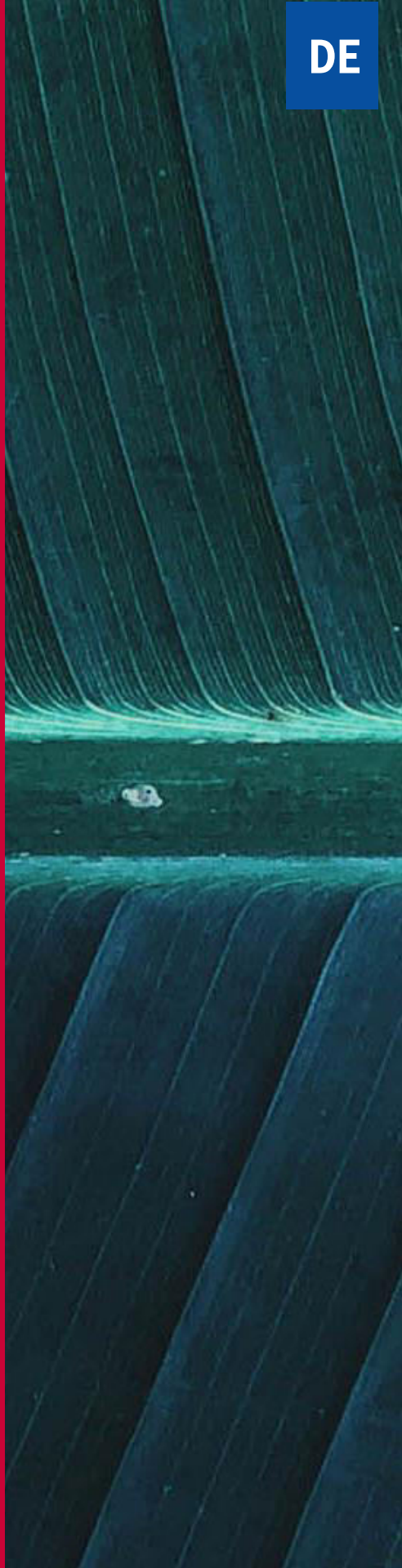
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE



Von Januar 2019 bis April 2020

S p a m

ENISA Threat Landscape

Überblick

Die erste Spam-Nachricht wurde 1978 von einem Marketingmanager über ARPANET an 393 Personen gesendet. Es war eine Werbekampagne für ein neues Produkt des Unternehmens Digital Equipment Corporation, für das er arbeitete. Für die ersten 393 von Spam betroffenen Personen war es genauso ärgerlich wie heute, unabhängig von der Neuheit der Idee.[1] Das Empfangen von Spam ist eine Unannehmlichkeit, kann aber auch einem böswilligen Akteur die Möglichkeit bieten, personenbezogene Informationen zu stehlen oder Malware zu installieren.[2] Spam besteht aus dem Versenden unerwünschter Nachrichten in großen Mengen. Es wird als Cybersicherheitsbedrohung angesehen, wenn es als Angriffsvektor zum Verteilen oder Aktivieren anderer Bedrohungen verwendet wird.

Ein weiterer bemerkenswerter Aspekt ist, wie Spam manchmal mit einer Phishing-Kampagne verwechselt oder falsch klassifiziert werden kann. Der Hauptunterschied zwischen beiden besteht darin, dass Phishing eine gezielte Aktion ist, bei der Social-Engineering-Taktiken eingesetzt werden, um die Daten der Benutzer zu stehlen. Im Gegensatz dazu ist Spam eine Taktik zum Senden unerwünschter E-Mails an eine Massenliste. Phishing-Kampagnen können Spam-Taktiken verwenden, um Nachrichten zu verbreiten, während Spam den Benutzer mit einer gefährdeten Website verknüpfen kann, um Malware zu installieren und personenbezogene Daten zu stehlen.

In den letzten 41 Jahren haben Spam-Kampagnen viele beliebte globale soziale und sportliche Ereignisse genutzt, darunter das UEFA Europa League-Finale und die US Open. Trotz allem ist dies nichts im Vergleich zu der Spam-Aktivität, die dieses Jahr mit der COVID-19-Pandemie beobachtet wurde.[8]

Erkenntnisse

85 % aller im April 2019 ausgetauschten E-Mails waren Spam, ein 15-Monats-Hoch[1]

14 Millionen Spam-E-Mails wurden im Zusammenhang mit Sextortierung beobachtet[23]

58,3 % der E-Mail-Konten im Bergbau waren Spam[17]

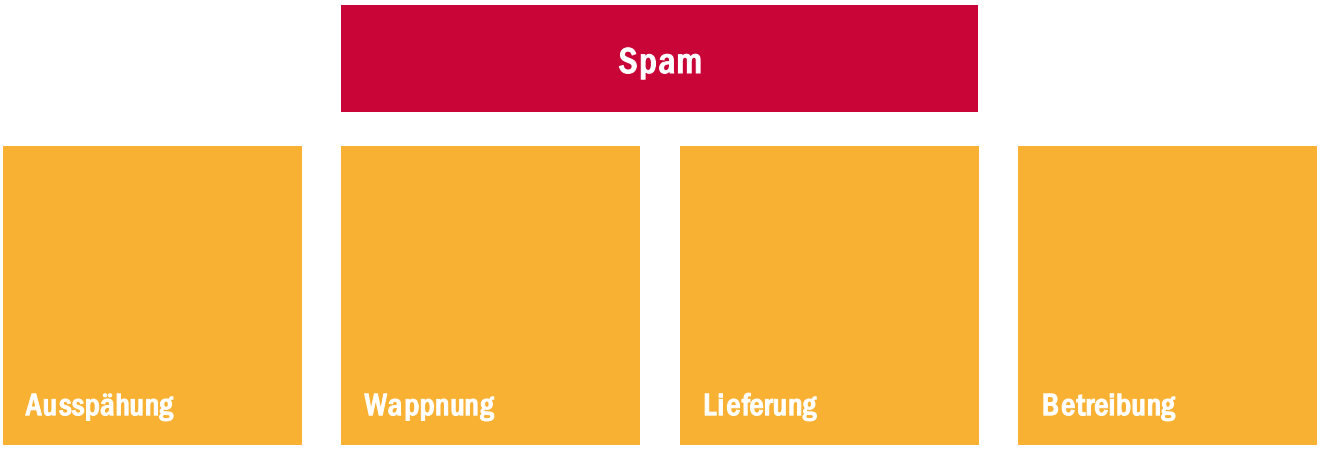
10 % aller Spam-Erkennungen richteten sich gegen deutsche E-Mail-Konten[2,3]

13 % der Datenschutzverletzungen wurden von bösartigem Spam verursacht[16]

83 % der Unternehmen waren nicht vor E-Mail-basierten Markenimitationen geschützt[20]

42 % oder Chief Information Security Officer (CISO) befassten sich mit mindestens einem durch Spam verursachten Sicherheitsvorfall[1]

Kill chain



Schritt des Angriffs-Workflows

Umfang des Zwecks

Installation

Command & Control

Zielführende Maßnahmen

Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

WEITERE INFORMATIONEN

Beschreibung

_Alter Kopf auf jungen Schultern

Nach 41 Jahren bleibt Spam eine bemerkenswerte Sicherheitsbedrohung, trotz anderer Bedrohungen, die viel effektiver sind. Im Berichtszeitraum tauchten jedoch erneut neue Zielgruppen, neue Mittel und neue Beute in Spam-Kampagnen auf. Im August 2019 zielten Spam-E-Mails beispielsweise auf mehrere Konten ab und ermutigten ihre Besitzer, nicht nur einen Scan ihrer Identität, sondern auch ein Selfie zu teilen, um ein kostenloses Smartphone-Gerät zu „gewinnen". In einer anderen Spam-Kampagne wurden Benutzer gebeten, ein persönliches Foto zu senden. Die Zielgruppe der Spammer wurde dann um die vom Benutzer verwendete E-Mail-Adresse erweitert, um Pay-TV- oder Live-Übertragungsdienste zu aktivieren. Diese Konten wurden mit gefälschten Nachrichten zum Ablauf oder zur Erneuerung der Lizenz gespammt. Die Benutzer wurden gebeten, zu antworten und ihre Bankkontodaten und persönlichen Daten einzugeben, um ihre Registrierung zu erneuern.[2]

_Spam zur Bereitstellung von Malware, Ransomware und RAS-Trojanern

Im August 2019 wurden Spam-E-Mails mit schädlichen ISO-Disk-Image-Dateien verwendet, um die LokiBot-Malware zu verbreiten und den RAT FlawedAmmyy (remote access trojan) zu löschen. Spamming wurde auch verwendet, um den TrickBot-Trojaner, den Negasteal-Trojaner (auch als Agent Tesla bekannt), die Ave Maria-RAT (auch als Warzone bekannt) und die seit 2018 berüchtigte Pawload-Makro-Malware zu verbreiten. Mehrere Ransomware Familien wurden ebenfalls durch Spamnachrichten verbreitet, wie Dharma, Crysis und Ryuk, von denen berichtet wurde, dass sie im Berichtsjahr sehr aktiv waren.[15,21]

_Spam SMS

In diesem Jahr wurde ein SMS-Spam Vorgang durchgeführt, bei dem mehr als 80 Millionen personenbezogene Daten von Benutzern offengelegt wurden. Eine große Anzahl von Telefonnummern erhielt Nachrichten, die bestimmte Ausdrücke wie „Gratisgeld" oder „Echtgeld" und Links zu gefälschten Websites enthielten. Ab diesem Zeitpunkt wird jeder, der dem Link folgt, aufgefordert, sich anzumelden und vertrauliche Informationen weiterzugeben. Es wurde nachgewiesen, dass die von den Spammern verwendete Datenbank der ApexSMS-Firma gehört, deren Legitimität noch unbekannt ist. Obwohl Sicherheitsforscher auf die Datenbank zugegriffen und versucht haben, so viele Informationen wie möglich abzurufen, weil sie befürchten, dass der Vorgang unerwartet beendet wird, ist immer noch nicht bekannt, wer und aus welchem Grund auf diese Daten zugreifen und sie verwenden kann, da sie noch verfügbar sind.[4]

_Formulare waren das Mittel

Spammer manipulierten Feedback-Formulare auf den Websites großer Unternehmen, die dazu dienten, Fragen zu stellen, Wünsche zu äußern oder Newsletter zu abonnieren. In diesem Berichtsjahr nutzten die Spammer jedoch nicht die verknüpften Postfächer des Unternehmens, sondern nutzten ein geringes Maß an Website-Sicherheit, umgingen alle reCAPTCHA-Tests und registrierten mehrere Konten mit gültigen E-Mail-Informationen. Infolgedessen erhielten die Opfer eine legitime Antwort des Unternehmens, einschließlich der Nachricht des Spammers.[2] Auf diese Weise wurde sogar Google Forms manipuliert, um Benutzerdaten abzurufen und kommerziellen Spam zu senden. Ein aggressiverer Fall war der Spam-Angriff auf Unternehmenskonten, bei dem Geld an den Angreifer überwiesen wurde. Um das Opfer zu überzeugen, gaben die Spammer an, missbräuchliche Nachrichten in der E-Mail des Opfers an mehr als 9 Millionen E-Mail-Adressen senden zu können, wobei die E-Mail-Adresse des Unternehmens auf die schwarze Liste gesetzt würde.[3]

Beschreibung

Chamäleon-Spam

Verschiedene Kampagnen im Jahr 2019 verwendeten dasselbe Botnetz-System, um Spam-Nachrichten zu verteilen, obwohl sie zufällige Header und Vorlagen zum Formatieren des Inhalts verwendeten. Aus diesem Grund haben Sicherheitsforscher begonnen, diese Kampagnen als eine Gruppe unter dem Pseudonym „Chamäleon-Spam" zu untersuchen.[5]

Chamäleon-Spam-Nachrichten stammten aus verschiedenen Ländern und enthielten gefälschte Links zu gefälschten Stellenausschreibungen oder Stellenangeboten, Websites zur Buchung von Flugtickets, Sonderangeboten für den Kauf von Produkten oder sogar einfache bekannte Dienste. Diese Spam-Nachrichten verwendeten eine Vorlage, die der von gültigen Unternehmen wie Google, Qatar Airways, FedEx, LinkedIn oder Microsoft verwendeten ähnelt, damit der Empfänger den Unterschied nicht bemerkt.[2]

So hart wie alte Bots

Im Oktober 2019 wurden E-Mails mit Vorlagen auf Englisch, Deutsch, Italienisch und Polnisch mit dem gemeinsamen Thema „Zahlungsüberweisungshinweis“ weit verbreitet. Diese Nachrichten enthielten ein angehängtes Dokument mit einem Makro, und die Empfänger wurden gebeten, es beim Öffnen des Dokuments zu aktivieren. Nach der Aktivierung kann das Makro den Infektionsprozess starten, indem es versucht, den Emotet-Trojaner herunterzuladen.[13]

Das Necurs-Spam-Botnetz war in dieser Zeit nach einer langen Zeit geringer Aktivität sehr aktiv. Das Gamut-Botnetz war 2019 das drittaktivste Spam-Botnetz. Gamut-Nachrichten beziehen sich hauptsächlich auf Vorschläge für Dating oder Treffen mit Menschen, Angebote für pharmazeutische Produkte und Stellenangebote.[1]

_Anzahl der C2-Botnetze, die Malware-Familien zugeordnet sind

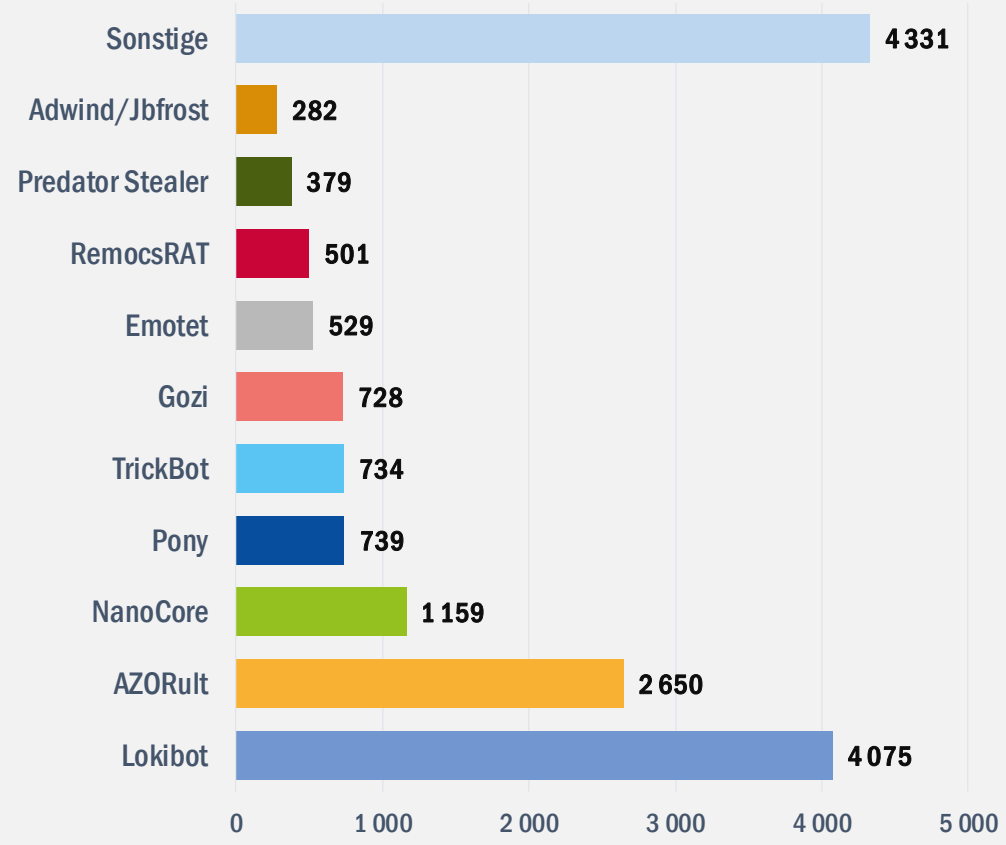


Abbildung 1 - Quelle: Spamhaus[14]

Beschreibung

_ COVID-19 öffnete neue Türen

Bald nach dem Beginn des COVID-19-Ausbruchs erschienen Phishing-Websites und schädliche Dateien, die per E-Mail übermittelt wurden, unter den Begriffen Coronavirus oder COVID-19. Es wurde berichtet, dass eine COVID-19-Spam-Kampagne die Eeskiri-COVID.chm19, eine getarnte Keylogger-Datei, verbreitet. Der Name der Akte könnte darauf hindeuten, dass die Kampagne ihren Ursprung in Estland hat (d. h. die estnische „Regel“ der Eeskirimäer).[11] Mitte Februar 2020 wurden nur wenige hundert COVID-19-Angriffe pro Tag registriert, bis März 2020 fanden jedoch täglich mehr als 2.500 Angriffe statt und verhießen ein hartes Jahr in Bezug auf Spam.[12]

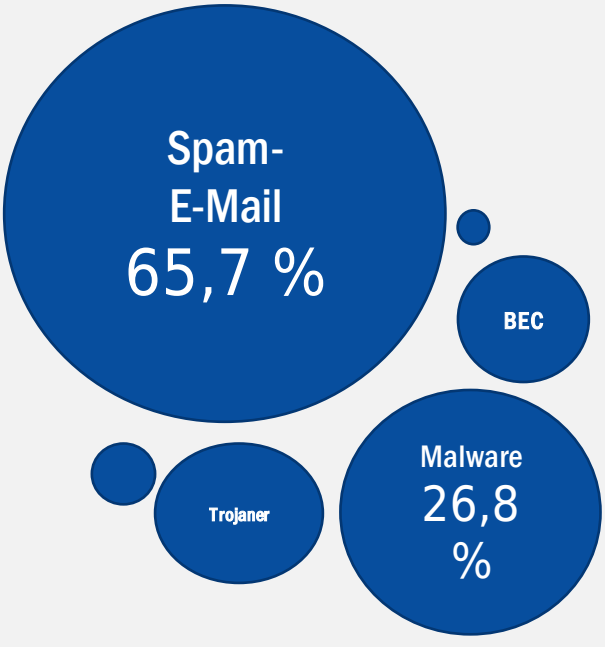


Abbildung 2: Bedrohungszunahme durch COVID-19. Quelle: Trend Micro[11]

_ Beispiele

01_Der ApexSMS-Spam-Vorgang

ApexSMS, ein SMS-Marketingunternehmen, erlitt eine Datenschutzverletzung, bei der die Kontaktdaten von mehr als 80 Millionen Menschen offengelegt wurden.

02_Die Chamäleon-Spam-Kampagne

Eine anhaltende Spam-Kampagne mit hohem Volumen ging von einem Botnetz-System aus, das Nachrichten mit zufälligen Headern sendete und häufig die Vorlage änderte.

03_Emotet Spam-Verteilungskampagne

Eine Spam-Kampagne zur Unterstützung der Verbreitung von Emotet-Malware.

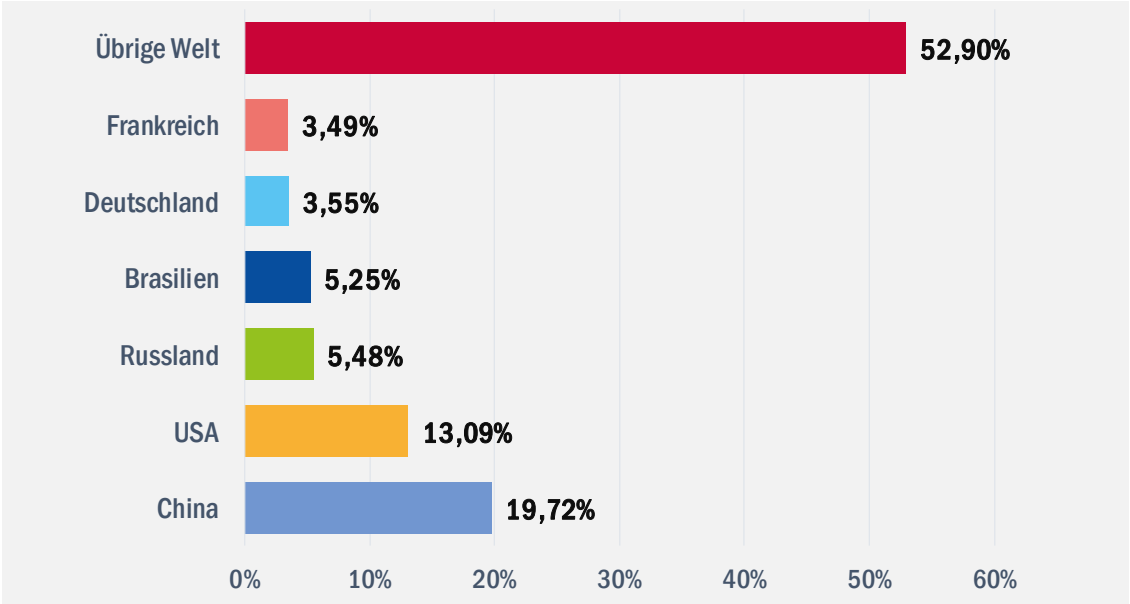
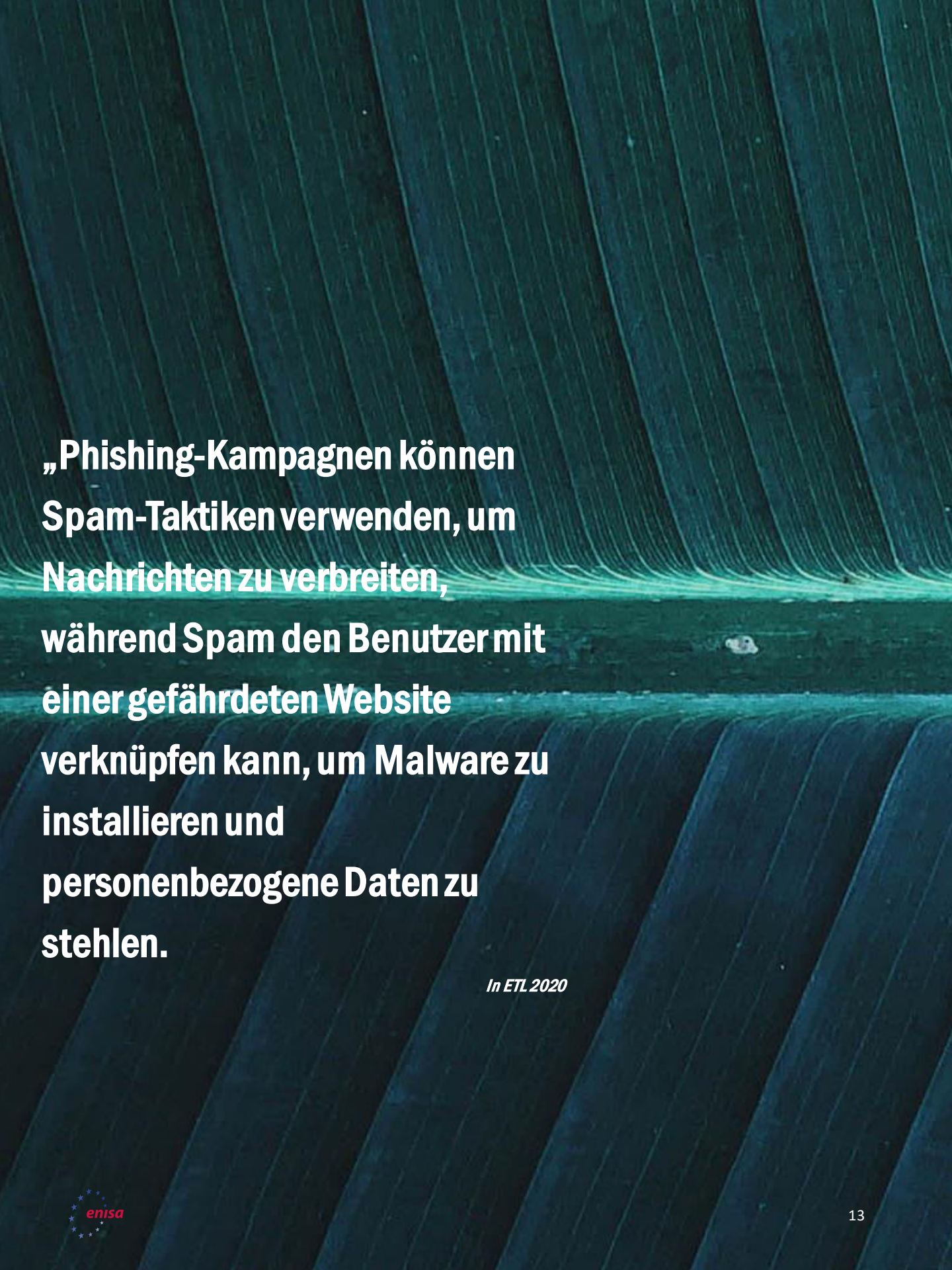


Abbildung 3: Die häufigsten SPAM-Quellen: Mehrere Quellen[17]

Minderung

Vorgeschlagene Maßnahmen

- Installieren Sie eine Inhaltsfilterung, um unerwünschte Anhänge, E-Mails mit schädlichem Inhalt, Spam und unerwünschten Netzwerkverkehr herauszufiltern.
- Aktualisieren Sie regelmäßig die Hardware, Firmware, das Betriebssystem sowie alle Treiber oder Software.
- Verwenden Sie die Multi-Faktor-Authentifizierung, um auf E-Mail-Konten zuzugreifen.
- Vermeiden Sie Geldtransfers auf nicht überprüfte Bankkonten.
- Vermeiden Sie es, sich bei neuen Links anzumelden, die in E-Mails oder SMS-Nachrichten empfangen werden.
- Entwickeln Sie Standardarbeitsanweisungen und -richtlinien für den Umgang mit sensiblen Daten.
- Verwenden Sie eine E-Mail-Gateway, falls möglich mit regelmäßiger und automatisierter Wartung von Filtern (Anti-Spam, Anti-Malware, richtlinienbasierte Filterung).
- Deaktivieren Sie die automatische Codeausführung, das Aktivieren von Makros und das Vorabladen von Grafiken und per E-Mail gesendeten Links.
- Implementieren Sie Sicherheitstechniken wie das SPF (Sender Policy Framework), die domänenbasierte Nachrichtenauthentifizierung, Reporting & Conformance (DMARC) und die DKIM (Domain Keys Identified Mail).
- Aktualisieren Sie regelmäßig Whitelists, Reputationsfilter und die Echtzeit-BlackholeList (RBS).
- Verwenden Sie KI und maschinelles Lernen zur Überprüfung von Anomalien.


„Phishing-Kampagnen können Spam-Taktiken verwenden, um Nachrichten zu verbreiten, während Spam den Benutzer mit einer gefährdeten Website verknüpfen kann, um Malware zu installieren und personenbezogene Daten zu stehlen.
In ETL 2020

Literaturangaben

1. "Email: Click with Caution - How to protect against phishing, fraud, and other scams" Juni, 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

2. "Spam and phishing in Q3 2019" 26. November, 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

3. "Spam and phishing in Q2 2019" 28. August, 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q2-2019/92379/

4. "SMS Spammers Doxxed" 9. Mai, 2019. Tech Crunch. https://techcrunch.com/2019/05/09/sms-spammers-doxxed/

5. "Tracking the Chameleon Spam Campaign" 25. September, 2019. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/

6 "5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned" 7. Juni, 2019. Gordon Flesch. https://www.gflesch.com/blog/biggest-cyberattacks-2019

7. "The world worst spammers". 2019. Spamhaus. https://www.spamhaus.org/statistics/spammers/

8. "Naming the coronavirus disease (COVID-19) and the virus that causes it". 2020. WHO. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

9. "WHO Director-General's opening remarks at the media briefing on 2019 novel coronavirus" 6. Februar, 2020. WHO. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-2019-novel-coronavirus/

10. "COVID-19 situation update worldwide, as of 11 June 2020" 2020. ECDC. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

11. "Developing Story: COVID-19 Used in Malicious Campaigns" 24. April, 2020. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

12. "2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape" 6. April, 2020. HIPAA Journal. https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

13. "Emotet is back: botnet springs back to life with new spam campaign" 16. September, 2019. Malwarebytes Lab. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

14. "Spamhaus Botnet Threat Report 2019" 28. Januar, 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

15. "Evasive Threats, Pervasive Effects" 27. August, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

16. "Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study" 28. Februar, 2019. Cisco. https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

17. "Internet Security Threat Report" Ausgabe 24, Feburar 2019. Broadcom. https://docs.broadcom.com/doc/istr-24-2019-en

18. "Spam and phishing in Q1 2019" 5. Mai, 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q1-2019/90795/

19. "Total Global Email & Spam Volume for May 2020" May, 2019. Talos. https://talosintelligence.com/reputation_center/email_rep#global-volume

20. "Q3 2019: Email Fraud and Identity Deception Trends" Juni, 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

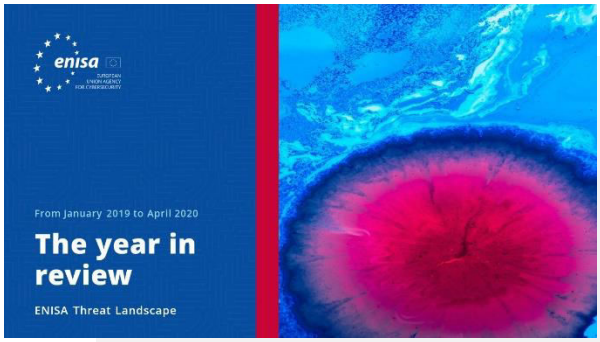
21. "The World's Most Abused TLDs" Spamhaus. https://www.spamhaus.org/statistics/tlds/

22. "Trend Micro Cloud App Security Report 2019" 10. März, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

23. "The Sprawling Reach of Complex Threats". 2019. Trend Micro Research. https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf

24. "SONIC WALL Security Center Metrics". SONIC WALL. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

Themenbezogen



ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

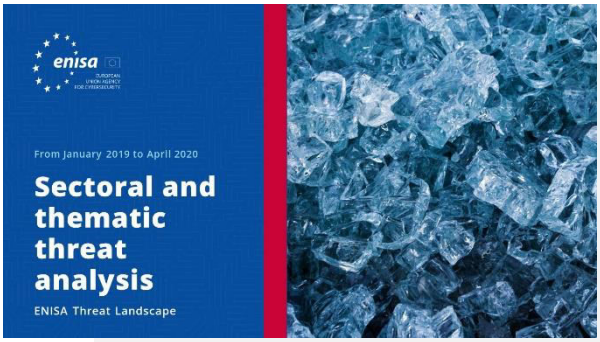
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

LESEN SIE DEN BERICHT



ENISA Threat Landscape-Bericht
Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

LESEN SIE DEN BERICHT

Über

_ Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Information über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

Herausgeber

Marco Barros Lourenço (ENISA) und Louis Marinos (ENISA).

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.
Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.

Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!
Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie hier klicken.

Impressum/Rechtshinweise

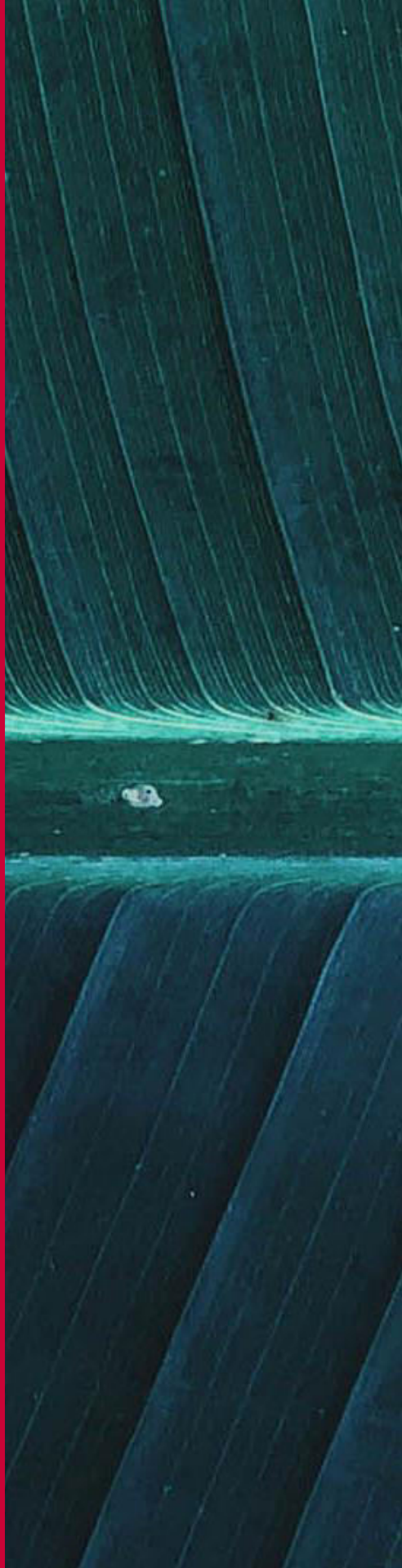
Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Griechenland
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu