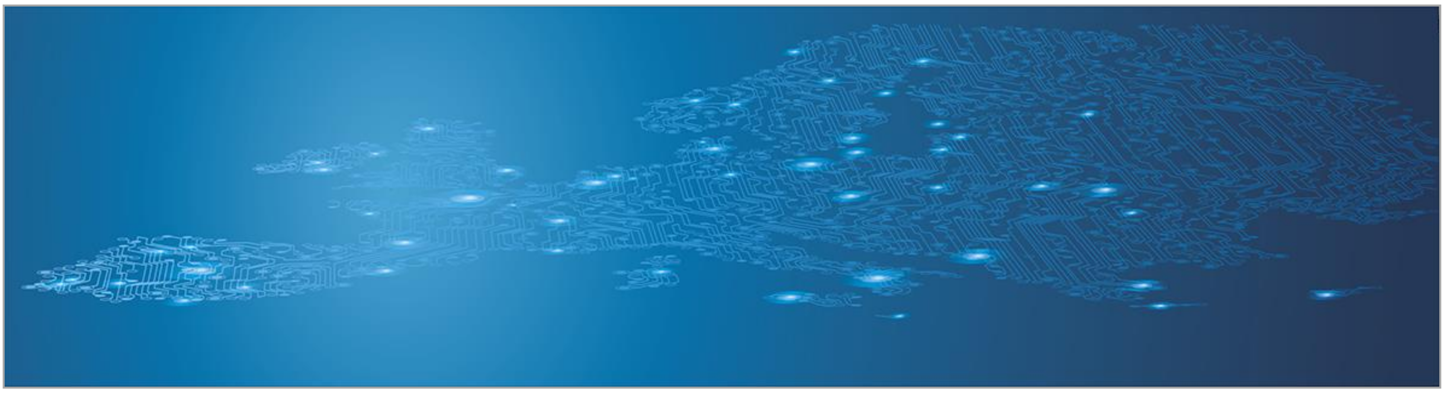
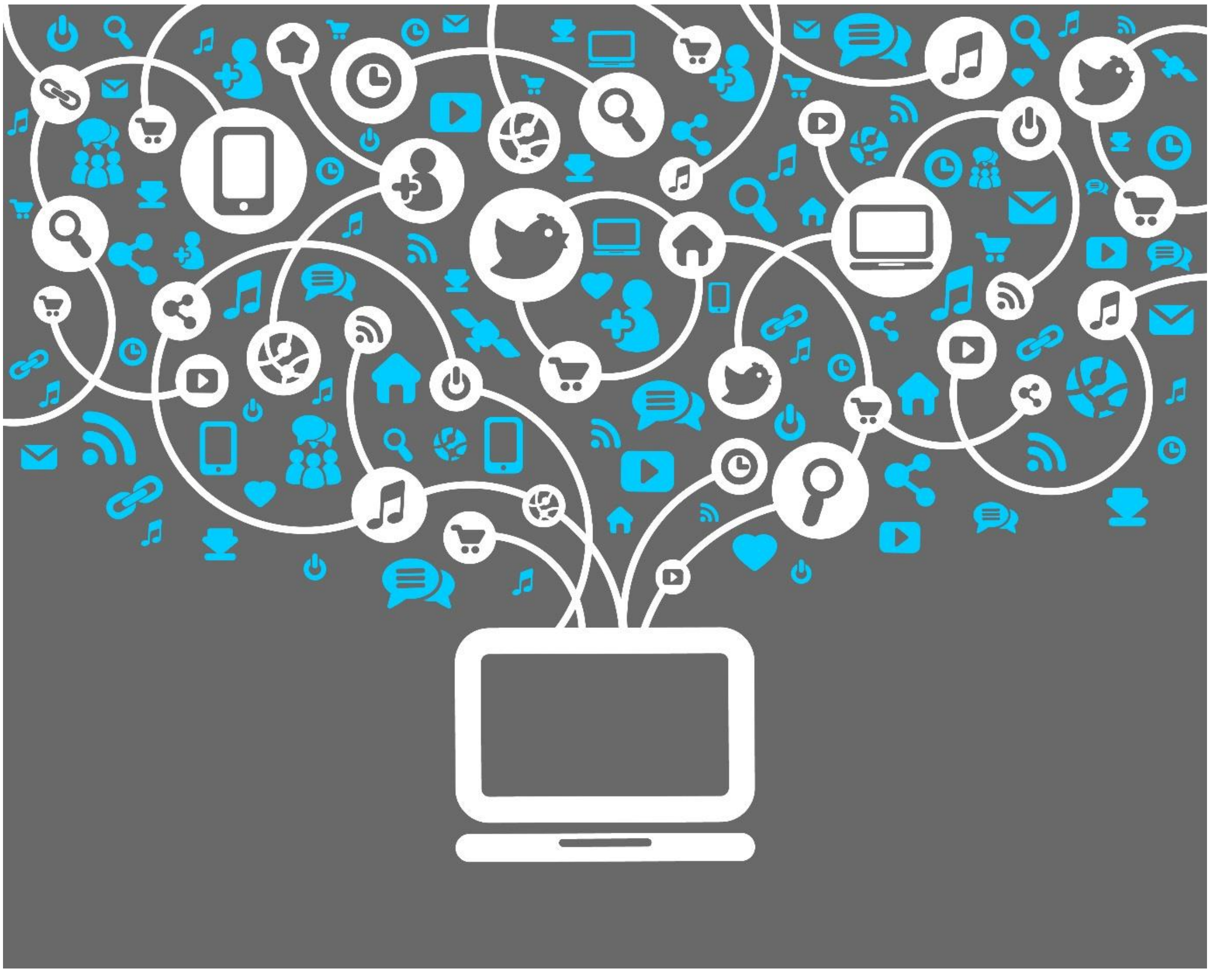




Social networks used as an attack vector for targeted attacks

Handbook, Document for teachers

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

1 Introduction

Goal

In this exercise, participants will investigate the vulnerabilities of social networks, using a targeted attack and Advanced Persistent Threat scenario as a test case to illustrate some examples of social network compromise examples. They will also examine the capabilities of social networks to respond to these kinds of threats.

Target audience

This exercise is useful for incident responders of all experience levels.

Course Duration

5 hours

Frequency

Once for each new CERT member

Structure of this document

	Task	Duration
🟥	General Description: The power and danger of social networks	30 min
🟥	Plenary Brainstorming	20 min
🟥	Real world example: attack of social network hack	10 min
🟥	Incident introduction and Advanced Persistent Threats	60 min
🟥	Group Exercise (mindmap): Social networks as vector for targeted attack	45 min
🟥	A Narrative and plenary discussion	90 min

2 GENERAL DESCRIPTION

If the original Internet boom of the 1990s was focused on connecting people and businesses through the World Wide Web, the next phase seems to be related to the rise of social media. Whether the crowd-sourced reviews aggregated on sites like Yelp, the microblogging broadcasts of Twitter or the relationship-hub portal of Facebook, hundreds of millions of people have started uploading information about themselves. They are not just sharing their daily lives, their likes and their purchasing habits with their friends, but are often publishing them for anyone and everyone to see: http://www.weknowwhatyouredoing.com/

However, as people add others to their circle of virtual friends, with everyone sharing information, this is not a Utopia. Real risks are associated with the openness of social networks. The UK Daily Mail reported that ‘officers logged 12,300 alleged offences involving’ Facebook in 2011.[1] Young people often use sites like Facebook despite official restrictions on accounts for those under 13 years old. Some have been targeted for cyber bullying, some by sexual predators. During vacations, Facebook and photo sharing sites have tipped off burglars that their homes are unoccupied and ripe for the picking.[2]

The technology of social networking can also protect those at risk. Facebook’s chat scanning software looks for key phrases before alerting site administrators who can review transcripts and decide if law enforcement should be contacted.[3]

Social networks provide many ways to connect outside of the usual channels. Social networks like Facebook and Twitter are also ways for more direct contact with the public, both to receive information from customers and to provide direct responses to their questions.

Pose the following questions to the class, largely to frame later discussions. But, if some trainees have some ideas to share, encourage the discussion.

- As social networks grow in their size and use, what are the risks to those companies and people who rely on such sites for the information they need to relay?
- What is the power of a social network over individual citizens and organisations?
- How are cyber criminals using social networks?
- What happens when social networks are attacked as part of an overall directed effort against a company?

In this exercise trainees will:

- learn about the phases of an Advanced Persistent Threat;
- see how social media access can be compromised during an APT attack;
- discuss how to coordinate action with CERTs, companies and social networks;
- develop ways individuals and organisations can re-establish control over their online social media presence after an attack;
- brainstorm methods to verify an individual’s or a company’s public social media profiles on sites like Facebook, Twitter or LinkedIn.

2.1 Introduction to social networks

Social networks are broadly defined by three shared characteristics:

- unified address book of contacts;
- combined with the ability to share pictures, videos, status updates, interests, locations, and schedules;
- communication with contacts via email, instant message, video conference, or telephone call.

2.1.1 General description, scope and trends in threats with social networks

What is the nature of threats when it comes to social networks?

[1] http://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html

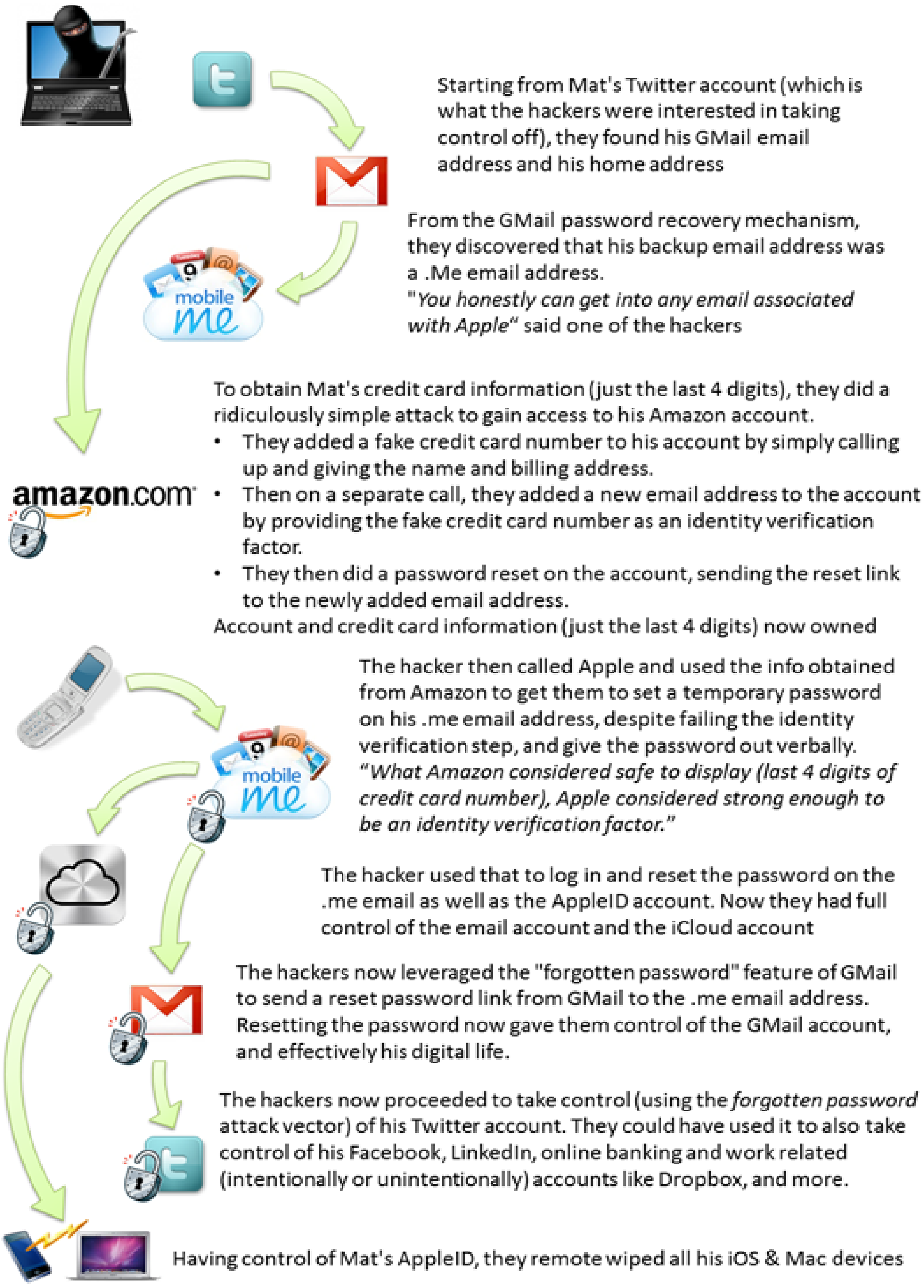
[2] http://arstechnica.com/tech-policy/2012/06/post-smug-vacation-statuses-on-facebook-get-your-house-burgled/

[3] http://www.neurope.eu/article/facebook-scans-users-chats-control-criminal-activity

- Privacy issues: users can expose information through misunderstood privacy settings or by approving ‘friend’ requests without knowing someone’s true identity. Things as simple as posting vacation or party pictures may reveal someone’s location at a given date and time. Vacation photos posted during a trip can reveal a user’s home is unoccupied to potential burglars.
- User profiling: information posted on social networks can allow attackers to learn where a target works, where he or she shops, and, significantly, the answers to many commonly used security challenge questions such as ‘Where did you go to high school?’ so that an attacker can reset passwords on other sites.
- Malware can spread via social networking apps
- Fake friends, compromised accounts: it is trivially easy to create social network accounts that masquerade as someone else (see Figure 81), tricking contacts to ‘friend’ the false account, giving an attacker greater access to information.

2.1.2 An example social network incident: The ‘Epic’ Honan Hack

The recent hacking of blogger Mat Honan as illustrated by Nishant Kaushik shows how compromised credentials from one system can cascade throughout someone’s digital life. As noted in the diagram, once hackers had taken over Honan’s Twitter account, they could have not only ruined his reputation, they could have accessed his Facebook and online banking accounts as well.



Starting from Mat's Twitter account (which is what the hackers were interested in taking control off), they found his GMail email address and his home address

From the GMail password recovery mechanism, they discovered that his backup email address was a .Me email address.
"*You honestly can get into any email associated with Apple*" said one of the hackers

To obtain Mat's credit card information (just the last 4 digits), they did a ridiculously simple attack to gain access to his Amazon account.

- They added a fake credit card number to his account by simply calling up and giving the name and billing address.
- Then on a separate call, they added a new email address to the account by providing the fake credit card number as an identity verification factor.
- They then did a password reset on the account, sending the reset link to the newly added email address.

Account and credit card information (just the last 4 digits) now owned

The hacker then called Apple and used the info obtained from Amazon to get them to set a temporary password on his .me email address, despite failing the identity verification step, and give the password out verbally.
"What Amazon considered safe to display (last 4 digits of credit card number), Apple considered strong enough to be an identity verification factor."

The hacker used that to log in and reset the password on the .me email as well as the AppleID account. Now they had full control of the email account and the iCloud account

The hackers now leveraged the "forgotten password" feature of GMail to send a reset password link from GMail to the .me email address. Resetting the password now gave them control of the GMail account, and effectively his digital life.

The hackers now proceeded to take control (using the *forgotten password* attack vector) of his Twitter account. They could have used it to also take control of his Facebook, LinkedIn, online banking and work related (intentionally or unintentionally) accounts like Dropbox, and more.

Having control of Mat's AppleID, they remote wiped all his iOS & Mac devices

Figure 1: Diagram of the steps in the Mat Honan hack.[4]

2.1.3 Plenary brainstorming session

Ask the following questions, one at a time, and ask the class to brainstorm answers. The idea is to stimulate creative thinking so that the trainees understand the kind of pressure that social media

[4] http://blog.talkingidentity.com/2012/08/the-epic-hacking-of-mat-honan-and-our-identity-challenge.html

hacks can have on a person. You can refer to this *Wired* magazine article (http://www.wired.com/threatlevel/2012/08/how-not-to-become-mat-honan/) that lists ways to avoid the vulnerabilities that Honan's attacker exploited.

- What if Honan's attacker threatened to empty his bank account unless he published favourable reviews of various technology products?
- What if Mat were a CEO, threatened with financial ruin and his reputation destroyed unless he delayed product plans to favour a competitor's release schedule?
- What might an attacker learn via compromised access to social networks that would compel his victim's compliance?
- If truly personal information is uncovered, what kind of power does the attacker have over the victim?

Share the process Mat Honan used to re-establish control over his online accounts after he was hacked as described in section 22.1.3 and also quoted below:

Because I couldn't send a backup to my now non-functioning phone, I had to fill out some forms online that asked me questions about my account usage that, presumably, only I would know. For example, I was asked to name the five people I e-mailed the most.

On Saturday morning, I received an automated e-mail from Google asking me to go online and define even more personal information. This time, I was asked for things like the names of folders in my Gmail account, and the dates on which I had set up various other Google accounts, like Google Docs. It was a little flummoxing, and I wasn't sure I knew the answers to these questions. But I tried, and I guess I got the answers right.

2.1.4 Real-world example of an attack that led to a social network hack

Another example of how an attack can grow from one security vulnerability to a full-out assault on a company's means of electronic communication is detailed in The book '*Hacking Exposed 7*', henceforth referred to as [HE7]. On p. 528:[5]

After accessing user account names and passwords through a SQL Injection attack on a website CRM system, hackers used these same passwords and usernames to access the company's Twitter, LinkedIn, and some email inboxes. They gained 'SSH access' and used 'a glibc privilege escalation [6] to gain super-user access. Once they achieved that, they were able to pilfer the system. But the coupe de grace was using the CEO's password to gain administrator-level privilege into HBGary's e-mail system (Google Apps), which allowed for IMAP downloading of employee inboxes. And the rest is security history—Anonymous published gigabytes' worth of e-mails from many of HBGary's employees. All from a simple SQL injection vulnerability.

Another reference for this particular attack is from ArsTechnica 'Anonymous speaks: the inside story of the HBGary hack'. [7]

PC World also published security tips based on this attack.[8]

[5] [HE7] : Hacking Exposed 7, McClure, Scott, Scambray, Joel, and Kurtz, George. McGraw-Hill: 2012. ISBN: 978-0-07-178028-5. References to this work have been abbreviated [HE7] with a page number.

[6] http://seclists.org/fulldisclosure/2010/Oct/257

[7] http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

[8] https://www.pcworld.com/businesscenter/article/221504/8_security_tips_from_the_hbgary_hack.html

2.2 INTRODUCTION TO TARGETED ATTACKS AND APTS

With the wealth of information that is available via social networks for learning about targeted individuals and organisations, attackers can launch targeted, customised attacks easier than ever before. The tempting option to masquerade as a target, either by compromising account credentials or resetting them as in the Honan hack, also gives attackers the ability to disseminate false information and gain greater access to a person's social network. When a Facebook 'friend' whose account has been compromised puts out a recommendation to try an app, malware can spread and more accounts can be attacked.

All of this means that targeted attacks, of which Advanced Persistent Threats (APTs) are one type, are enabled by and propagated through social networks.

2.2.1 Plenary lecture: Hallmark phases and vectors of APT attacks

The book [HE7] puts APTs generally:

…into two groups according to the attackers' objectives. The first group focuses on criminal activities that target personal identity and/or financial information and, coincidentally, information from corporations that can be used in a similar manner to commit identity and financial fraud and theft.

The second group serves competitive interests of industry or state-sponsored intelligence services (sometimes the two are not separate); and the activities target proprietary and usually non-public information, including intellectual property and trade secrets, to bring competing products and services to market or to devise strategies to compete with or respond to the capabilities of the organisations they steal information from.' ([HE7] p. 314)

Activist hacker groups like Anonymous and non-state terror organisations may seek to do damage without being concerned with long-term information extraction. Stuxnet, Flame and Gauss attacks are all examples of these as are Wikileaks-style information dumps.

Such attacks do still follow the general framework of an APT. In brief, these phases of an APT are:

- reconnaissance;
- initial attack using a blend of vectors;
- obtaining account credentials and elevating access;
- searching for and extracting data;
- using diversion or other techniques to maintain and extend access.

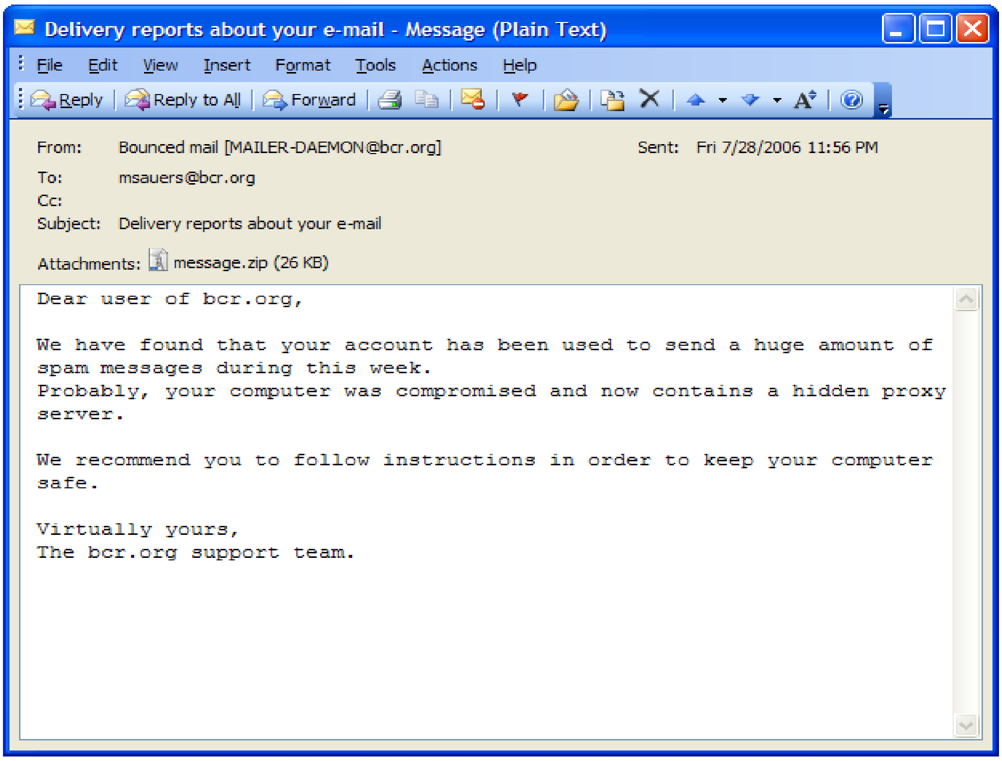
2.2.2 Reconnaissance to gather information on target companies and vulnerabilities

- Search for publically available information such as website lists of employee names and departments, financial records and planning documents.
- Perform electronic reconnaissance with steps like scanning IP addresses and ports, DNS records,[9] website code and email headers coming from the target company.
- Obtain physical access by posing as an employee of an outsourced janitorial service, getting a temporary job at the company's headquarters without a background check, delivery service or service technician. There are innumerable ways to gain access to a building and obtain access to files, infect computers, or attach network sniffing devices, which are linked to wireless data networks back to the attacker. Many companies lock the server room, but how many secure all loose papers on desks and shred everything in every waste bin?

[9] http://www.whitehats.ca/main/members/Jeff/jeff_dns_security/jeff_dns_security.html

2.2.3 Initial attack could be targeted email messages with embedded links to malicious websites, often with socially engineered detail to evade both technological and human detection. APTs are usually a blend of attack vectors from email messages, infected media, malicious websites, and key logging malware, in centrally controlled botnets.

- Over the last year, targeted, sophisticated viruses like Stuxnet, Flame, and Gauss have been delivered by all of the vectors listed above – but most notably by infected USB flash drives – to enter a network of industrial equipment that had no external network connection, let alone personnel running an email client to receive a malicious message. The specificity of the targets of these viruses makes them a key reminder of an APT: http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution
- One example of how USB flash drives can be used as a vector for an APT: The U3 file system on SanDisk and Memorex USB flash drives contains two partitions. One partition automatically runs a configured file when the drive is mounted under Windows's default autorun settings. Each manufacturer provides a tool to replace the U3 partition with a custom ISO file, allowing malicious programs to execute in the current logged on user's account with its privileges on the network. (This is especially damaging if the targeted users have extensive access to private information like the engineering staff or HR.) 'The most obvious attacks are to read the password hashes from the local Windows password file or install a Trojan for remote access. The password file can be e-mailed to the attacker or stored on the flash drive for offline cracking later using tools like fgdump.' ([HE7], p. 507)
- Malicious email in spearphishing attempts can leave behind clues. One such message looked like this:


Delivery reports about your e-mail - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward

From: Bounced mail [MAILER-DAEMON@bcr.org] Sent: Fri 7/28/2006 11:56 PM
To: msauers@bcr.org
Cc:
Subject: Delivery reports about your e-mail
Attachments: message.zip (26 KB)

```
Dear user of bcr.org,

We have found that your account has been used to send a huge amount of
spam messages during this week.
Probably, your computer was compromised and now contains a hidden proxy
server.

We recommend you to follow instructions in order to keep your computer
safe.

Virtually yours,
The bcr.org support team.
```

Figure 2: Sample malicious attachment email from a spearphishing attack

Another sample reads:

> From: Jessica Long [mailto:administrateur@hacme.com]
>
> Sent: Monday, 19 December 2011 09:36
>
> To: US_ALL_FinDPT
>
> Subject: Bank Transaction fault
>
> This notice is mailed to you with regard to the Bank payment (ID: 012832113749) that was recently sent from your account.
>
> The current status of the referred transfer is: ‘failed due to the technical fault’. Please check the report below for more information:
>
> https://finiancialservicesc0mpany.de/index.html
>
> Kind regards,
>
> Jessica Long
>
> TEPA – The Electronics Payments Association – securing your transactions

Figure 3: Sample malicious link in email from a spearphishing attack. [HE7] p. 325.

Clicking on the link in the email would show a user a webpage with text like ‘Please wait…’ and nothing more. In the background, a malicious piece of software would be invisibly installed on the user’s computer, one that can capture keystrokes, transfer files, send junk email as a user, prove the computer’s LAN for other hosts to infect – in short, any and all mischief that modern malware is capable of.

- False friend requests on social networks could also be a way to receive more private information from a target. Such friend requests can blend in with other, legitimate requests:

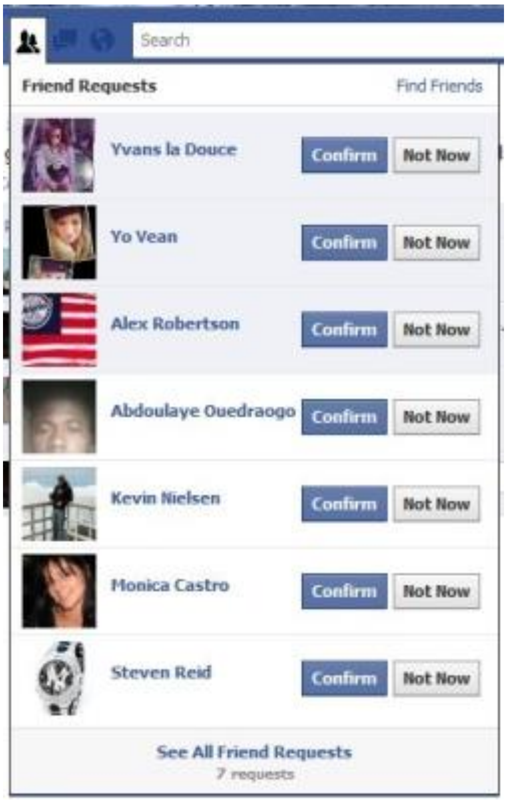
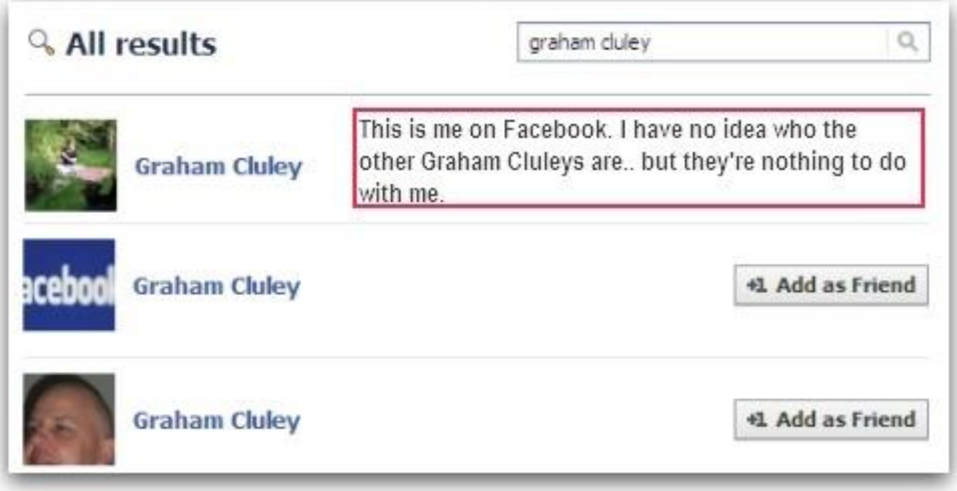


Figure 4: Sample list of friend requests on Facebook. Are all these people actually who they represent themselves to be?

Indeed, knowing who is who on sites like Facebook is not easy:



This is me on Facebook. I have no idea who the other Graham Cluleys are.. but they're nothing to do with me.

Figure 5: A sample Facebook friend search. When someone sees several people with the same name as a known friend when searching social network sites like Facebook, how can he or she know which person to add to their network?

- Malicious apps on social networking sites can trick users into giving them access to their personal data. Indeed, fake social networking 'friends' may serve as channels for false recommendations for malicious apps or links to malicious websites using URL shorteners like Bit.ly or Goo.gl. Koobface was a prominent example of an older malicious social networking worm that targeted Facebook, MySpace, Friendster, and Twitter users.[10]

[10] http://nakedsecurity.sophos.com/koobface/

2.2.4 Obtaining account credentials and elevating access

This is the third phase of an APT attack, included here for completeness. For the purposes of this exercise about social networks, you need not discuss the myriad of methods attackers may use to obtain credentials to user accounts and how they can achieve deeper levels of access.

2.2.5 Searching and extracting valuable data

This is the fourth phase of an APT attack, included here for completeness. For the purposes of this exercise on social networks, you need not discuss the processes attackers may follow to find, identify and remove the data they seek from a target.

2.2.6 Use diversion or varied techniques to maintain and extend illicit access for the long term

- Launching unrelated, 'louder,' more easily detected malware attacks to distract IT staff from the real infiltration
- Sometimes, diversion can be something very out of place. The Stuxnet worm, for example, was reported to play AC/DC's 'Thunderstruck' heavy metal song on some computers in Iran's uranium processing lab in the middle of the night – surely a confusing moment for those working the Help Desk that night.[11]
- Ultimately, attackers will create and/or control user accounts and profiles that appear normal on the network and have the same access levels and methods as legitimate users. Unless accounts are carefully audited, they could remain on a system for a long period of time.

2.2.7 Specific Signs of an malware and APT compromise (section 22.2.2 is quoted from [HE7] p. 326)

(This section, 22.2.2, is quoted from [HE7] p. 326.)

Malware, always wants to survive a reboot and all possible user actions. To do this, the malware can use several mechanisms, including:

- Using various 'Run' Registry keys
- Creating a service
- Hooking into an existing service
- Using a scheduled task
- Disguising communications as valid traffic
- Overwriting the master boot record
- Overwriting the system's BIOS

To investigate a 'suspicious' system, investigators use a mix of forensic techniques and incident response procedures. The correct way to perform incident response is by using the order of volatility described RFC-3227.[12] This RFC outlines the order in which evidence should be collected based upon the volatility of the data:

- Memory
- Page or swap files
- Running process information
- Network data such as listening ports or existing connections to other systems
- System Registry

[11] http://www.newscientist.com/blogs/onepercent/2012/07/iranian-nuclear-facilities-thu.html
[12] http://www.ietf.org/rfc/rfc3227.txt

- System or application log files
- Forensic image of disks
- Backup media

One possibility to investigate a compromised machine is to create a kit using several different tools. One example of a pre-made kit is the SANS Investigate Forensics Toolkit (SIFT) found at http://computer-forensics.sans.org/community/downloads. During any investigation, it is important to avoid contaminating the evidence as little as possible. Incident response tools should be copied to a CD-ROM and an external mass-storage device. The toolkit investigators used in this case [the 'case' is a description of Gh0st Attack from 2008–2010 in [HE7] pp. 323–349] consisted of a mix of SysInternals and forensics tools:

- AccessData FTK Imager[13]
- SysInternals Autoruns[14]
- SysInternals Process Explorer[15]
- SysInternals Process Monitor[16]
- WinMerge[17]
- Currports[18]
- SysInternals Vmmap[19]

'We have observed a common set of indicators in the numerous APTs cases that analysts have investigated and have found the following phenomena indicative of an APT…' ([HE7] p. 363):

- Network communications utilizing SSL or private encryption methods, or sending and receiving base64-encoded strings
- Services registered to Windows NETSVCS keys and corresponding to files in the %SYSTEM% folder with DLL or EXE extensions and similar filenames as valid Windows files
- Copies of CMD.EXE as SVCHOST.EXE or other filenames in the %TEMP% folder
- LNK files referencing executable files that no longer exist
- RDP files referencing external IP addresses
- Window Security Event Log entries of Types 3, 8 and 10 logons with external IP addresses or computer names that do not match organisational naming conventions
- Windows Application Event Log entries of antivirus and firewall stop and start
- Web server error and HTTP log entries of services starting/stopping, administrative or local host logons, file transfers, and connection patterns with select addresses
- Antivirus/system logs of C:\, C:\TEMP, or other protected areas of attempted file creations
- PWS, Generic Downloader, or Generic Dropper antivirus detections
- Anomalous .bash_history, /var/logs, and service configuration entries
- Inconsistent file system timestamps for operating system binaries

Break (15 minutes)

[13] http://accessdata.com/products/digital-forensics/ftk
[14] http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx
[15] http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx
[16] http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx
[17] http://winmerge.org
[18] http://www.nirsoft.net/utils/cports.html
[19] http://technet.microsoft.com/en-us/sysinternals/dd535533.aspx

3 Exercise course

3.1 Incident summary

All managers of CurrentCo, an electric utility, receive forged emails and messages in social networking sites, purporting to be from their immediate colleagues, containing links, which, when visited, silently install spyware. The week before, many members of the utility's engineering team received USB flash drives at a conference. The drives contained a hidden root kit, installed when the engineers open vendor sales material. Using the information gleaned from the spyware, credentials to access the utility's Twitter and Facebook accounts were stolen.

3.2 Small group discussion and mindmap creation

Divide the trainees into groups of four (if there are enough people, then a fifth person could represent the attacker). Ideally, several whiteboards or flipcharts and markers are available, one for each small group. If only one is available, trainees can create the mindmap on paper and re-draw it on the room's whiteboard for the class to see. (Comparisons of maps will be more difficult in this setup, but the re-drawing process will facilitate each group explaining their map to the rest of the class.)

3.3 Small group discussion and mindmap setup

- Encourage the groups to include trainees from different organisations, countries and job roles to avoid one set of views or ideas dominating the group.
- Ask the trainees to select among themselves who will represent the roles and perspectives of the following people:
  - CurrentCo IT technician;
  - CurrentCo media director, primary user of company's Twitter and Facebook accounts as well as primary news media contact;
  - Twitter customer service representative;
  - CERT representative;
  - Attacker.
- Remind the class of the incident description in section 22.3.1. Direct the trainee groups to develop the various concepts and solutions in the points of discussion section 22.3.4. The trainees have the questions listed in their toolsets.
- Locate the groups in break-out areas if available or at least ensure that they are sufficiently separated that their discussions don't interfere with each other.
- The trainer, assisted by a co-trainer, should visit each group in turn. Briefly answer questions from the groups if needed, allowing the trainees themselves to expound upon different possibilities and perspectives.
- The overall next small group discussion and mind mapping should take about 60 minutes. Trainers may need to nudge the groups forward if they take too much time on some items. If some groups move through the items quickly, the trainers can entertain some discussion with the group, ask additional questions or make suggestions.

A note about group size: groups of two are too small to have various perspectives presented in group discussion. Groups of five may result in some people being silent while two or three trainees do all the talking. Encourage groups to be sure to review each discussion topic from the perspective of each role listed.

- In each group, one trainee will draw a mindmap in collaboration with the others (the trainer sample mindmap is at the end of section 22.4.4). At the end of the small group discussion, each group will present their mindmap to the class, explaining their thought process and comparing and contrasting with other maps. Trainers should also note differences between the trainees' and the sample mindmap to prompt further discussion among the whole class.

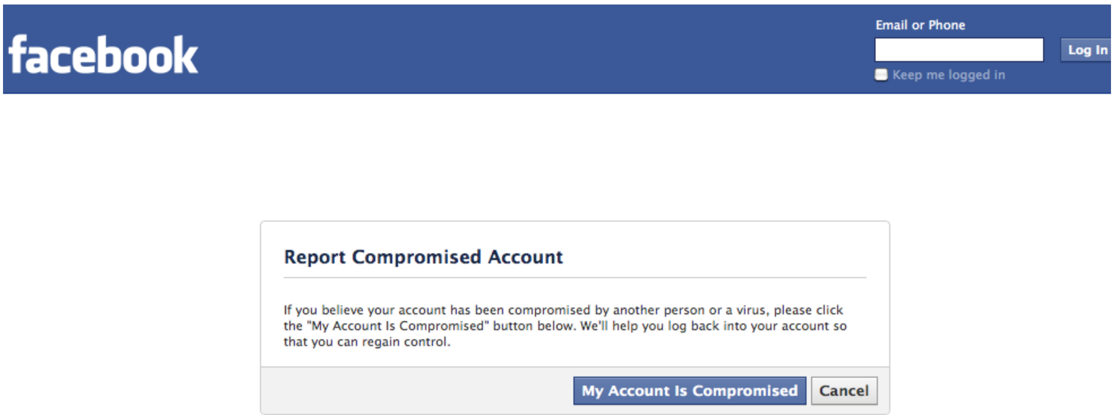
3.4 Small group points of discussion

In their groups, students should discuss the following stages of response to the above scenario:

- Report issue: Who are the proper authorities and representatives to contact? When?

Twitter: https://support.twitter.com/forms/hacked

Facebook: http://www.facebook.com/hacked



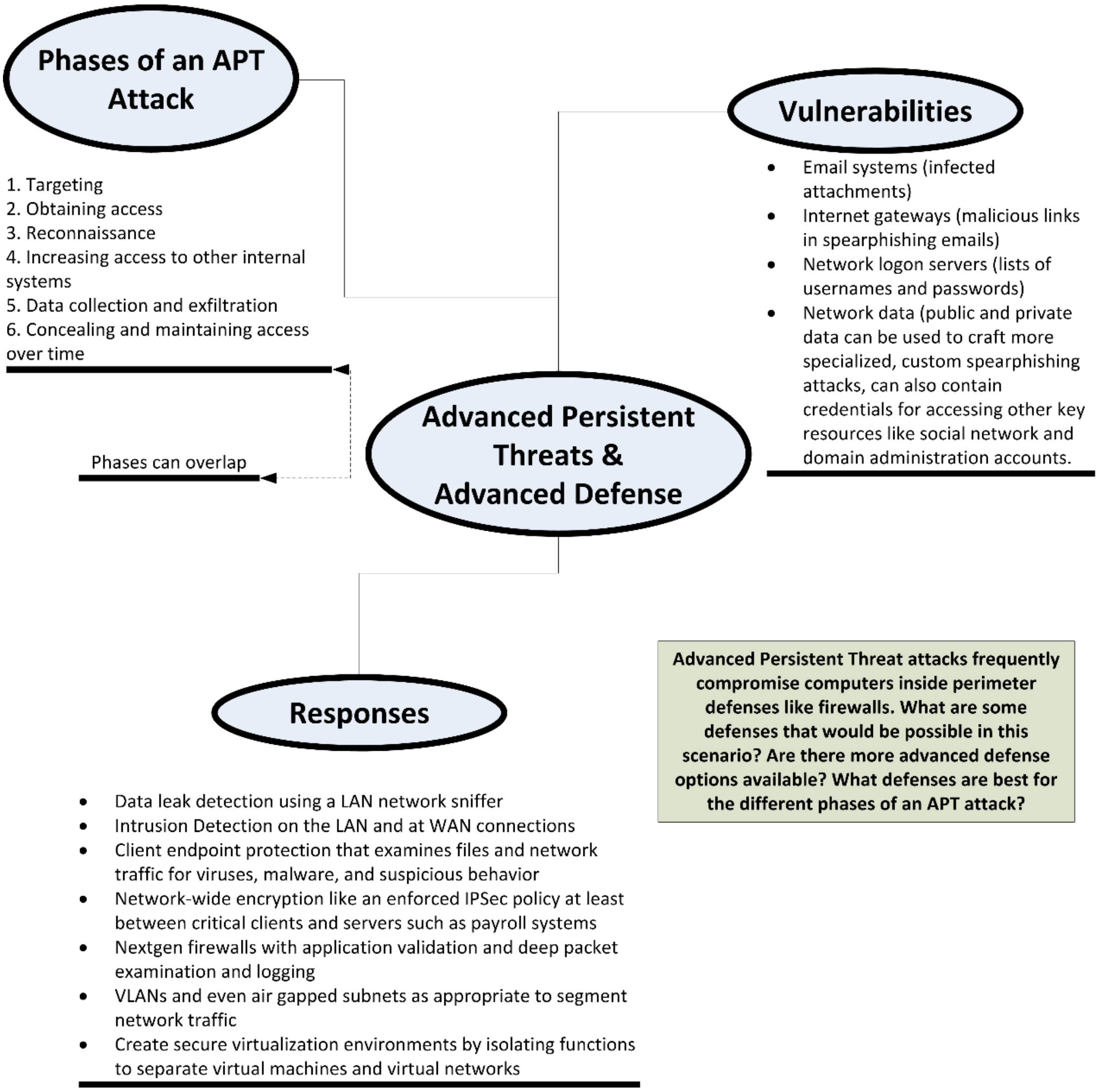
Report Compromised Account

If you believe your account has been compromised by another person or a virus, please click the "My Account Is Compromised" button below. We'll help you log back into your account so that you can regain control.

Figure 6: Facebook's webpage for reporting compromised accounts

- Correct issue: What is needed to protect the company's networks, both during the attack period and during the clean-up phase afterward? What can be done if social media outlets are themselves compromised and used to disseminate false information?
- Prevent issue in future: Do APT-style attacks require more advanced responses such as data leak detection on corporate networks to stop data from leaving the local network even if internal computers are compromised?
- Let the groups draw a mindmap as they discuss and present the maps to the whole class

A sample mindmap follows:



Advanced Persistent Threats & Advanced Defense

Phases of an APT Attack

1. Targeting
2. Obtaining access
3. Reconnaissance
4. Increasing access to other internal systems
5. Data collection and exfiltration
6. Concealing and maintaining access over time

Phases can overlap

Vulnerabilities

- Email systems (infected attachments)
- Internet gateways (malicious links in spearphishing emails)
- Network logon servers (lists of usernames and passwords)
- Network data (public and private data can be used to craft more specialized, custom spearphishing attacks, can also contain credentials for accessing other key resources like social network and domain administration accounts.

Responses

- Data leak detection using a LAN network sniffer
- Intrusion Detection on the LAN and at WAN connections
- Client endpoint protection that examines files and network traffic for viruses, malware, and suspicious behavior
- Network-wide encryption like an enforced IPSec policy at least between critical clients and servers such as payroll systems
- Nextgen firewalls with application validation and deep packet examination and logging
- VLANs and even air gapped subnets as appropriate to segment network traffic
- Create secure virtualization environments by isolating functions to separate virtual machines and virtual networks

Advanced Persistent Threat attacks frequently compromise computers inside perimeter defenses like firewalls. What are some defenses that would be possible in this scenario? Are there more advanced defense options available? What defenses are best for the different phases of an APT attack?

Figure 7: Sample mindmap about advanced defences to Advanced Persistent Threats

Break (15 minutes)

3.5 Narrative

While the trainer may read the following narrative section aloud to the trainees, the trainee toolset includes the following text in full and it is recommended the trainer ask the trainees to read the narrative to themselves.

Jane Smith, CurrentCo Media Director, said she usually spent her lunch hour updating her personal Facebook page on her work PC. 'It's just easier to catch up on friend requests and wall posts while I have my sandwich,' she said. She had accepted a batch of new friend requests that had been built up over the weekend. A few weeks before a major thunderstorm, she noticed an update from a friend with a URL-shortened link, labelled as registration for her college reunion. She clicked the link amidst eating her lunch and taking a few phone calls.

'I do like trying out all the different apps,' she said, 'but honestly I'm sure most of them I don't use more than a few times, if that, after adding them in and clicking 'Allow' before they go to the bottom of my homepage.'

Asked when she was first unable to log into the company's Facebook and Twitter accounts, Jane responded, 'I'm not sure. I usually just have those sites remember my password, so I don't have to type it in normally. After IT took my computer, I had to use my password sheet to sign in from another laptop to update customers after the storm. Yes, that's when I couldn't get in.'

***

'Our IDS system did detect an unusual amount of traffic coming from Jane's PC,' CurrentCo's IS Manager reported. 'It was just around when that big thunderstorm knocked out power to half the town? Anyway, I think we just got the thing off her desk, but then we started getting reports of all kinds of errors. Database and web servers were going throwing off a lot of errors and, oh yeah, for some reason all the print spoolers kept shutting down. You know how many calls we got from the Executive office about not being able to print in one hour?'

***

'I recommended that CurrentCo immediately contact the social media companies and offered to make the calls and conference them in,' said Ingrid Johansen. 'Even though we had some delay between when Jane Smith's computer was infected, we could recommend steps that the company's IT staff could perform to regain control over their accounts and to search their network for other penetrations. It took some digging to find those USB flash drives in the maintenance department.'

***

'We just got back from a maintenance services convention,' said Geoff Peterson, head dispatcher for CurrentCo's repair department. 'They were pushing an "eco" theme this year and so they gave us those thumb drives to get digital brochures from the vendor area. Since management wanted us to make new contacts and learn about new products, I visited almost every booth and plugged that thing into the computer when I got back to the office to print off some of the specification sheets I collected.'

'After the storm hit, I used our scheduling program to put every crew out on repair duty. It wasn't until we didn't see changes in line status after a few hours that I started to think something was wrong. A few crews were close enough to the garage for our old walkie-talkie radios to work and I called them back in. We coordinated everything with those radios and paper maps I kept in every truck.'

***

Nigel Henry, Twitter technical support, reviewed Jane's initial report that CurrentCo's account had been hacked. 'Given that it was from a verified account from a public utility, we immediately called the contact phone number on their record to confirm. We just had two numbers—the main switchboard and Jane's mobile phone—but with the storm, both those lines were inaccessible for about a day so it took a while before we could freeze the account.'

***

Dossier:
CurrentCo Attacker, [name unknown, alias 'UltiKaos']
Began posting CurrentCo customer information on the company's Twitter feed late Saturday night after a large thunderstorm knocks out power to thousands of houses and businesses. The attacker disrupts repair work assignments on the company's intranet work assignment system, sending crews away from problem areas. Customers direct messages on Twitter are responded to with insults. With full access, changes all email and phone number access on the company's Twitter account, delaying its recovery by several days.

3.6 Plenary discussion

After the trainees have read the narrative in section 22.3.4.1, ask the following questions to the full class. Encourage creative discussion to think of new possibilities not just for social network hacks, but also for how to improve responses to such attacks and to blunt their effects in the future.

- Can social media contacts be more trustworthy (or less) based on the amount of verification done when opening an account?
- How is trust established in social media; who do you trust in this network?

Trusted introductions, professional organisations, and even more so, cooperative teams like CERTs need to build ties and connections before moments of crisis.

- How could we authenticate a person or company's identity if their account has been hacked? What if it's an emergency?

Sample ideas: using a standard hashtag (#outage) or a pre-established, custom tag to verify a poster's identity assist communication on a microblogging site, setting multiple to authenticate a contact's identity beyond just one or two phone numbers or email addresses

- What data needs to be collected for later forensic analysis? Who needs to collect it and how? How can we save data from a site like Facebook or Twitter?
  Potential resources:
  - http://readwrite.com/2009/08/10/10_ways_to_archive_your_tweets
  - *'Inside Social Media Archiving' from Legal Talk Network: http://legaltalknetwork.com/podcasts/digital-detectives/2010/10/inside-social-media-archiving/*

The key concept – doubly true with social networks as the rest of the Internet – is that once something is posted online, it is practically impossible to delete it. Though this concept is most helpful to keep in mind before joining social networks, before information is made public, it is always relevant.

3.7 Remind trainees of ENISA's Golden Rules from 'Online as soon as it happens' to reduce social media risk[20]

- Pay attention to what you upload.
- Verify virtual friends before trusting them with personal information.
- Maintain divide between corporate and personal accounts and information.
- Respect others' privacy.
- Learn about and use social networks' privacy control settings.

3.8 Sophos has also published a best practice guide for Facebook security[21]

- Use Facebook privacy settings to create levels of information that is shared.
- Accept friendship requests only from those people you actually know.
- Create a 'limited friend' group who cannot see all the information shared on your account.
- Like hardening a server by running only needed services and opening only needed ports to a network, disable any functions of a social networking site that you don't actually want to use.

If time permits, show the following Sophos videos about malware apps on Facebook.

- What does a Facebook worm look like? (http://www.youtube.com/watch?v=_uFa3P0sLA4&feature=player_embedded)
- Demonstration on removing malicious apps from Facebook account: http://www.youtube.com/watch?v=Or-qR0Y300w&feature=player_embedded
- Demonstration that people are willing to become friends with strangers on Facebook:

http://www.youtube.com/watch?v=9LPRaiu0Y8M&feature=relmfu

1. *Ask the trainees: What are these 'Advanced Persistent Threats'? How are they different from computer hacking in the past?*
2. *What if these hackers start putting up false information on Twitter or Facebook? How will we know it's really CurrentCo, for example, posting the information?*

3.9 Pivot: Social networks can give us greater security too

Social media can be used as an effective identity verification system. Some bouncers in the UK check online if someone's ID matches their online profiles (http://www.digitaltrends.com/social-media/club-bouncers-are-now-checking-your-facebook-to-confirm-identity/)

4 EVALUATION METRICS

Evaluating the results of this exercise, the trainer should consider the class's understanding of these key concepts:

- the strengths of social networks to respond to incidents like APT, even as they expose some vulnerabilities of identity theft;
- weaknesses of storing increasing amounts of information on social networks instead of directly controlled systems;
- concepts of identify verification through checking credentials, national ID schemes, and other forms of authority compared to a more peer-to-peer system (enabled by social networks) of identity and trust that can include pseudonyms. PGP public key servers are an example of a decentralised verification system;

[20] http://www.enisa.europa.eu/ activities/cert/security-month/deliverables/2010/onlineasithappens
[21] http://www.sophos.com/en-us/security-news-trends/best-practices/facebook.aspx

- how can an organisation recover from a compromised social network account if it is used for disinformation or releasing confidential information?

Refer back to original Exercise Goals:

- Learn about the phases of an Advanced Persistent Threat
- See how social media access can be compromised during an APT attack
- Discuss how to coordinate action with CERTs, companies and social networks
- Develop ways individuals and organisations can re-establish control over their online social media presence after an attack
- Brainstorm methods to verify an individual's or a company's public social media profiles on sites like Facebook, Twitter or LinkedIn

5 REFERENCES

1. Nemey, Chris, *5 top social media security threats*, Network World, 31 May 2011 (http://www.networkworld.com/news/2011/053111-social-media-security.html)
2. Thomas, Keir, *8 Security Tips from the HBGary Hack*, PCWorld, 7 March 2011 (https://www.pcworld.com/businesscenter/article/221504/8_security_tips_from_the_hbgary_hack.html)
3. M86 Security, *Advanced Persistent Threats*, 20 August 2010 (http://www.sysec.co.uk/media/3371/wp_advanced_persistent_threats.pdf)
4. Miller, Russel, *Advanced persistent threats: defending from the inside out*, CA Technologies, 2012 (http://www.ca.com/~/media/Files/whitepapers/advanced-persistent-threats-wp.pdf)
5. Ernst & Young, *Advanced Persistent Threats: What's all the Hype?*, 10 May 2012 (http://www.isaca-northtexas.org/Presentations/2012-05%20Lunch%20-%20Advanced%20Persistent%20Threats.pdf)
6. Bright, Peter, *Anonymous speaks: the inside story of the HBGary hack*, ArsTechnica, 15 February 2011 (http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/)
7. Fowler, Geoffrey, *App Watch: The Deadly Sins of Facebook Malware*, WSJ Blogs, 29 March 2011 (http://blogs.wsj.com/digits/2011/03/29/app-watch-the-deadly-sins-of-facebook-malware/)
8. Vaas, Lisa, *Facebook hacking and godawful gold lamé sneakers*, Naked Security Blog from Sophos, 7 June 2012 (http://nakedsecurity.sophos.com/2012/06/07/facebook-hacking/)
9. Gonzolez, Zuly, *Guide To Removing Malicious Apps From Your Facebook Account*, Light Point Security Blog, 8 January 2011 (http://lightpointsecurity.com/content/guide-to-removing-malicious-apps-from-your-facebook-account)
10. McClure, Scott, Scambray, Joel, and Kurtz, George. *Hacking Exposed 7*, McGraw-Hill: 2012.
11. Perez, Sarah, *How Safe are Facebook Applications?*, ReadWriteWeb [blog], 16 October 2009 (http://www.readwriteweb.com/archives/how_safe_are_facebook_applications.php)
12. Cluley, Graham, *I accepted a fake Facebook friend request, should I be afraid?,* Naked Security [blog] from Sophos, 21 February 2011 (http://nakedsecurity.sophos.com/2011/02/21/i-accepted-a-fake-facebook-friend-request-should-i-be-afraid/)
13. ENISA, *Online as soon as it Happens*, 8 Feburary 2010 (http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/onlineasithappens)
14. Hogben, Giles, *Security issues in the future of social networking*, ENISA, January 2009 (www.w3.org/2008/09/msnws/papers/Future_of_SN_Giles_Hogben_ENISA.pdf)
15. Taylor, Will, *Social networking's nasty habits*, ZDNet, 31 May 2012 (http://www.zdnet.com/social-networkings-nasty-habits-3040155290/)

16. Pace, David; Paganini, Pierluigi; Kelson, Ron; Martins, Fabian; and Gittins, Benjamin, *Social Networks Part 2 – Have you been infiltrated?*, The Malta Independent Online, 26 August 2012 (http://www.independent.com.mt/news.asp?newsitemid=149674)
17. *Stay Away From Malicious Facebook Apps,* Hacktrix [blog] (http://www.hacktrix.com/stay-away-from-malicious-and-rogue-facebook-applications)
18. Information Warfare Monitor, *Tracking GhostNet – Investigating a Cyber Espionage Network,* 29 March 2009 (http://infowar-monitor.net/research).
19. Bennett, Shea, *Twitter, Facebook, LinkedIn: Social Networking Security And Privacy*, All Twitter [blog], 2 November 2011 (http://www.mediabistro.com/alltwitter/social-networking-security-privacy_b15359)
20. Paul, Ian, *Update: LinkedIn Confirms Account Passwords Hacked*, PC World, 6 June 2012 (http://www.pcworld.com/article/257045/update_linkedin_confirms_account_passwords_hacked.html) [risks to security when unhashed password tables are posted publically]

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu