- sensibilizzare il personale al rischio.

Per **gestire il rapporto con i fornitori**, i clienti devono:

- gestire i fornitori durante l'intero ciclo di vita di un prodotto o di un servizio, comprese le procedure per la manipolazione di prodotti o componenti alla fine del ciclo di vita;
- classificare le attività e le informazioni condivise con i fornitori o ad essi accessibili e definire le procedure pertinenti per il loro accesso e il loro trattamento;
- definire gli obblighi dei fornitori per la protezione delle risorse dell'organizzazione, la condivisione delle informazioni, i diritti di audit, la continuità operativa, lo screening del personale e la gestione degli incidenti in termini di responsabilità, obblighi di notifica e procedure;
- definire i requisiti di sicurezza per i prodotti e i servizi acquisiti;
- includere tutti questi obblighi e requisiti nei contratti; concordare norme per i subappalti e requisiti potenziali a cascata;
- monitorare le prestazioni del servizio ed eseguire controlli di sicurezza di routine per verificare la conformità ai requisiti di sicurezza informatica negli accordi; tali azioni devono includere la gestione di incidenti, vulnerabilità, patch, requisiti di sicurezza, ecc.;

[48]Derivato dai controlli di cibersicurezza nelle norme ISO/IEC 27002, ISO 9001 e ISO 31000.

- ricevere la garanzia dei fornitori e dei prestatori di servizi che non sono intenzionalmente inclusi elementi occulti o backdoor;
- garantire che siano presi in considerazione i requisiti normativi e giuridici;
- definire processi per gestire i cambiamenti negli accordi con i fornitori, ad esempio cambiamenti negli strumenti, nelle tecnologie, ecc.

D'altro canto, i fornitori dovrebbero garantire **lo sviluppo sicuro di prodotti e servizi**, conformemente alle pratiche di sicurezza comunemente accettate[49]. I fornitori dovrebbero:

- garantire che l'infrastruttura utilizzata per progettare, sviluppare, fabbricare e fornire prodotti, componenti e servizi segua le pratiche di cibersicurezza,[50,51];
- attuare un processo di sviluppo, manutenzione e supporto del prodotto coerente con i processi comunemente accettati di sviluppo del prodotto;
- attuare un processo ingegneristico sicuro coerente con le prassi di sicurezza comunemente accettate[52, 53];
- considerare l'applicabilità dei requisiti tecnici in base alla categoria di prodotto e ai rischi[54];
- offrire dichiarazioni di conformità ai clienti per norme note, ossia ISO/IEC 27001, IEC 62443-41, IEC 62443-42 (o specifiche quali la matrice CSA Cloud Controls Matrix (CCM) per i servizi cloud), e garantire e attestare, nella misura del possibile, l'integrità e l'origine del software open source utilizzato in qualsiasi porzione di prodotto;
- definire obiettivi di qualità quali il numero di difetti o le vulnerabilità individuate esternamente o i problemi di sicurezza segnalati esternamente e utilizzarli come strumento per migliorare la qualità complessiva;
- mantenere dati accurati e aggiornati sull'origine del codice o dei componenti software e sui controlli applicati ai componenti, agli strumenti e ai servizi software interni e di terzi presenti nei processi di sviluppo del software;
- effettuare audit regolari per garantire che le misure adottate siano rispettate.

Inoltre, poiché qualsiasi prodotto o servizio si basa su componenti e software soggetti a vulnerabilità, i fornitori **dovrebbero applicare buone pratiche per la gestione delle vulnerabilità**[55], quali:

- il monitoraggio delle vulnerabilità di sicurezza segnalate da fonti interne ed esterne che comprendono componenti di terzi usati;
- l'analisi dei rischi delle vulnerabilità utilizzando un sistema di punteggio delle vulnerabilità (ad esempio CVSS[56]);
- politiche di mantenimento per il trattamento delle vulnerabilità individuate in funzione del rischio,
- processi di informazione dei clienti,
- verifica e prova delle patch per garantire che i requisiti operativi, di sicurezza, giuridici e di cibersicurezza siano soddisfatti e che la patch sia compatibile con componenti di terzi non incorporati;
- i processi per la consegna sicura di patch e la documentazione relativa alle patch ai clienti, o
- partecipare a un programma di divulgazione delle vulnerabilità che comprenda un processo di segnalazione e divulgazione.

[49] es. IEC 62443-4-1.
[50] es. quelle della norma ISO/IEC 27001.
[51] Tali misure possono includere misure tecniche, quali: (a) separazione di ambienti; (b) controllo dei rapporti di fiducia; (c) creazione di un'autenticazione basata sul rischio e di un accesso condizionato multifattore nell'organizzazione; (d) riduzione delle dipendenze da prodotti che fanno parte degli ambienti utilizzati per sviluppare, costruire e modificare software; (e) crittografia dei dati; (f) monitoraggio di operazioni e avvisi, e attività di risposta a tentativi e incidenti informatici effettivi.
[52] es. IEC 62443-2-4
[53] Tali processi possono includere l'utilizzo di strumenti automatizzati o processi comparabili per mantenere catene di approvvigionamento di codice sorgente attendibili, garantendo in tal modo l'integrità del codice, o l'uso di strumenti automatizzati o processi comparabili, che controllano la presenza di vulnerabilità note e potenziali e le risolvono.
[54] Norme come la IEC 62443-4-2 forniscono una serie completa di requisiti di sicurezza, classificati come requisiti applicabili a tutti i prodotti, applicabili ad applicazioni software (SAR), applicabili a dispositivi integrati (EDR), applicabili a dispositivi host (HDR) e applicabili a dispositivi di rete (NDR).
[55] ulteriori orientamenti sulla gestione delle vulnerabilità e delle patch sono reperibili nelle norme IEC 62443-41, IEC 62443-2-4 e IEC TR 62443-23.
[56] Cfr. https://www.first.org/cvss/specification-document ;.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Le vulnerabilità dovrebbero essere gestite dai fornitori sotto forma di patch. Analogamente, un cliente dovrebbe monitorare il mercato per individuare potenziali vulnerabilità o ricevere le rispettive notifiche di vulnerabilità dai suoi fornitori. Tra le **buone pratiche per la gestione delle patch** figurano[57]:

- tenuta di un inventario delle attività che includa informazioni pertinenti per la ricerca;
- utilizzo di risorse di informazione per individuare le vulnerabilità tecniche pertinenti;
- valutazione dei rischi delle vulnerabilità individuate e disponibilità di una politica di manutenzione documentata e attuata;
- acquisizione di patch solo da fonti legittime e test delle patch prima della loro installazione;
- applicazione di misure alternative qualora una patch non sia disponibile o applicabile;
- applicazione di procedure di retromarcia e di un efficace back-up & ripristino dei processi.

Oltre alle azioni che clienti e fornitori possono adottare individualmente, esistono iniziative che possono avere luogo a livello settoriale. Google ha introdotto, nel giugno 2021, un quadro End-to-end per garantire l'integrità degli artefatti software lungo tutta la catena di approvvigionamento del software denominato SLSA (Supply chain Levels for Software Artifacts)[58]. L'obiettivo dello SLSA è migliorare lo stato dell'industria, in particolare l'open source, per difendersi dalle minacce più pressanti all'integrità. Sebbene lo SLSA si concentri sugli attacchi alla catena di approvvigionamento del software e non su tutti gli altri tipi, si tratta di un buon punto di partenza che può andare a beneficio delle organizzazioni.

Una serie più generale ma ampia di raccomandazioni per la difesa dalle minacce alla cibersicurezza è stata presentata nel giugno 2021 dalla commissione ITRE, nota come progetto MITRE D3FEND[59]. MITRE D3FEND è un quadro o una knowledge base strutturata che consente alle organizzazioni di trovare attenuazioni specifiche per prevenire attacchi specifici, come indicato nel quadro MITRE ATT&CK®. Il progetto non è specifico per la catena di approvvigionamento né per gli attacchi APT, ma le raccomandazioni possono essere utilizzate per aumentare il livello fondamentale di sicurezza delle organizzazioni.

Tuttavia, non tutti i rischi della catena di approvvigionamento possono essere attenuati dalle buone pratiche attuate da clienti, fornitori o organizzazioni. In particolare, le funzioni nascoste e le capacità di accesso non documentate (backdoor) nei componenti hardware non possono essere individuate in modo esaustivo dalle certificazioni più comuni o dai test standard di penetrazione. Inoltre, le vulnerabilità a zero giorni, ossia quelle note solo a un gruppo specifico e da esso utilizzate, continuano a rappresentare una sfida. Di conseguenza, può essere necessario intervenire a livello nazionale o addirittura europeo. Le autorità nazionali competenti potrebbero effettuare valutazioni nazionali dei rischi per la sicurezza della catena di approvvigionamento, che tengano conto dei soggetti noti al fine di definire misure relative all'approvvigionamento dai fornitori a livello nazionale. Inoltre, gli attacchi alla catena di approvvigionamento possono essere sponsorizzati da attori statali con capacità avanzate e in tal caso può essere necessaria l'assistenza delle autorità competenti per attenuare i rischi di attacchi sponsorizzati da uno stato.

[57] Derivata dalla norma ISO/IEC 27002.
[58] Google Online Security Blog: Introducing SLSA, an End-to-End Framework for Supply Chain Integrity, Google, https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html. consultato il 03/12/2021.
[59] MITRE D3FEND™, D3FEND Matrix, Version 0.9.2-BETA-3, https://d3fend.mitre.org/. consultato il 03/12/2021.

8. CONCLUSIONI

Con l'aumentare del costo degli attacchi diretti contro le organizzazioni ben protette, gli autori di attacchi preferiscono attaccare la catena di approvvigionamento tali organizzazioni, il che costituisce l'ulteriore motivazione di un impatto transfrontaliero potenzialmente su larga scala. La migrazione ha portato a un **numero di attacchi alla catena di approvvigionamento superiore al solito**, con una previsione di **attacchi alla catena di approvvigionamento quattro volte superiore nel 2021 rispetto al 2020**. La natura globale intrinseca delle attuali catene di approvvigionamento aumenta l'impatto potenziale di tali attacchi e amplia la superficie degli attacchi per gli attori malintenzionati. La presente relazione riguarda una serie di attacchi noti ma, in realtà, potrebbero esservi più attacchi alla catena di approvvigionamento che non vengono individuati, non indagati o attribuiti ad altre cause.

In particolare nel software, gli attacchi alla catena di approvvigionamento compromettono la fiducia nell'ecosistema del software. Gli incidenti descritti evidenziano la possibilità per gli attori malintenzionati di **compromettere la catena di approvvigionamento del software fin dalle sue primissime fasi** (fase di sviluppo). Occorre sviluppare nuovi approcci per garantire la sicurezza della catena di approvvigionamento fin dalla progettazione. In questa direzione, nuove iniziative quali Google SLSA e MITRE D3FEND sembrano piuttosto promettenti.

L'analisi contenuta nella presente relazione mostra che vi è ancora un gran numero di fattori sconosciuti negli incidenti oggetto di indagine. **Il 66 % dei vettori di attacco utilizzati presso i fornitori è ancora sconosciuto**. La mancanza di trasparenza o la capacità di indagare rappresentano un grave rischio per la fiducia della catena di approvvigionamento. Migliorare il processo di trasparenza e responsabilità è il primo passo per migliorare la sicurezza di tutti gli elementi della catena di approvvigionamento e proteggere i clienti finali.

Gli attacchi alla catena di approvvigionamento possono essere complessi, richiedono un'attenta pianificazione e spesso la loro esecuzione richiede mesi o anni. Mentre **oltre il 50 % di questi attacchi è attribuito a gruppi APT o ad aggressori noti**, l'efficacia degli attacchi alla catena di approvvigionamento può rendere i fornitori un obiettivo interessante per altri tipi più generici di aggressori in futuro. È pertanto fondamentale che le organizzazioni concentrino la propria sicurezza non solo sulle proprie organizzazioni, ma anche sui loro fornitori. Questo vale in particolare per i fornitori di servizi cloud e i fornitori di servizi gestiti, nel cui settore recenti attacchi evidenziano la crescente necessità di controlli della cibersicurezza.

A causa dell'aumento delle interdipendenze e delle complessità, l'impatto degli attacchi contro i fornitori può avere **conseguenze di vasta portata**. Ciò è dovuto non solo al gran numero di parti interessate, ma, soprattutto nei casi in cui le informazioni classificate sono esfiltrate, tale impatto è fonte di preoccupazione per la sicurezza nazionale o per conseguenze di natura geopolitica.

In questo contesto complesso per le catene di approvvigionamento, la definizione di **buone pratiche a livello dell'UE e azioni coordinate sono entrambe importanti** per sostenere tutti gli Stati membri nello sviluppo di capacità analoghe, al fine di raggiungere un livello comune di sicurezza.

ALLEGATO A: SINTESI DEGLI ATTACCHI ALLA CATENA DI APPROVVIGIONAMENTO

La presente sezione riporta una sintesi dei 24 incidenti alla catena di approvvigionamento individuati e analizzati nella presente relazione. Ogni incidente è identificato attraverso il fornitore coinvolto nell'attacco. La tassonomia proposta nella presente relazione viene quindi applicata a ciascun caso e, a fini di chiarezza, è riportato uno schema che illustra come si è verificato l'attacco. Le informazioni contenute nelle sintesi si riferiscono alle informazioni disponibili al momento della redazione della presente relazione.

ELENCO DEGLI INCIDENTI ALLA CATENA DI APPROVVIGIONAMENTO:

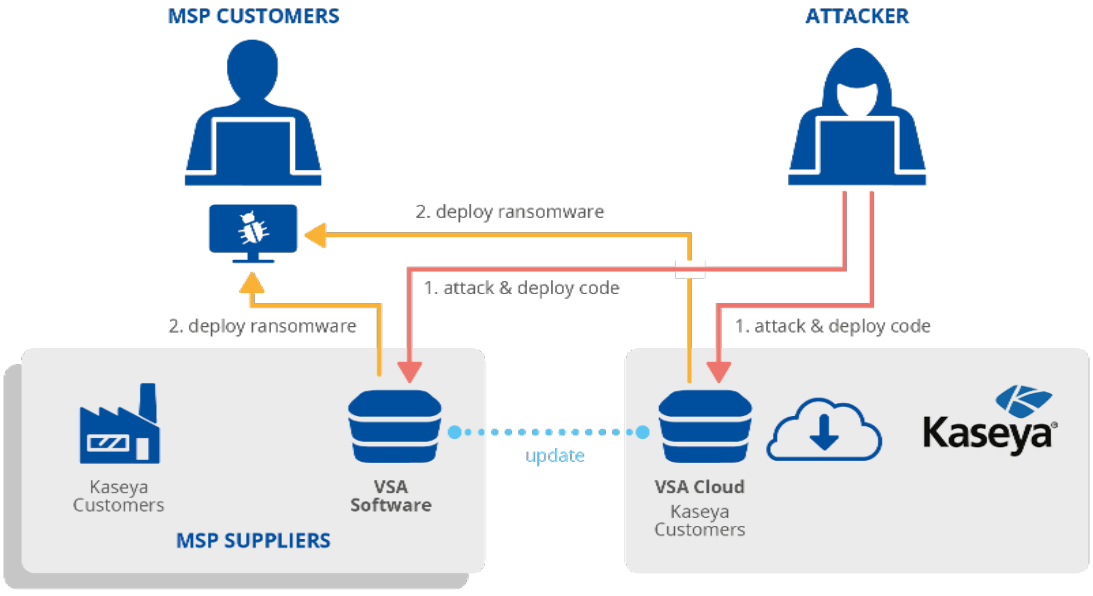
A.1 KASEYA. GESTIONE SOFTWARE INFORMATICO

Kaseya[60] è un fornitore di software specializzato in strumenti di monitoraggio e gestione a distanza. Offre software VSA (Virtual System/Server Administrator) e fornisce i propri server cloud. I provider di servizi gestiti (MSP) possono utilizzare il software VSA in sede oppure possono operare con licenza sui server cloud VSA di Kaseya. Gli MSP, a loro volta, offrono vari servizi IT ad altri client[61].

Nel luglio 2021, utenti malintenzionati hanno sfruttato una vulnerabilità a zero giorni nei sistemi di Kaseya (CVE-2021-30116[62]). Gli aggressori potrebbero eseguire a distanza i comandi sugli apparecchi VSA dei clienti di Kaseya. Kaseya è in grado di inviare aggiornamenti remoti a tutti i server VSA. Venerdì 2 luglio 2021, è stato distribuito un aggiornamento al sistema VSA dei client Kaseya che ha eseguito codice proveniente dagli autori degli attacchi. Questo codice dannoso ha, a sua volta, distribuito ransomware[63,64] ai clienti gestiti da tale VSA.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Sfruttamento della vulnerabilità del software	Software preesistente

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199], Infezione da malware	Dati, Ambito finanziario



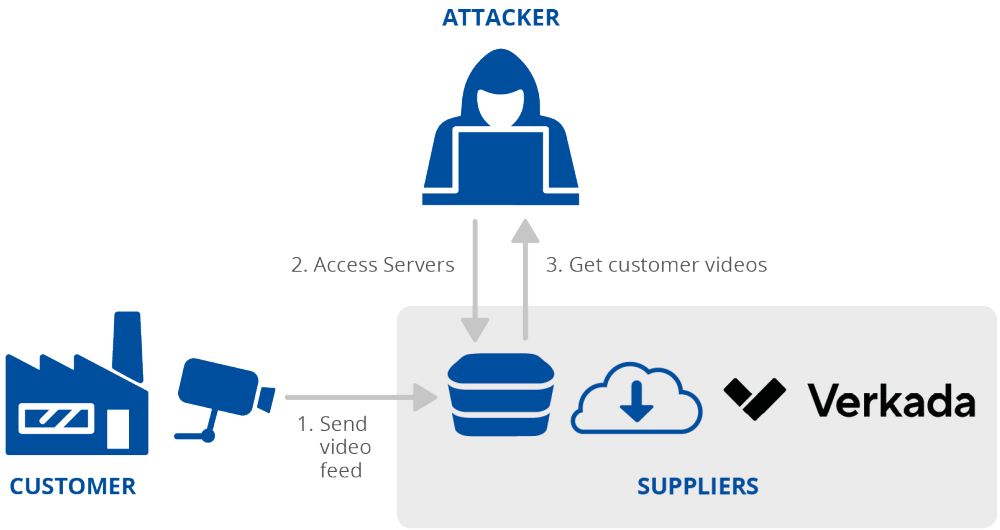
[60] IT Management Software - for MSPs and IT Teams, Kaseya, https://www.kaseya.com/. consultato il 03/12/2021.
[61] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. consultato il 03/12/2021.
[62] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116, consultato il 03/12/2021.
[63] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/, consultato il 03/12/2021.
[64] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. consultato il 03/12/2021.

A.2 VERKADA. SOLUZIONI DI SORVEGLIANZA DELLA SICUREZZA BASATE SUL CLOUD

Verkada offre soluzioni di sorveglianza della sicurezza basate sul cloud a più di 5 000 clienti[65]. Nel marzo 2021 è stato compromesso un server di produzione. Questa compromissione ha consentito agli autori dell'attacco di ottenere credenziali privilegiate per accedere alle telecamere di sicurezza installate nelle strutture dei clienti[66]. Le credenziali sarebbero state rinvenute "su Internet"[67]. Gli autori dell'attacco hanno avuto accesso ai video e alle immagini dei clienti da più di 150 000 videocamere situate in scuole, carceri, ospedali, stazioni di polizia e fabbriche di Tesla[68]. Un gruppo hacktivista ha rivendicato la responsabilità dell'attacco[69].

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
OSINT	Configurazioni Data

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199]	Dati



[65] The Future of Physical Security for the Enterprise: About Verkada, Verkada, https://www.verkada.com/about/. consultato il 03/12/2021.
[66] Verkada Security Update, Verkada, https://www.verkada.com/security-update/. consultato il 03/12/2021.
[67] Verkada Mass Hack, IPVM, https://ipvm.com/reports/verkada-hack. consultato il 03/12/2021.
[68] A hacker who exposed Verkada's surveillance camera snafu has been raided, The Verge, https://www.theverge.com/2021/3/12/22328344/tillie-kottmann-hacker-raid-switzerland-verkada-cameras. consultato il 03/12/2021.
[69] Tesla (TSLA), Cloudfare (NET) Breached in Verkada Security Camera Hack, Bloomberg, https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams. consultato il 03/12/2021.

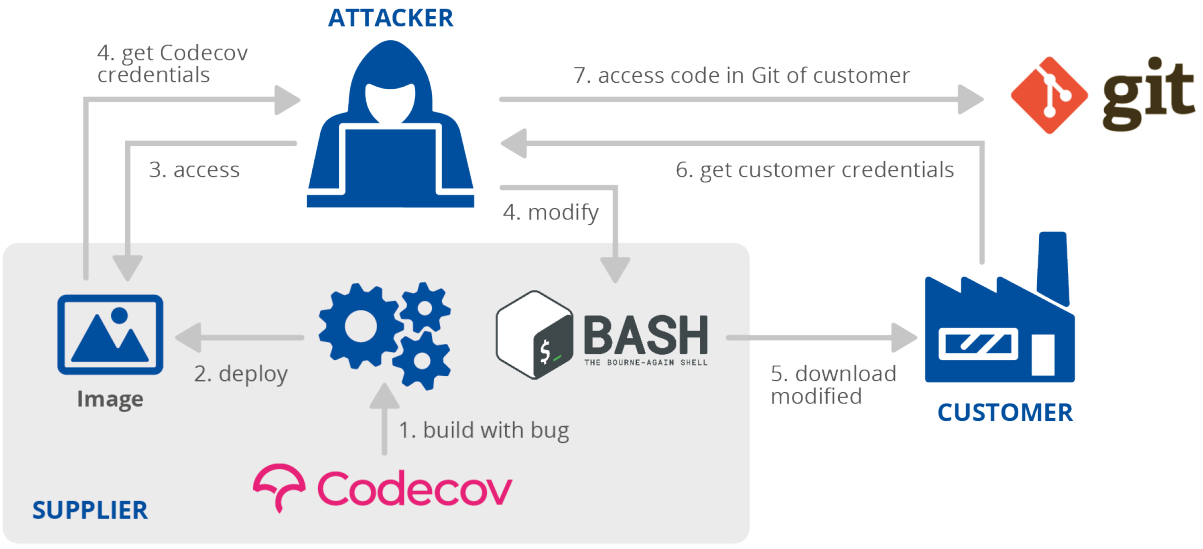
A.3 CODECOV. CODE MANAGEMENT AND AUDIT SOLUTIONS (GESTIONE DEI CODICI E SOLUZIONI DI AUDIT)

Codecov è un'azienda che fornisce software per la copertura di codice e strumenti di test. L'azienda fornisce strumenti ad altre aziende come IBM e Hewlett Packard Enterprise. Nell'aprile 2021, Codecov ha riferito che utenti malintenzionati hanno ottenuto alcune loro credenziali valide attraverso un'immagine Docker,a causa di un errore nella creazione di tali immagini Docker.

Gli autori dell'attacco hanno utilizzato le credenziali per compromettere uno "script di caricamento bash"[70] utilizzato dai clienti di Codecov. Quando i clienti scaricavano ed eseguivano lo script, gli autori degli attacchi riuscivano ad esfiltrare i dati dai clienti di Codecov, incluse informazioni riservate che hanno consentito loro di accedere ai beni dei clienti[71]. Più clienti Codecov hanno riferito che gli autori degli attacchi erano in grado di accedere al codice sorgente utilizzando informazioni rubate dalla violazione di Codecov[71]. Gli autori dell'attacco sono sconosciuti.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Sfruttamento della vulnerabilità della configurazione	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199]	Software



[70] Codecov supply chain attack breakdown, https://blog.gitguardian.com/codecov-supply-chain-breach/. consultato il 03/12/2021.

[71] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. consultato il 03/12/2021.

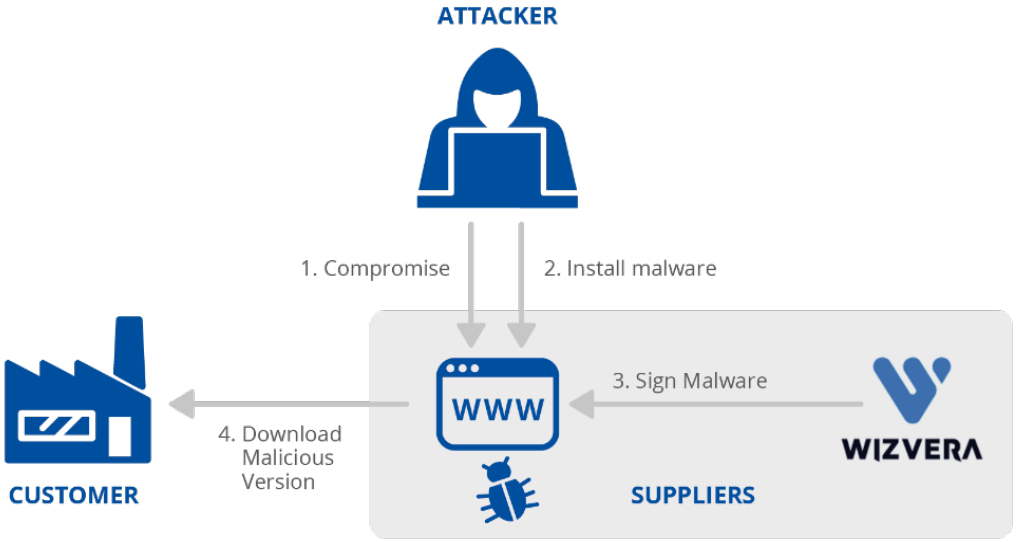
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.4 WIZVERA VERAPORT. PROGRAMMA DI INSTALLAZIONE DI INTEGRAZIONE

Wizvera è un'impresa che fornisce soluzioni per la verifica dell'identità, la gestione delle password e i certificati cloud[72]. Wizvera possiede un prodotto denominato VeraPort, per l'integrazione dell'installazione che consente agli utenti di installare il software di sicurezza richiesto dai datori di lavoro[73]. Nel novembre 2020, utenti malintenzionati hanno compromesso un sito Web legale supportato da VeraPort. Hanno sostituito la configurazione VeraPort nel sito Web compromesso per fornire software maligni invece del previsto software di sicurezza.

La configurazione è stata firmata digitalmente da Wizvera[73]. VeraPort verifica se il software scaricato abbia una firma digitale valida, ma non verifica chi ha rilasciato il certificato. Attraverso questo meccanismo, gli utenti della Corea del Sud che hanno effettuato l'accesso al sito Web compromesso hanno scaricato il software maligno. L'attacco è stato attribuito al gruppo APT Lazarus[73].

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Processi	Compromissione "by-drive" (T1189), Infezione da malware	Dati



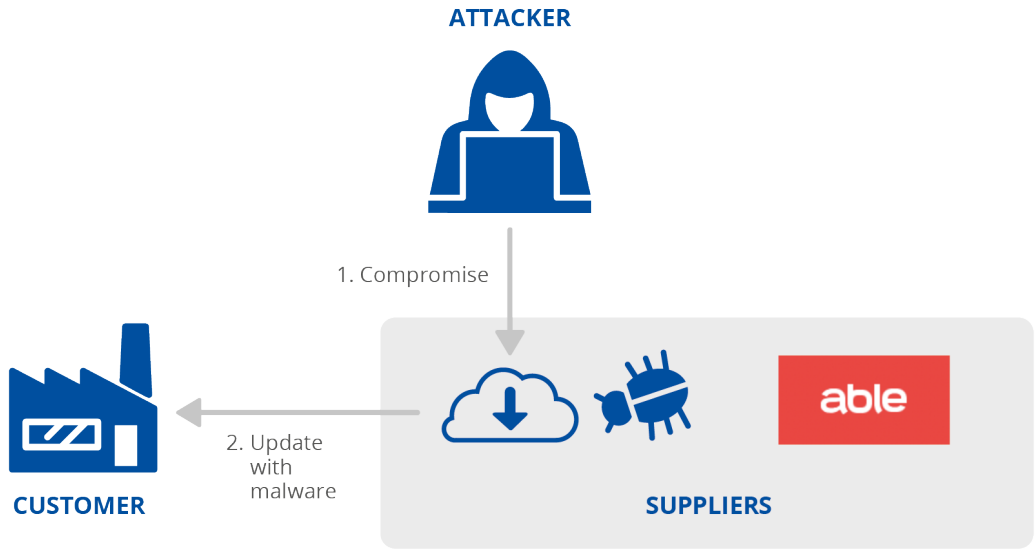
[72] Wizvera Company Profile & Funding, Crunchbase, https://www.crunchbase.com/organization/wizvera. consultato il 03/12/2021.
[73] Lazarus supply-chain attack in South Korea, WeLiveSecurity, https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/. Accessed consultato il 03/12/2021.

A.5 DESKTOP ABILE. SOFTWARE CHAT

Able è un'impresa con sede in Mongolia che fornisce soluzioni software alle agenzie governative e alle imprese della regione[74]. Nel giugno 2020 gli aggressori hanno effettuato l'accesso al backend di Able e compromesso il sistema che fornisce aggiornamenti software a tutti i clienti. Gli autori degli attacchi hanno aggiunto malware all'applicazione "Able Desktop" (un supplemento che fornisce messaggi istantanei al prodotto principale di Able)[75]. Sebbene non sia noto in che modo il fornitore è stato compromesso, gli aggressori sono riusciti a far installare software maligni agli utenti[75]. Il malware è stato poi utilizzato per ricavare informazioni dai dispositivi infetti dei clienti[75]. L'attacco è stato attribuito all'APT TA428.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199], Infezione da malware	Dati



[74] Able - Working online, Able, https://web.able.mn/, consultato il 03/12/2021.
[75] Operation StealthyTrident: corporate software under attack, WeLiveSecurity, https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/. consultato il 03/12/2021.

A.6 AISINO. SUITE DI SOFTWARE FISCALE INTELLIGENTE

Aisino Credit Information Company fornisce software per il pagamento delle imposte a clienti internazionali attraverso il suo dipartimento "Golden Tax", tra cui "Aisino Tax Software Suite". Nel giugno 2020, esperti hanno rivelato che il "Aisino Tax Software Suite" era compromesso dall'inclusione i software maligni[76]. Non è noto in che modo il software sia stato compromesso e quale fosse l'obiettivo dell'attacco[76]. L'attacco è stato rivolto alle imprese in Cina, dove il software fa parte di un programma nazionale[77]. Gli autori dell'attacco sono sconosciuti.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199], Infezione da malware	Tecnica sconosciuta

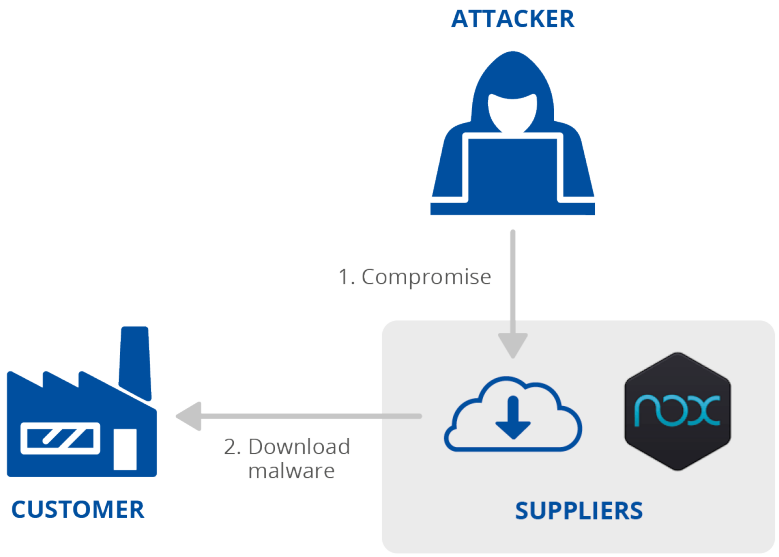
[76] The Golden Tax Department and Emergence of GoldenSpy Malware, Trustwave SpiderLabs, https://trustwave.azureedge.net/media/16929/the-golden-tax-department-and-emergence-of-goldenspy-malware.pdf. consultato il 03/12/2021.
[77] GoldenSpy Chapter 4: GoldenHelper Malware Embedded in Official Golden Tax Software, Trustwave, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/. consultato il 03/12/2021.

A.7 BIGNOX NOXPLAYER. EMULATORE ANDROID PER PC E MAC

BigNox è un'impresa che fornisce software di emulazione. Il principale prodotto, NoxPlayer, è un emulatore Android molto apprezzato per Windows e Mac[78]. Nel febbraio 2021, esperti hanno segnalato la compromissione dell'infrastruttura di NoxPlayer. Il rischio è la possibilità di abusare del meccanismo di aggiornamento dello strumento, fornendo software maligni, invece degli aggiornamenti sicuri[79].

Una volta distribuito il payload iniziale, gli autori degli attacchi potrebbero raccogliere informazioni sulle vittime e distribuire ulteriore malware a target specifici[79]. L'obiettivo degli autori degli attacchi sembra essere quello di acquisire la capacità di rilevare obiettivi specifici[79]. Gli autori dell'attacco sono sconosciuti.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Codice	Rapporto di fiducia [T1199], Infezione da malware	Persone, Dati

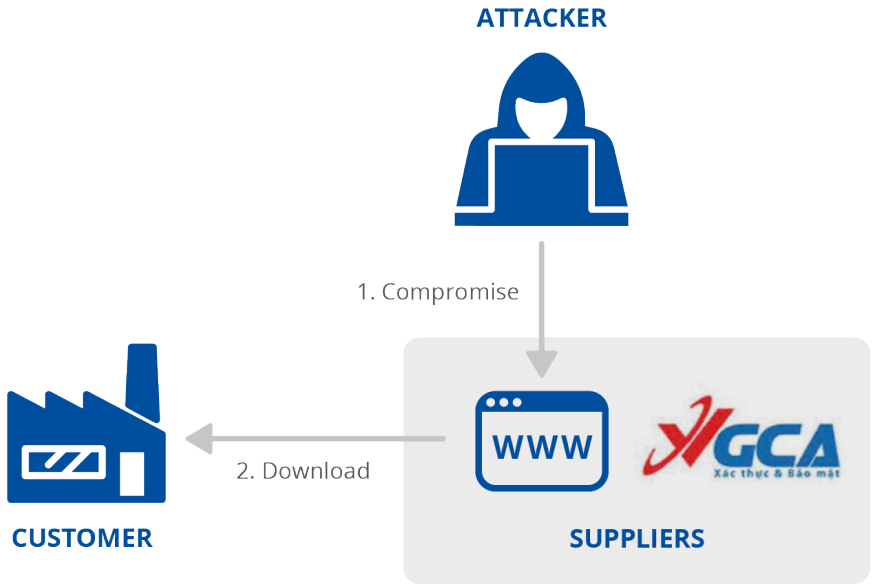


[78] NoxPlayer - Free Android Emulator on PC and Mac, BigNox, https://www.bignox.com/. consultato il 03/12/2021.
[79] Operation NightScout: Supply-chain attack targets online gaming in Asia, WeLiveSecurity, https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/. consultato il 03/12/2021.

A.8 AUTORITÀ DI CERTIFICAZIONE GOVERNATIVA DEL VIETNAM (VGCA)

L'autorità di certificazione governativa vietnamita (VGCA) fornisce certificati digitali e una serie di applicazioni che aiutano i cittadini e le imprese a firmare elettronicamente i documenti[80]. Nel dicembre 2020, esperti hanno riferito che il sito web dell'infrastruttura VGCA era stato compromesso per sostituire i binari legittimi con applicazioni con trojan[81]. L'obiettivo dell'attacco non è chiaro, ma gli esperti ritengono che possa far parte di un attacco più ampio[81]. Gli strumenti utilizzati indicano che gli autori potrebbero essere i gruppi APT (TA413, TA428)[82].

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Codice	Rapporto di fiducia [T1199], Infezione da malware	Persone



[80] Vietnam targeted in complex supply chain attack, ZDNet, https://www.zdnet.com/article/vietnam-targeted-in-complex-supply-chain-attack/. consultato il 03/12/2021.
[81] Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia, WeLiveSecurity, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/. consultato il 03/12/2021.
[82] Panda's New Arsenal: Part 3 Smanager, Hiroki Hada, https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager. consultato il 03/12/2021.

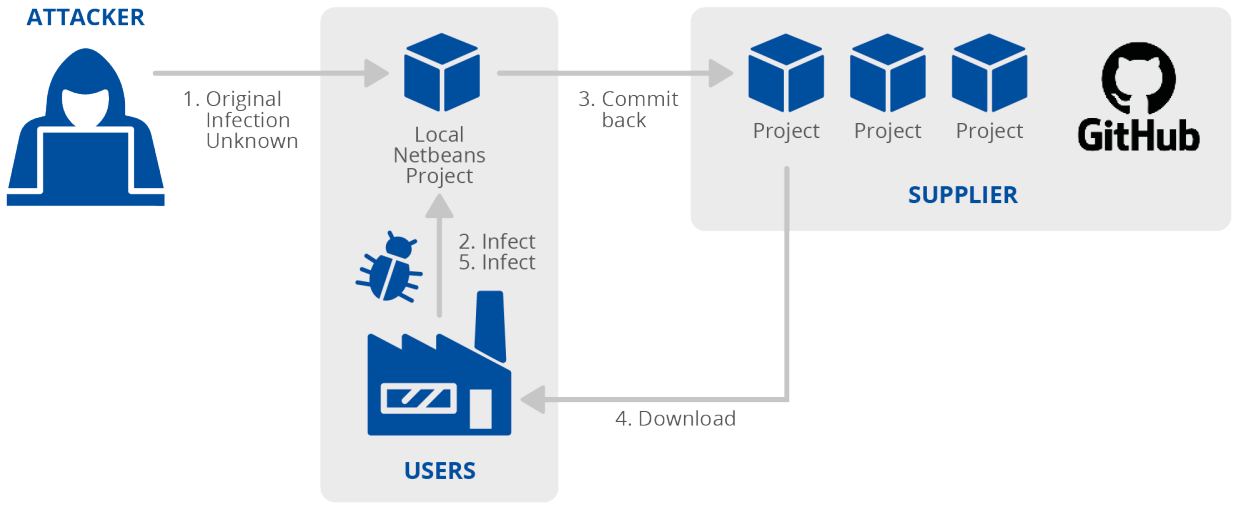
A.9 APACHE NETBEANS. PIATTAFORMA DI SVILUPPO

Netbeans è una piattaforma integrata di sviluppo Java di Apache. Nel maggio 2020, esperti hanno riferito che alcuni progetti Netbeans su GitHub contenevano malware senza che i proprietari ne fossero a conoscenza. Tutti coloro che scaricavano e utilizzavano questi progetti rischiavano di infettare con virus trojan tutti i progetti locali Netbeans, caricandoli su GitHub.

Gli utilizzatori sono stati infettati anche da un malware RAT[83,84]. L'obiettivo degli autori dell'attacco sembra essere la raccolta di informazioni proprietarie. Questo attacco sembra far parte di un attacco più ampio alla catena di approvvigionamento. In questo caso gli utenti sono sia il fornitore che le vittime. GitHub è l'unico mezzo di condivisione utilizzato. Gli autori dell'attacco sono sconosciuti.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Infezione da malware	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Infezione da malware	Il software, Dati

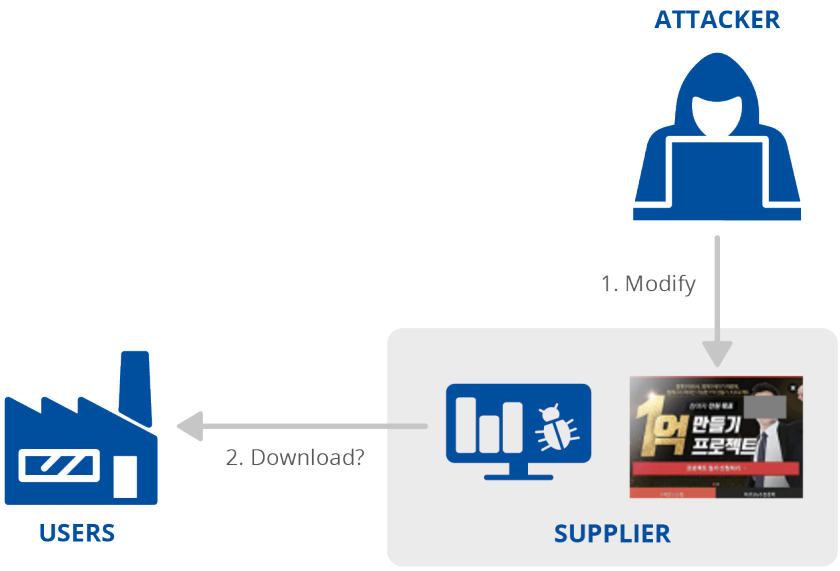


[83] The Octopus Scanner Malware: Attacking the open source supply chain, GitHub Security Lab, https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain/. consultato il 03/12/2021.
[84] Supply Chain Attack Event - Targeted Attacks on Java Projects in GitHub, NSFOCUS, https://nsfocusglobal.com/supply-chain-attack-event-targeted-attacks-on-java-projects-in-github/. consultato il 03/12/2021.

A.10 MESSENGER DI INVESTIMENTO PER AZIONI PRIVATE

Nel gennaio 2021, esperti hanno riferito che alcuni investitori azionari erano stati presi di mira dal gruppo Thallium APT, il che comprometteva un'applicazione di messaggistica ampiamente utilizzata per gli investimenti azionari[85]. Gli autori degli attacchi avevano utilizzato dei trojan sui programmi di installazione dell'applicazione di messaggistica per inserire malware[86]. Il malware è stato quindi utilizzato per spiare gli utenti infetti[87]. Non sono disponibili informazioni attendibili sull'attacco o sui metodi utilizzati.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Sconosciuto	Codice	Infezione da malware	Persone



[85] Thallium Hacker Targeted Users of Private Stock Investment Messenger, Cyware Alerts - Hacker News, https://cyware.com/news/thallium-hacker-targeted-users-of-private-stock-investment-messenger-ac33d20d. consultato il 05/12/2021

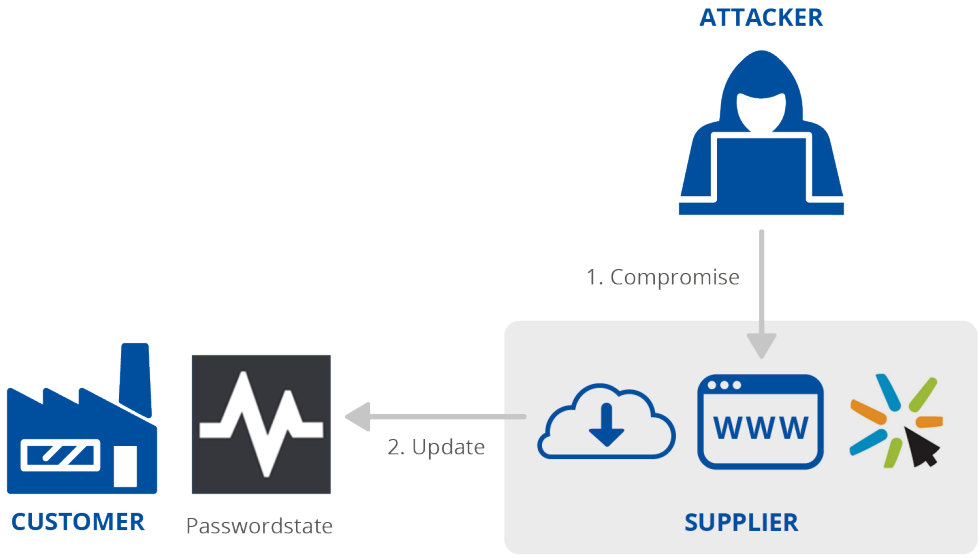
[86] Thallium Altered the Installer of a Stock Investment App, E Hacking News, https://www.ehackingnews.com/2021/01/thallium-altered-installer-of-stock.html. Consultato il 03/12/2021.

[87] Thallium organization exploits private equity investment messenger to launch software supply chain attack, ESTsecurity, https://blog.alyac.co.kr/3489. consultato il 05/12/2021.

A.11 CLICKSTUDIOS PASSWORDSTATE: SISTEMA DI GESTIONE DELLE PASSWORD

ClickStudios è un'impresa che fornisce soluzioni di gestione delle password aziendali[88]. Il loro prodotto principale è uno strumento denominato Passwordstate. Nell'aprile 2021 il meccanismo web dell'"upgrade director" di Passwordstate, utilizzato per aggiornare lo strumento, è stato compromesso[89], riorientando gli utenti verso il download di software maligni invece degli aggiornamenti previsti. Il software maligno installato è stato progettato per intercettare le informazioni provenienti dai sistemi compromessi[89, 90]. Gli autori dell'attacco sono sconosciuti.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Codice	Rapporto di fiducia [T1199], Infezione da malware	Dati



[88] Enterprise Password Management Software - Web based Server Password Manager, ClickStudios https://www.clickstudios.com.au/. consultato il 05/12/2021.
[89] ClickStudios PASSWORDSTATE Incident Management Advisory #01, ClickStudios, https://www.clickstudios.com.au/advisories/Incident_Management_Advisory-01-20210424.pdf. consultato il 05/12/2021.
[90] Moserpass supply chain, CSIS Security Group, https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/. consultato il 05/12/2021.

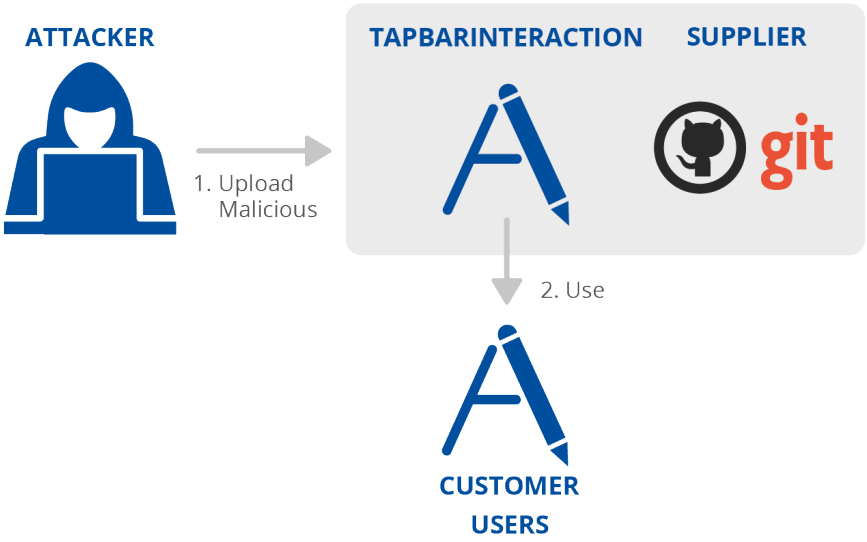
A.12 APPLE XCODE. AMBIENTE DI SVILUPPO INTEGRATO

Apple Xcode è un ambiente di sviluppo utilizzato per sviluppare le applicazioni OSX e iOS[91]. Nel marzo 2021, esperti hanno riferito che un singolo progetto doloso Xcode era stato utilizzato per infettare gli sviluppatori Xcode con una backdoor[92]. Il progetto Xcode dannoso era una copia di un progetto reale. Il progetto Xcode dannoso ha infettato l'utente sfruttando una debolezza in Xcode che consentiva agli autori degli attacchi di gestire automaticamente uno script al momento dell'avvio del progetto[92].

Non è stato possibile individuare gli autori dell'attacco e non è chiaro il tipo di attacco effettivamente subito dai clienti[93]. Inoltre, non è chiaro in che modo il progetto "trojanised Xcode" abbia raggiunto potenziali vittime o se le abbia effettivamente raggiunte.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Infezione da malware	Tecnica sconosciuta

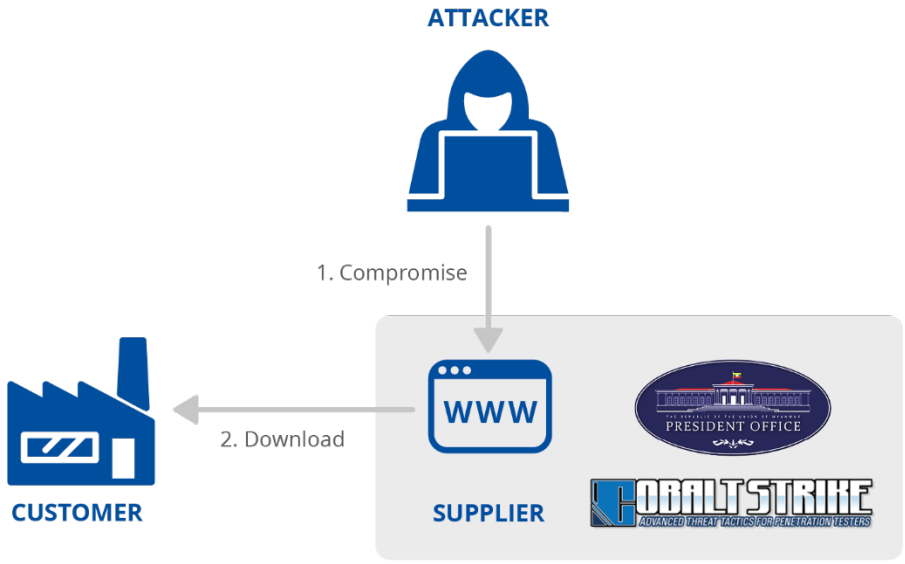


[91] Xcode 13 Overview, Apple Developer, https://developer.apple.com/xcode/. consultato il 05/12/2021.
[92] New macOS Malware XcodeSpy Targets Xcode Developers with EggShell Backdoor, SentinelLabs, https://labs.sentinelone.com/new-macos-malware-xcodespy-targets-xcode-developers-with-eggshell-backdoor/, consultato il 05/12/2021.
[93] XcodeSpy Mac Malware Targets Developers, SecureMac, https://www.securemac.com/news/xcodespy-mac-malware-targets-developers. consultato il 05/12/2021.

A.13 SITO DEL PRESIDENTE DEL MYANMAR

Nel giugno 2021 esperti hanno riferito che le risorse ospitate nel sito web presidenziale del Myanmar/della Birmania avevano subito un attacco trojan con inserimento di malware[94]. L'attacco non è stato ufficialmente attribuito a uno specifico gruppo APT[95], tuttavia sono state evidenziate analogie con il gruppo APT Mustang Panda[94,96].

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Codice	Phishing [T1566], Infezione da malware	Persone



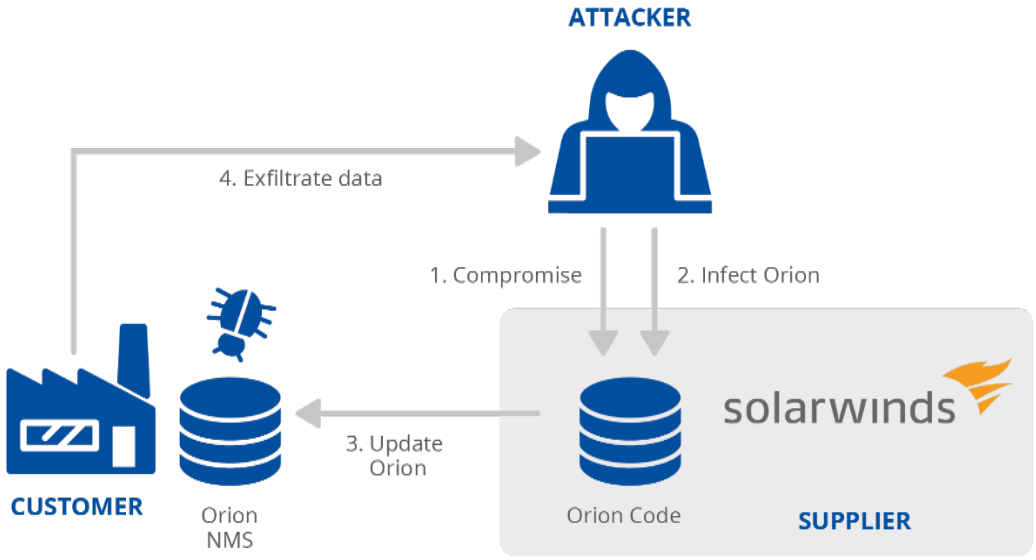
[94] "ESETresearch uncovered a supply chain attack on the Myanmar president office website", Twitter, https://twitter.com/ESETresearch/status/1400165767488970764. consultato il 05/12/2021.
[95] Backdoor malware found on the Myanmar president's website, again, The Record by Recorded Future, https://therecord.media/backdoor-malware-found-on-the-myanmar-presidents-website-again/. consultato il 05/12/2021.
[96] Cobalt Strike Beacons Being Hosted on Myanmar President's Website, Binary Defense, https://www.binarydefense.com/threat_watch/cobalt-strike-beacons-being-hosted-on-myanmar-presidents-website/. consultato il 05/12/2021.

A.14 SOLARWINDS ORION. GESTIONE IT E MONITORAGGIO REMOTO

SolarWinds è un'azienda che fornisce software di gestione e monitoraggio[97]. Orion è il prodotto del sistema di gestione della rete SolarWinds (NMS)[98]. Nel dicembre 2020 è stata riscontrata un compromessione in Orion. Da un'indagine approfondita è emerso che gli autori dell'attacco hanno avuto accesso alla rete SolarWinds, probabilmente sfruttando una vulnerabilità a zero giorni in un'applicazione o un dispositivo di terzi, un attacco di tipo "brute-force" o attraverso l'ingegneria sociale[99]. Attraverso la compromissione, gli autori degli attacchi hanno raccolto informazioni per un periodo di tempo prolungato.

Dopo la compromissione, un software maligno è stato inserito nel processo di costruzione di Orion[99,100]. Il software compromesso è stato poi scaricato ed eseguito direttamente dai clienti ed è stato utilizzato per raccogliere e rubare informazioni[101,102]. L'attacco è stato attribuito al gruppo APT29[103].

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Sfruttamento della vulnerabilità del software, Attacco "brute-force", Ingegneria sociale	Processi, Codice	Rapporto di fiducia [T1199], Infezione da malware	Dati



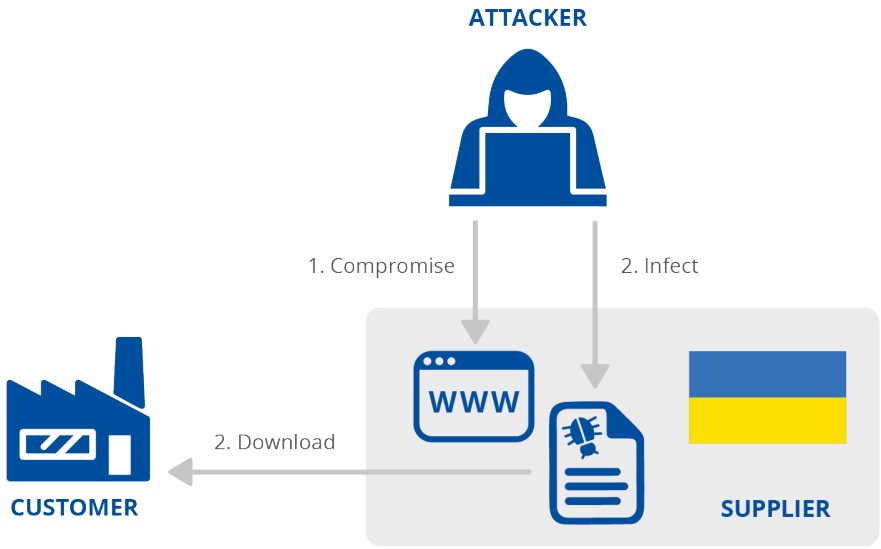
[97] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. consultato il 05/12/2021.
[98] Orion Platform, SolarWinds, https://www.solarwinds.com/solutions/orion. consultato il 05/12/2021.
[99] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. consultato il 05/12/2021.
[100] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. consultato il 05/12/2021.
[101] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, ireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. consultato il 05/12/2021.
[102] SUNBURST Additional Technical Details, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html. consultato il 05/12/2021.
[103] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. consultato il 05/12/2021.

A.15 UCRAINA SEI EB. SISTEMA DI INTERAZIONE ELETTRONICA DEGLI ORGANI ESECUTIVI

Il governo e le autorità pubbliche ucraine utilizzano il sistema di interazione elettronica degli organi esecutivi (SEI EB), un portale web concepito per lo scambio di documenti[104]. Nel febbraio 2021 è stato segnalato che il sistema era stato compromesso da utenti pericolosi che sono riusciti a caricare documenti dannosi nel portale[105]. I documenti dannosi potrebbero successivamente infettare gli utenti con malware concepiti per raccogliere e rubare informazioni. L'attacco è stato attribuito a vari gruppi APT, ma non a un gruppo particolare[104].

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Infezione da malware	Persone, Dati



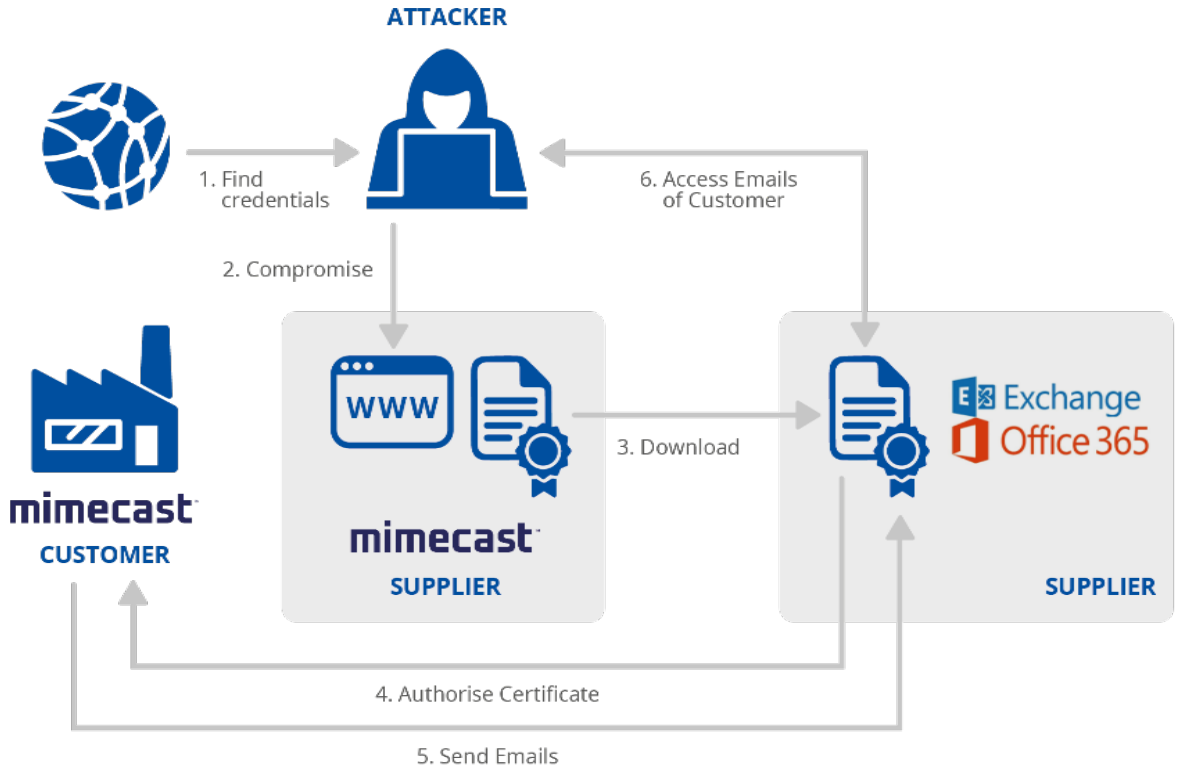
[104] Russian hackers aim cyber attack on Ukrainian government agencies, Teiss News, https://www.teiss.co.uk/russian-hackers-targeting-ukrainian-government-agencies/. consultato il 05/12/2021.
[105] The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies, National Security and Defense Council of Ukraine, https://www.rnbo.gov.ua/en/Diialnist/4823.html. consultato il 05/12/2021.

A.16 MIMECAST. SERVIZI DI CIBERSICUREZZA CLOUD

Mimecast è un fornitore di servizi di cibersicurezza basati sul cloud[106]. Tra i servizi forniti, Mimecast offre servizi di protezione della posta elettronica, che richiedono ai clienti di connettersi in modo sicuro ai server Mimecast per utilizzare i propri account Microsoft 365. Nel gennaio 2021 è stato scoperto che utenti malintenzionati avevano compromesso Mimecast (tramite il fornitore SolarWinds). La compromissione ha fatto sì che tali utenti malintenzionati ottenessero un certificato rilasciato da Mimecast, utilizzato dai clienti per accedere ai servizi Microsoft 365; gli autori degli attacchi hanno potuto così intercettare le connessioni di rete e connettersi agli account Microsoft 365 per rubare informazioni[107,108]. L'attacco è stato attribuito al gruppo APT29[109]. La compromissione del fornitore è stata collegata a SolarWinds, ma non vi sono informazioni concrete su come sia avvenuta.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Dati

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199]	Dati



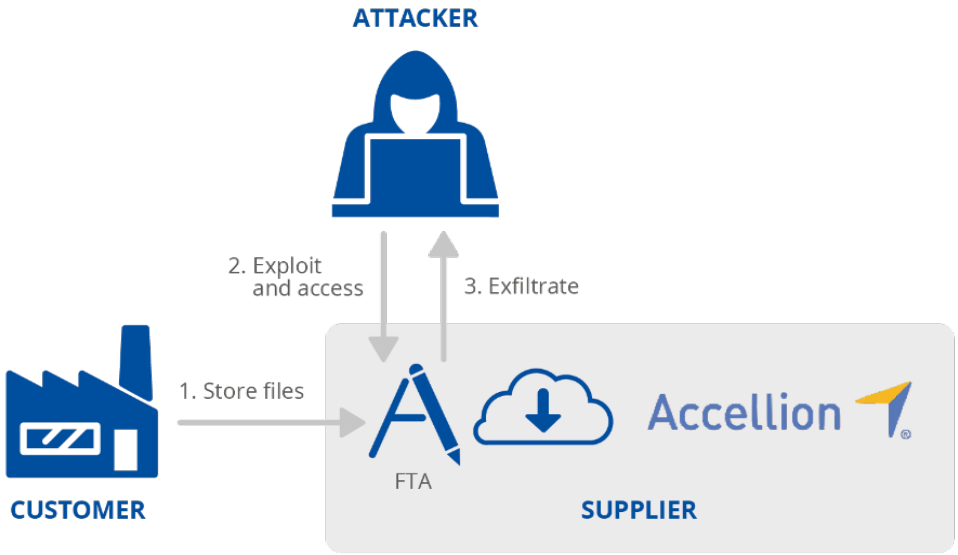
[106] Our Company, Mimecast, https://www.mimecast.com/company/. consultato il 05/12/2021.
[107] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. consultato il 05/12/2021.
[108] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. consultato il 05/12/2021.
[109] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. consultato il 05/12/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.17 ACCELLION. SOFTWARE FTA (FILE TRANSFER APPLIANCE)

Accellion è una società che fornisce software di sicurezza alle imprese, in particolare applicazioni per la condivisione sicura dei file e la collaborazione[110]. Nel dicembre 2020 Accellion ha riferito che utenti malintenzionati sfruttavano vulnerabilità multiple a zero giorni presenti nel software FTA (File Transfer Appliance) per accedere ai registri dei clienti[111][112] ed esfiltrarli utilizzando una WebShell. Molte imprese colpite da tali vulnerabilità hanno subito estorsioni da parte degli autori degli attacchi, che minacciavano di pubblicare i file rubati. L'attacco è stato attribuito a un gruppo di criminalità informatica noto come UNC2546[112].

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Sfruttamento della vulnerabilità del software	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199]	Dati



[110] About Accellion, Accellion, https://www.accellion.com/company/. consultato il 05/12/2021.
[111] File Transfer Appliance (FTA) Security Assessment, Accellion, https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf. consultato il 05/12/2021.
[112] Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion, FireEye Inc, https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html. consultato il 05/12/2021.

A.18 SISTEMA DI ASSISTENZA PASSEGGERI SITA

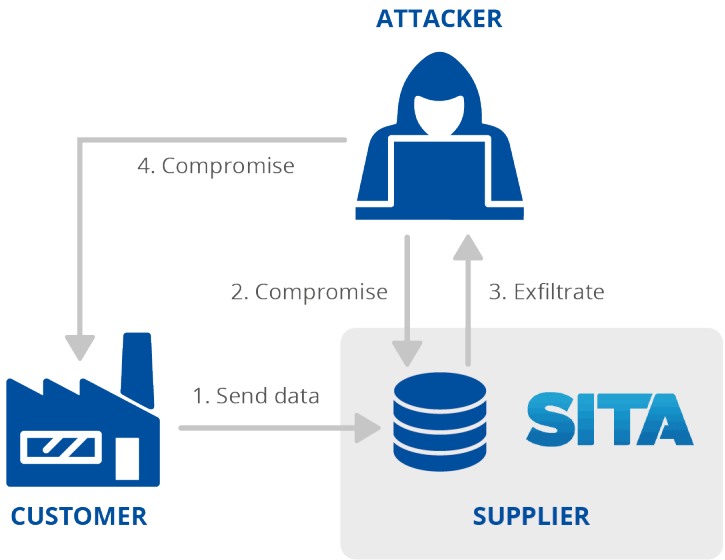
SITA è un'azienda specializzata in tecnologia di informazione aerea e informazioni di trasporto[113]. Il sistema di servizio passeggeri SITA è utilizzato per fornire alle compagnie aeree informazioni sui passeggeri al momento dell'imbarco, compreso il rischio che i passeggeri potrebbero rappresentare per un paese[114]. Nel marzo 2021, è stato rivelato che utenti malintenzionati avevano compromesso i server SITA per ottenere l'accesso ai dati dei passeggeri dai clienti di SITA. Alcuni clienti di SITA hanno segnalato anche violazioni dei dati, come Air India, Singapore Airlines e Malaysia Airlines.

A seguito di segnalazioni di dati trapelati su Internet, Air India ha anche riferito che le sue reti erano state compromesse e i dati rubati. La compromissione delle reti interne di Air India era presumibilmente legata all'incidente SITA, perché una società di sicurezza ha scoperto che il nome di un computer interno di Air India era "SITASERVER4".

Ad oggi, non è ancora noto come gli autori degli attacchi abbiano ottenuto l'accesso ai server SITA e non è noto come abbiano avuto accesso a Air India o se vi siano effettivamente riusciti. L'attacco interno alle reti di Air India è stato attribuito al gruppo APT41[115].

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Dati

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Dati personali



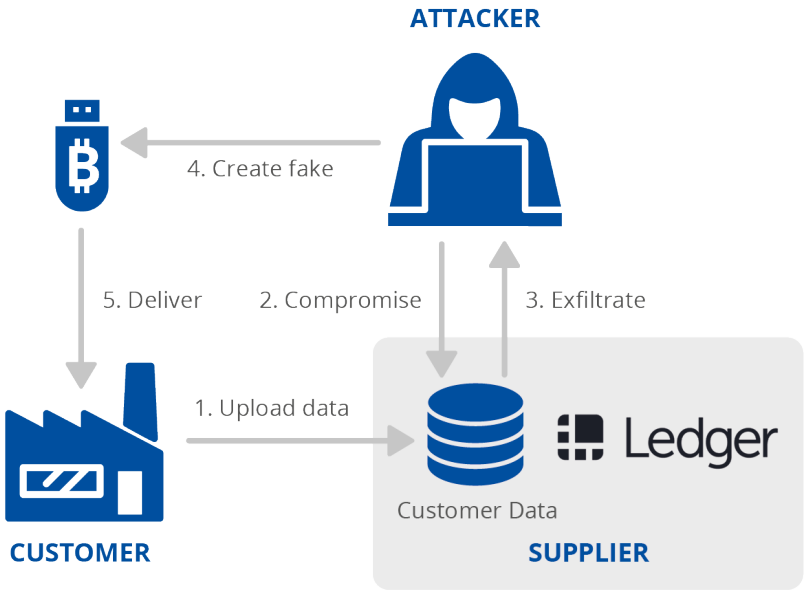
[113] About us, SITA, https://www.sita.aero/about-us/. consultato il 05/12/2021.
[114] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. consultato il 05/12/2021.
[115] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. consultato il 05/12/2021.

A.19 LEDGER. PORTAFOGLI HARDWARE

Ledger è un'impresa che fornisce tecnologia hardware per portafogli per criptovalute[116]. Nel luglio 2020, gli aggressori hanno ottenuto valide credenziali per accedere alla banca dati di commercio elettronico Ledger [117]. Il modo in cui gli aggressori hanno avuto accesso a queste credenziali non è noto. I dati rubati sono stati resi pubblici in un forum online[118].

Gli autori degli attacchi hanno utilizzato i dati rubati per phishing e estorsione online degli utenti[119,120]e per rubare denaro degli utenti attraverso un attacco fisico, dopo aver fornito agli utenti portafogli Ledger contraffatti che, se collegati a un computer che richiede le chiavi di sicurezza, potrebbero infettare il computer con malware e rinviare le informazioni rubate agli autori degli attacchi[121]. Gli autori dell'attacco sono sconosciuti.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Dati	Rapporto di fiducia [T1199], Phishing [T1566], Contraffazione	Ambito finanziario

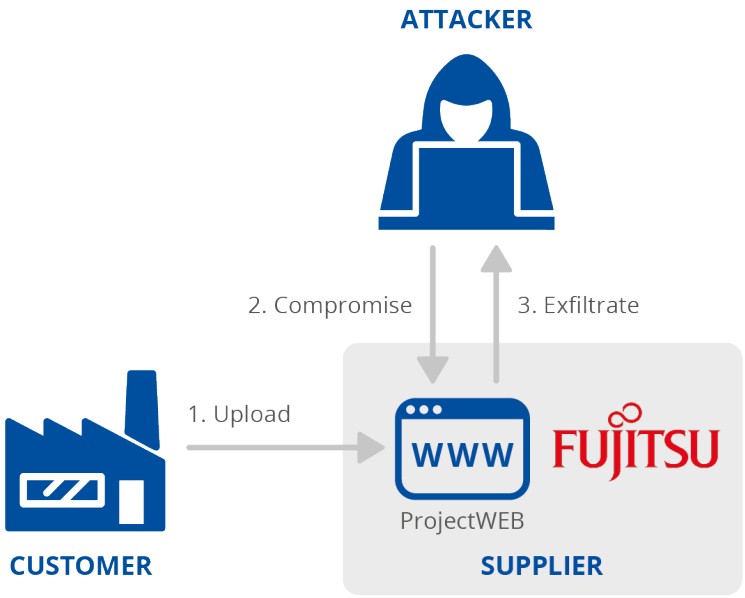


[116] Hardware Wallet, Ledger, https://www.ledger.com/. consultato il 05/12/2021.
[117] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership | Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. consultato il 05/12/2021.
[118] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. consultato il 05/12/2021.
[119] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. consultato il 05/12/2021.
[120] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html. consultato il 05/12/2021.
[121] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. consultato il 05/12/2021.

A.20 PROGETTO FUJITSU WEB. SOFTWARE PER LA COLLABORAZIONE E LA GESTIONE DEI PROGETTI

Fujitsu ProjectWEB è un software basato su cloud utilizzato dalle imprese per la collaborazione online, la gestione di software e la condivisione di file[122]. Lo strumento è popolare tra le agenzie governative giapponesi. Nel maggio 2021, utenti malintenzionati hanno ottenuto l'accesso ai dati del governo giapponese[123] dopo aver sfruttato le debolezze delle installazioni ProjectWEB[122,124]. A causa della posizione dei server compromessi, anche i dati del controllo del traffico aereo giapponese sono stati rubati nell'attacco[122,125]. Gli autori dell'attacco sono sconosciuti.

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Tecnica sconosciuta	Codice, dati	Tecnica sconosciuta	Dati



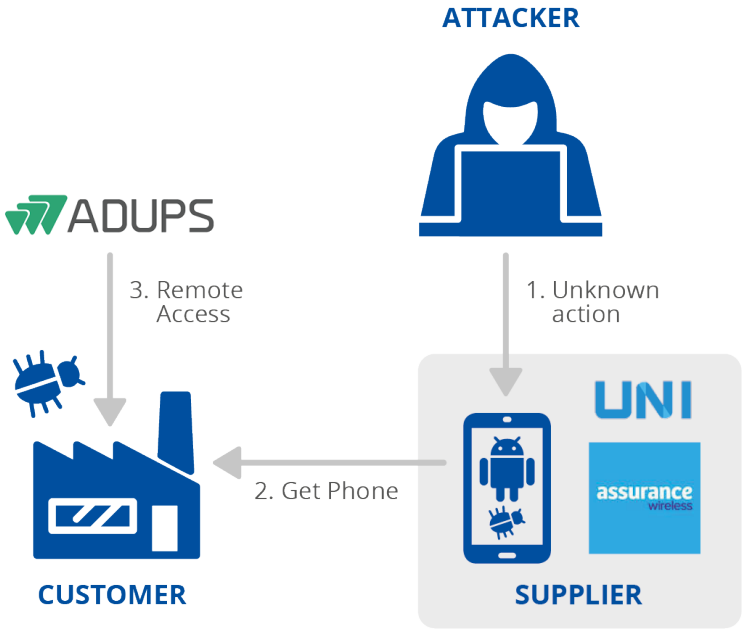
[122] Japanese government agencies suffered breaches after ProjectWEB hack, Teiss News, https://www.teiss.co.uk/japanese-government-agencies-suffered-breaches-following-fujitsus-projectweb-hack/. consultato il 05/12/2021.
[123] Japanese government agencies suffer data breaches after Fujitsu hack, Bleeping Computer, https://www.bleepingcomputer.com/news/security/japanese-government-agencies-suffer-data-breaches-after-fujitsu-hack/. consultato il 05/12/2021.
[124] Data theft via Fujitsu ProjectWEB, INCIBE-CERT, https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/data-theft-fujitsu-projectweb. consultato il 05/12/2021.
[125] Fujitsu pulls ProjectWEB tool offline after apparent supply chain attack sees Japanese infosec agency data stolen, The Register, https://www.theregister.com/2021/05/27/fujitsu_projectweb_supply_chain_attack/. consultato il 05/12/2021.

A.21 TELEFONI CELLULARI UNIMAX COMMUNICATIONS

Unimax, nota anche come UMX, fornisce dispositivi mobili a basso costo. I clienti dei telefoni UMX comprendono persone che ricevono i loro telefoni attraverso il programma di assistenza Lifeline del governo degli Stati Uniti[126]. Nel gennaio 2020, esperti hanno riferito che i dispositivi mobili erano dotati di malware preinstallati non rimovibili progettati per spiare gli utenti[127,128]. Non è stato possibile rimuovere il malware nemmeno con un sistema rigido. Un altro produttore di telefonia mobile che aveva rilevato il malware precaricato, Transsion, ha accusato un fornitore non identificato della catena di approvvigionamento[126]. Gli autori dell'attacco sono sconosciuti[126].

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Tecnica sconosciuta	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199], Infezione da malware	Persone



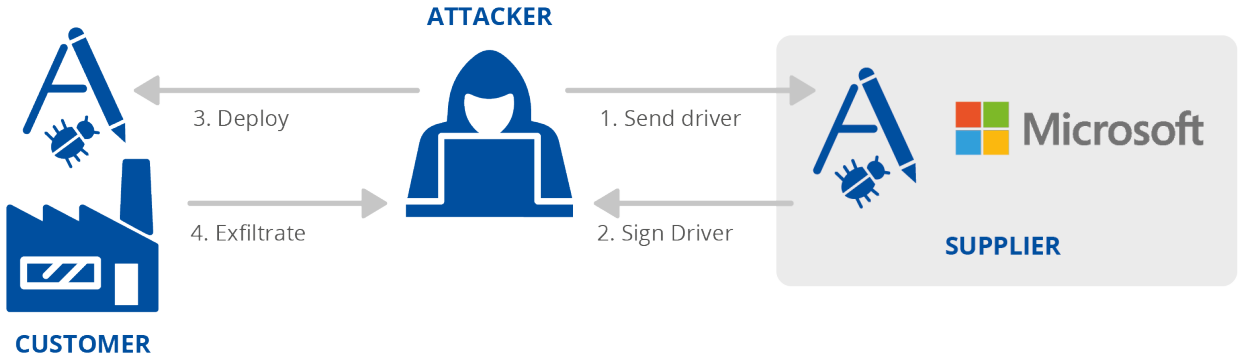
[126] Chinese Cell Phones Ship Preloaded with Malware, BlueVoyant, https://www.bluevoyant.com/blog/chinese-cell-phone-malware/. consultato il 05/12/2021.
[127] UMX Phone: US-funded Gov Phones come pre-installed with malicious apps, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/. consultato il 05/12/2021.
[128] We found yet another phone with pre-installed malware via the Lifeline Assistance program, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/07/we-found-yet-another-phone-with-pre-installed-malware-via-the-lifeline-assistance-program/. consultato il 05/12/2021.

A.22 MICROSOFT WINDOWS. PROGRAMMA DI COMPATIBILITÀ HARDWARE

Nel giugno 2021 è stato rivelato che utenti malintenzionati hanno abusato dei processi di firma dei codici utilizzati da Microsoft per convalidare i driver di terzi, infiltrarsi e distribuire un malware rootkit[129]. Attraverso la convalida della firma, sarebbe stato possibile installare il malware nei sistemi degli utenti[130]. L'attacco sembra aver colpito il settore del gioco d'azzardo in Cina[129]. Gli autori dell'attacco sono sconosciuti.

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Ingegneria sociale	Processi

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Rapporto di fiducia [T1199]	Dati



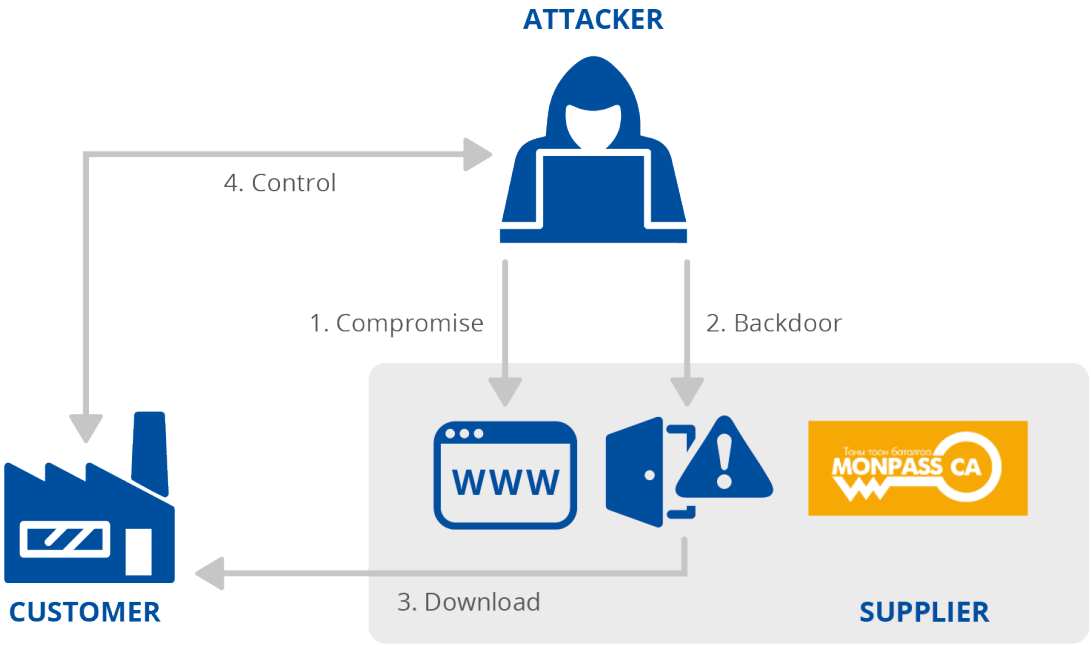
[129] Microsoft admits to signing rootkit malware in supply-chain fiasco, Bleeping Computer, https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/. consultato il 05/12/2021.
[130] Microsoft signed a malicious Netfilter rootkit, G DATA, https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit. consultato il 05/12/2021.

A.23 AUTORITÀ DI CERTIFICAZIONE MONPASS

MonPass è il principale ente di certificazione della Mongolia. Nel febbraio 2021, il suo sito web è stato compromesso e almeno un programma di installazione binario è stato rinviato con un binary Cobalt Strike[131]. Il sito web è stato ripetutamente compromesso e sono state trovate diverse Webells e backdoor[132]. Il codice dannoso è stato scaricato dai visitatori sul sito web di MonPass, che ha eseguito il malware al momento del download. Almeno un cliente è noto per essere stato infettato, secondo quanto riscontrato con Avast Software[131].

FORNITORE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento
Sfruttamento della vulnerabilità del software	Codice

CLIENTE	
Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Compromissione "by-drive" (T1189), Infezione da malware	Tecnica sconosciuta

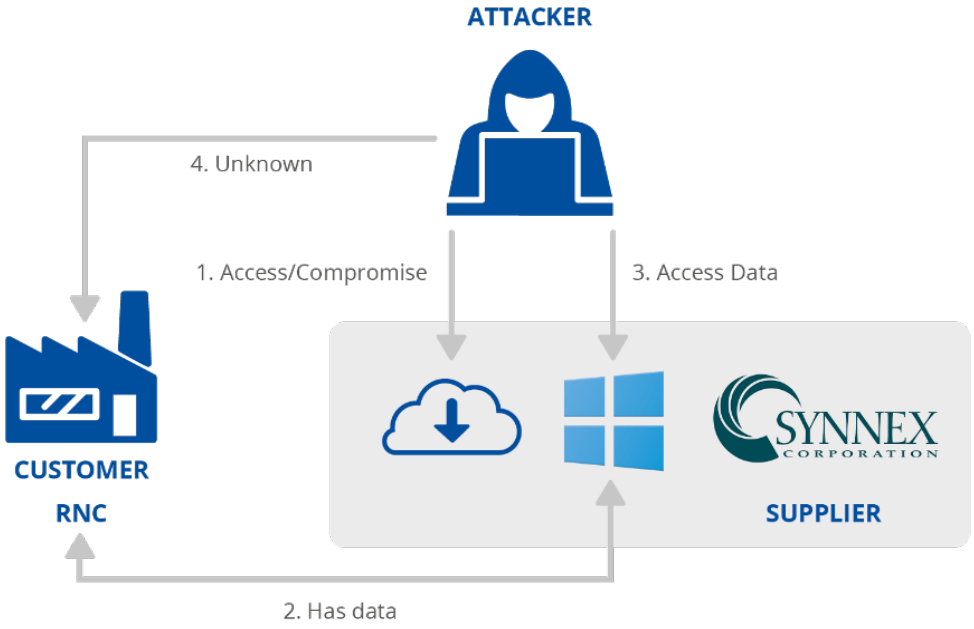


[131] Backdoored Client from Mongolian CA MonPass, Avast Threat Labs, https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/. Consultato il 03/12/2021.
[132] Mongolian Certificate Authority Hacked to Distribute Backdoored CA Software, The Hacker News, https://thehackernews.com/2021/07/mongolian-certificate-authority-hacked.html. consultato il 05/12/2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.24 SYNNEX IT DESIGN-TO-DISTRIBUTION COMPANY

Synnex è un distributore di tecnologia e integratore. Nel luglio 2021, i suoi sistemi sono stati violati[133]. Synnex ha ammesso che gli attacchi potrebbero essere stati collegati ai recenti attacchi della MSP di Kaseya[134]. Gli autori degli attacchi utilizzavano Synnex per accedere alle applicazioni dei clienti nell'ambiente cloud Microsoft. Tali domande comprendevano il comitato nazionale del Partito repubblicano degli Stati Uniti (RNC), che ha riferito di essere stato violato tramite Synnex[135].

FORNITORE		CLIENTE	
Tecniche di attacco utilizzate per compromettere la catena di approvvigionamento	Beni dei fornitori interessate dall'attacco alla catena di approvvigionamento	Tecniche di attacco utilizzate per compromettere il cliente	Beni di clienti oggetto dell'attacco della catena di approvvigionamento
Sfruttamento della vulnerabilità del software	Codice	Compromissione "by-drive" (T1189), Infezione da malware	Tecnica sconosciuta



[133] Mega-distie SYNNEX attacked and Microsoft cloud accounts it tends tampered, The Register, https://www.theregister.com/2021/07/07/synnex_rnc_microsoft_attack/. Consultato il 03/12/2021.
[134] SYNNEX Responds to Recent Cybersecurity Attacks and Media Mentions, SYNNEX Corporation, https://ir.synnex.com/news/press-release-details/2021/SYNNEX-Responds-to-Recent-Cybersecurity-Attacks-and-Media-Mentions/default.aspx. consultato il 03/12/2021.
[135] Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit, The Washington Post, https://www.washingtonpost.com/business/on-small-business/russia-cozy-bear-breached-gop-as-ransomware-attack-hit/2021/07/06/3e9e200a-de9b-11eb-a27f-8b294930e95b_story.html. consultato il 03/12/2021.

TP-05-21-171-IT-N

INFORMAZIONI SULL'ENISA

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento dell'UE sulla cibersicurezza, l'ENISA contribuisce alla politica dell'UE in materia di sicurezza nel settore informatico, migliora l'affidabilità dei prodotti, dei servizi e dei processi TIC con programmi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sul suo lavoro sono disponibili al seguente indirizzo: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-509-8
DOI: