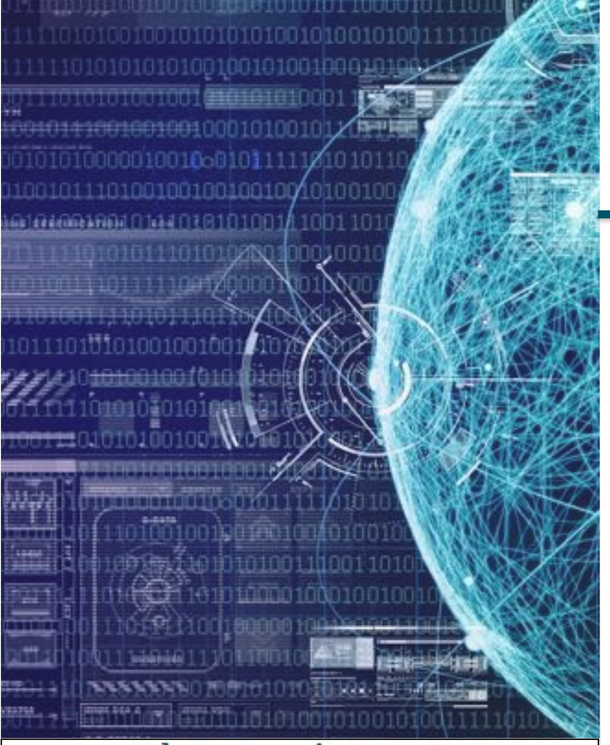


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

UNIVERSITY OF Southampton

COMP6224: Introduction

Vladimiro Sassone
Cyber Security Centre
University of Southampton

what is cyber security?

UNIVERSITY OF Southampton

CYBER SECURITY: protection of the cyberspace against ***cyber threats*** and ***vulnerabilities***

CYBER SPACE: complex of activities carried out through networks of computers; more precisely it's a ***cyber ecosystem****:* it includes computer systems and devices, critical infrastructures(e.g. telephone network or power grid), entire economic processes (e.g. eCommerce or electronic banking and payment systems), users, their data, their interests

it's not just computers or smart phones, it's not just the Internet, it's the network of small computers and its sensors in your car, it's your pace-maker sending information to your doctor, it's the network of controllers regulating industrial control systems etc.

what is cyber security?

CYBER THREAT: typical threats include ***unauthorised access***, ***destruction***, ***system overrun and takeover***, ***propagation of malicious code***, ***data thieving and fabrication***, … The attacks are "*cyber*" themselves. E.g., if your computer is stolen, that's not a breach of cybersecurity. If anybody manages to access data on your stolen computer, that is an issue for cybersecurity.

CYBER VULNERABILITY: the presence of weaknesses or loopholes in systems which may lead (systematically) to cyber attacks.

what are the challenges?

Rather than mentioning a few specific problems, it is convenient to put in focus the fact that the organisation of our society and our lives are by now largely computer-supported, and this creates a very significant vulnerability to all sorts of attacks to very different aspects of what we do. For instance, it concerns

NATIONAL SECURITY: attacks to critical infrastructures such as Transport, Energy and Communications can have devastating effects, and are now regular part of warfare and terrorist scenarios;

GOVERNMENT AND PUBLIC BODIES: the robustness to intrusion and tamper of electronic services, which typically hold very sensitive information;

THE ECONOMIC PROCESSES: the protection of industrial secrets and practices, the confidentiality of business information and tenders; the viability of the network economy, just think of the banking system.

THE CITIZEN: the privacy and legitimate use of personal data against deanonymisation and impersonation attacks from all sources; the challenged from cybercrime.

what are the challenges?

To mount a credible programme of **research and education** to create and actuate **countermeasure** to cyber threats and limit our vulnerability.

Government says that a lot can be achieved by **educating users**. Similarly, Government points out that Cyber Security is a **board level responsibility** for companies. From the view of having a safer Internet, that's is of course true, given that the most commonly used password in the UK is 123 and most companies have no Cyber Security policy at all.

Yet, to put the **burden on the end-users is somehow unfair**. The issue we face can be extraordinarily complex and subtle. We have no solution to some cyber-threats, every day new attacks are created (e.g. we foresee in the near future a stepping up of cloud-based attacks, as the technology becomes more and more used), we have no comprehensive map of our vulnerabilities.

why unfair?

Just think of the security upgrades of your favourite operating systems. This is software that has been around for ages, created and maintained by some of the smarted people in the smartest companies, yet you keep hearing that a vulnerability has been discovered in this or that web browser that allows arbitrary code to be executed etc.

Now, of course you can be careful about your passwords, you can adopt safer practice, the same way you don't misplace your credit card or leave it there for the grab. But, what can you do if the drive-by-wire system in your car is taken over maliciously? That's beyond your control as user, as are many many things. In fact, you really have no idea of what is on your phone or laptop. *There are easily 2M+ files in my laptop.*

Make no mistake, this has the potential to destroy the way we live & work.

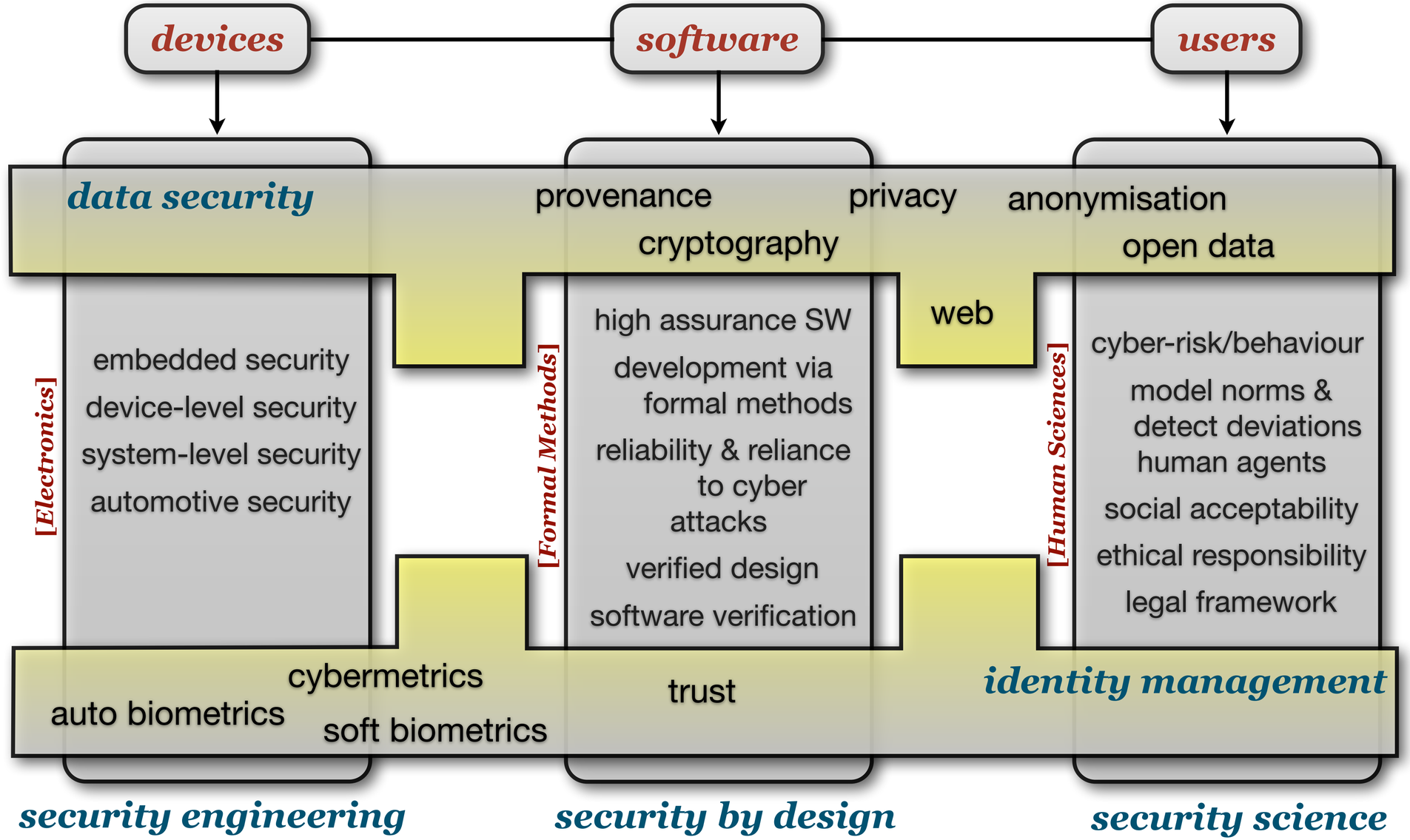
what do we need?

We need to carry out the research to come up with systematic countermeasure, with security frameworks and infrastructures able to react quickly to new attacks. We need to identify and develop the cyber security professionals to go our there on the network and patrol it, to be the good guys in the cyberspace. ***EDUCATION is an EMERGENCY.***

It doesn't stop here. The legal framework is important too. Cyber threats have no frontiers and are more real than many are aware. Cybercrime software now exists online as a free download and cyber criminals are finding it easier and easier to engage in malicious activity. Within government and academia, we have a responsibility to share knowledge, intelligence and expertise, and to develop countermeasures. Southampton is likely to be bidding to host the new centre.

All this in the respect of the rights of the citizen. The risk of falling into hyper-restrictive regulations exists. I think it's a human reaction to a situation where we feel we do not have in place adequate countermeasures to the potentially tremendous effect of large-scale cyber attacks. That is why I believe that research (both in Law and technical) will help also in this respect, by empowering us.

work at the southampton ACE



EPSRC
Engineering and Physical Sciences Research Council

GCHQ

Scheme to Recognise Academic Centres of Excellence in Cyber Security Research

Call type: Invitation for Applications

Closing date: 16 December 2011, 16:00

Briefing meeting date[1]: 15 November 2011

Summary

UNIVERSITY OF Southampton

EPSRC
Engineering and Physical Sciences Research Council

GCHQ

13 ACEs
all similar in aggregation of cyber talent and expertise & high density of cyber research

all different in variety of focus and approach

Summary

UNIVERSITY OF Southampton

EPSRC
Engineering and Physical Sciences Research Council

GCHQ

13 ACEs
all similar in aggregation of cyber talent and expertise & high density of cyber research

all diff ty of f d
appro

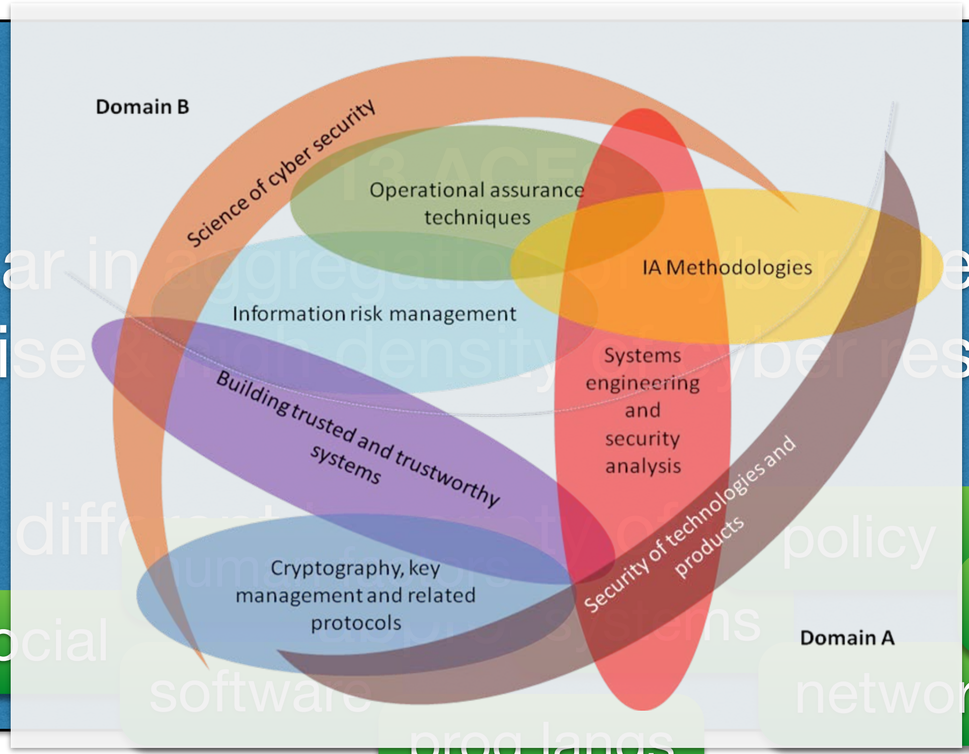
crypto
human factors
policy
social
systems
trust
software
networks
prog langs
privacy
risk

Summary

it all started here

EPSRC
Engineering and Physical Sciences Research Council

GCHQ



all similar in aggregate ent and
expertise research

all

crypto

social

trust

policy

networks

privacy

risk

Summary

what does the world look like from an ACE?

what does the world look like from an ACE?

what does the world look like from an ACE?

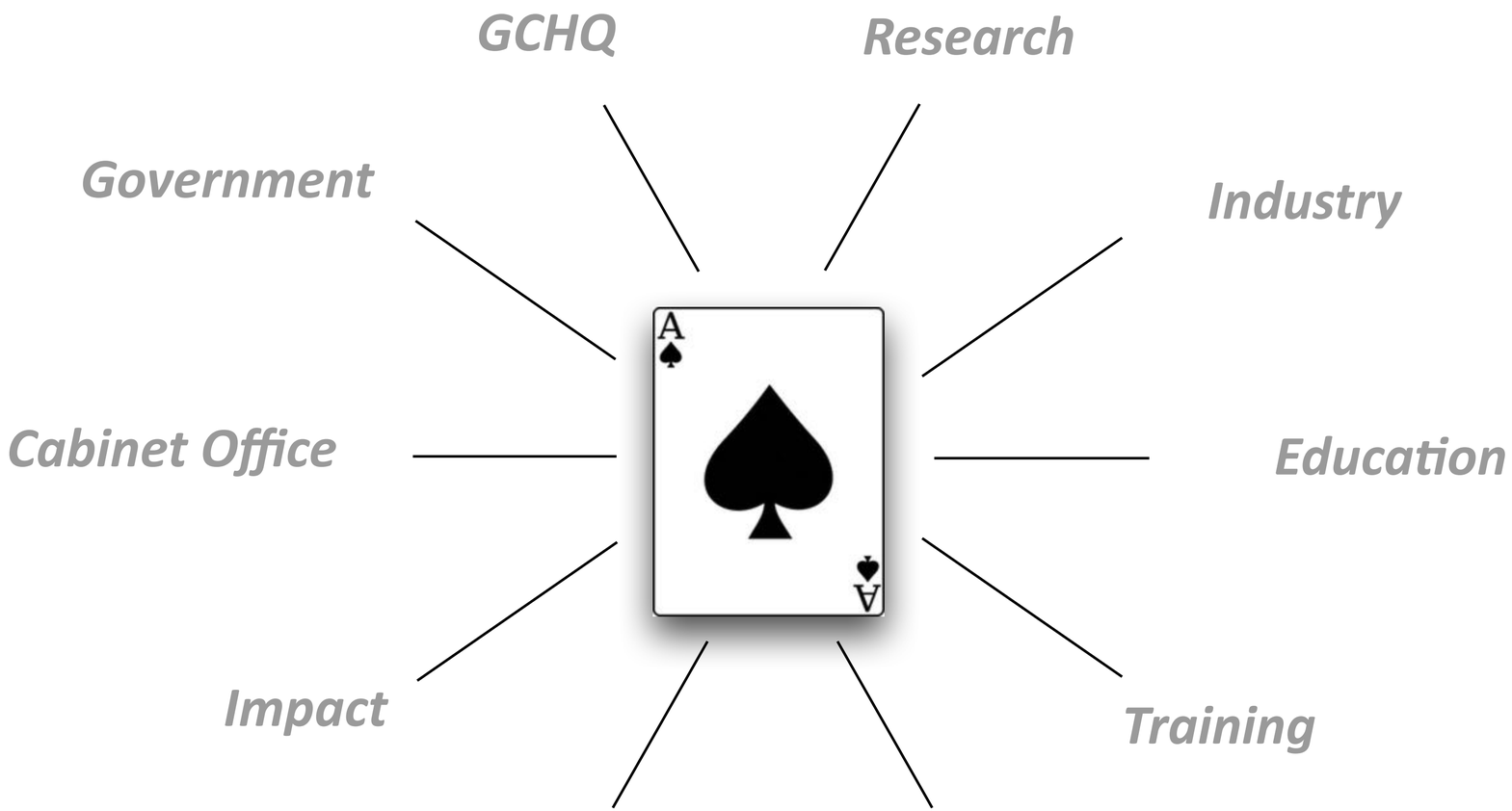
what does the world look like from an ACE?

what does the world look like from an ACE?

new MSc degrees
adapt UG degrees
fill gaps in industry

what does the world look like from an ACE?

what does the world look like from an ACE?



work with IAA and BIS to design education pathways

what does the world look like from an ACE?

assist in set up cybercrime units, training, support investigations

what does the world look like from an ACE?

what does the world look like from an ACE?

what does the world look like from an ACE?

on economy, policies and society

what does the world look like from an ACE?

It may be egocentric view, but illustrates how ACEs can be important

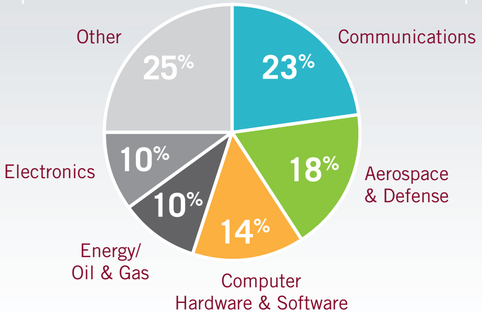
the harsh reality in figures (mandiant 2011)

UNIVERSITY OF Southampton

INTRUSIONS BY THE NUMBERS

This **M-Trends** focuses on Mandiant's observations while responding to targeted attacks over the last year. During our investigations, we observed **6 trends.**

What Industries Are Being Targeted By Advanced Attackers?



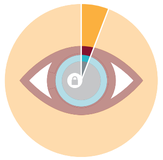
In What % of Cases Did the Bad Guys Use Valid Credentials?

100%

How Many Advanced Threats Used Publicly-Available Malware?

77%
of all intrusions Mandiant investigated

How Are Compromises Being Detected?



6%
of victims discovered the breach internally

94%
of victims were notified by an external entity

What Was the Time From Earliest Evidence of Compromise to Mandiant's Involvement?

416
median number of days that the attackers were present on a victim network before detection

TRENDS

1 Malware Only Tells Half the Story

Searching for malware identifies only 54% of systems compromised in an incident.

2 Everything Old Is New Again

Attackers are using passive backdoors to evade network- and host-based detection methods.

3 RATs!

The use of publicly available malware in targeted attacks is increasing.

4 M&A Is Being Served With a Side of Compromise

Organizations are buying and selling compromise during merger & acquisition activities.

5 Some Assembly Required

Attackers are targeting companies that collaborate together within a supply chain in order to assemble a comprehensive intellectual property portfolio.

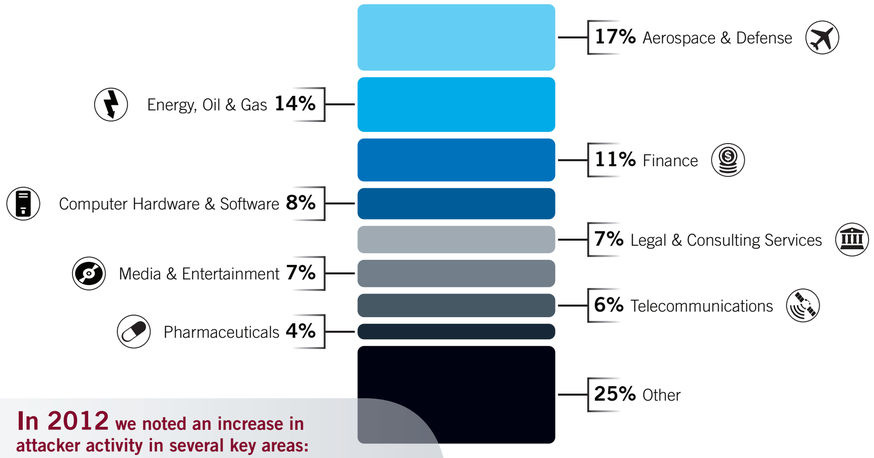
6 It Pays to Be Persistent

Financially motivated attackers are shifting toward longer-term persistence on victim networks.

updated data (2012)

VICTIMS BY THE NUMBERS

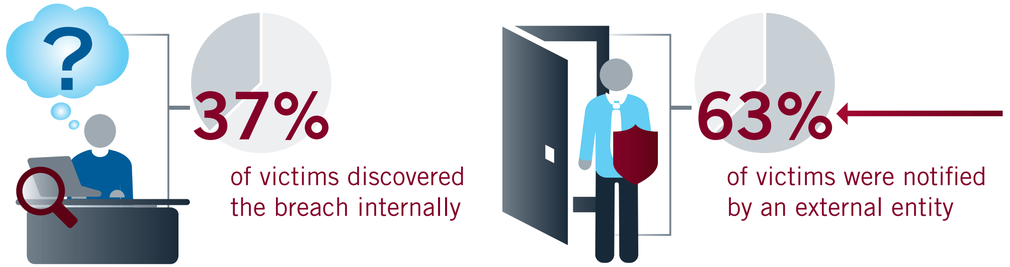
Industries Being Targeted by Advanced Attackers



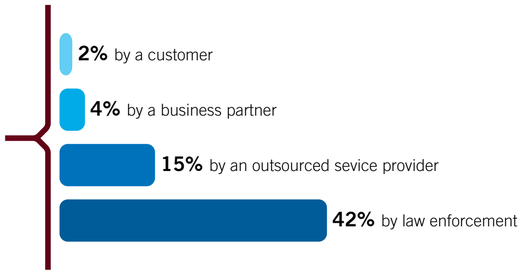
In 2012 we noted an increase in attacker activity in several key areas:

- Media & Entertainment — up from 2% to 7%
- Pharmaceuticals — up from 1% to 4%
- Finance — up from 7% to 11 %

How Compromises Are Being Detected



a most shocking figure



4 Years 10 Months

Longest time period Mandiant observed APT1 in a single victim's network

TABLE 2: EVIDENCE OF COMPROMISE BEYOND MALWARE

EVIDENCE OF COMPROMISE	DESCRIPTION
 Unauthorized Use of Valid Accounts	In 100% of the cases Mandiant responded to this year the attacker used valid credentials. Evidence of such account activity can be found through the examination of Windows event logs, registry entries, file ownership, and network traffic captures.
 Remote System/File Access	Attackers use compromised systems to remotely access systems and files within the target environment. The Windows registry and web browser history often contains evidence of this activity.
 Trace Evidence & Partial Files	Attackers frequently remove tools, scripts, and files generated by their activities. Remnants of attacker activity can be found in restore points, scheduled task logs, and the Windows event logs.

If only 54% of a compromise can be discovered by searching for malware, the other 46% must be identified through enterprise-wide analysis of registry entries, event logs, scheduled task logs, inventory management logs, network traffic captures, and file system artifacts. Systems identified as suspect during this process are triaged to determine if full forensic analysis is necessary.[1]

THE TAKEAWAY

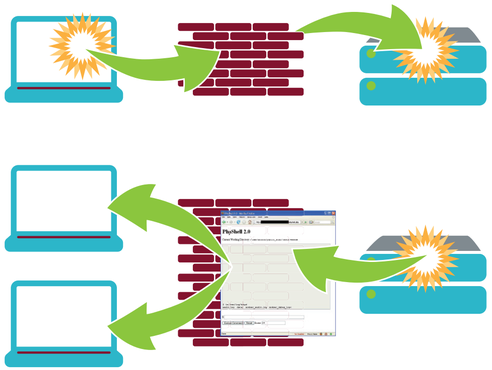
Effective computer incident response teams combine software and intelligence to overcome issues of scale and limitations of malware-centric tools and techniques. Countering sophisticated threats requires technology that can rapidly sweep endpoints for indicators of compromise, extract evidence of an intrusion, and determine incident scope and impact.

EVERYTHING OLD IS NEW AGAIN

Attackers are using passive backdoors to evade network- and host-based detection methods.

Historically, the Advanced Persistent Threat (APT)[2] has used reverse backdoors for remote access to compromised environments. These backdoors initiate outbound network connections and use traditional persistence mechanisms such as ServiceDLL or ImagePath replacement and startup folders. These backdoors were detectable because they generated consistent and routine network traffic and resided in common locations.

During 2011, Mandiant has seen the APT diversify their backdoor mechanisms to be more resilient against detection and remediation efforts. Specifically, they are using a new persistence mechanism that we are calling "Passive Backdoors." These backdoors are harder to detect using standard network traffic analysis and traditional forensic techniques. They do not generate network traffic. They do not always use traditional persistence mechanisms, and they are frequently deployed outside of the known attack path. Two examples of passive backdoors are port listeners and web shells.



Port Listeners: A port listener is a sophisticated passive backdoor. In the past year, Mandiant identified low-level network drivers, such as miniport drivers, being used for command and control (C2). The low-level network driver allows network traffic to be examined, before higher-level drivers and applications, such as FTP, process the traffic. This allows the backdoor to identify its C2 traffic, activate the passive malware, and pass non-C2 traffic to the higher-level application. For example, the higher-level application might be an FTP server listening for connections on TCP port 21.

Web Shells: Web shells provide an attacker simple access to a number of administrative functions on the server — from enumerating users, to uploading files, to providing an interactive command shell. By utilizing HTTPS they blend in easily with legitimate web traffic. Web shells are typically created within an existing web directory, are timestomped[3] to match the date/time information from legitimate web pages and are disguised as a legitimate part of the application.

THE TAKEAWAY

Rather than solely rely on client-initiated backdoors, the APT attackers have blended the more traditional backdoor listening as a server. The use of passive backdoors is an indication that targeted attack methodologies continue to evolve as attackers seek to ensure continued access to environments and thwart detection mechanisms.

RATS!

UNIVERSITY OF Southampton

TABLE 3: OVERVIEW OF PUBLICLY AVAILABLE TOOLS USED IN TARGETED ATTACKS

TOOL NAME	DESCRIPTION	TYPE
ASPXSpy	This open-source ASP web application provides an intruder with the ability to perform remote command execution, upload/download files, interact with SQL databases, perform port scans, and query registry keys.	RAT
Cachedump	This tool obtains password hashes for domain logins that have been cached in the Windows registry.	Privilege Escalation
GetHashes	This tool obtains password hashes from the SAM file.	Privilege Escalation
Gh0st RAT	This widely available backdoor provides a graphical client builder and graphical server.	RAT
Gsecdump	This tool obtains hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets.	Privilege Escalation
Hookmsgina	This tool hooks the legitimate Microsoft Graphical Identification and Authentication DLL (msgina.dll) and dumps the username, domain, password and old password (in the event of a password change logout) to a file.	Privilege Escalation
Htran	The "Honkers Union of China Packet Transmit Tool" is a port director which takes incoming traffic on one port and sends it to a specified IP and port of another system.	Other
Incognito	This tool performs Windows access token manipulation.	Privilege Escalation
Pass-the-Hash toolkit	This set of tools accesses hashes of users who have interactively logged into a system and then allows an intruder to impersonate those users by "passing" those hashes to other systems.	Privilege Escalation
Poison Ivy	The Poison Ivy (PI) Remote Access Trojan (RAT) is a publicly available backdoor which provides comprehensive remote access capabilities on a compromised system. Poison Ivy variants are configured, built, and controlled using a graphical Poison Ivy management interface.	RAT
PsExec	The SysInternals tools, now distributed by Microsoft, also have myriad legitimate uses to allow system administrators to remotely invoke executable file across a network.	Lateral Movement
Pwdump	This tool obtains password hashes from the SAM file. Many password dumping tools are variants of Pwdump.	Privilege Escalation
Radmin	This remote administration tool is commonly used by legitimate system administrators.	RAT
Windows Credential Editor (WCE)	This tool is used to grab current sessions, modify credentials, and perform pass-the-hash.	Privilege Escalation
Xdoor	This backdoor's interface and server are displayed in Chinese. Its functions include key logging, audio and video capture, file transfers, HTTP proxy, retrieval of system information, reverse command shell, DLL injection, and command execution.	RAT
ZXshell	This backdoor functions include key logging, file transferring, SYN floods, the ability to launch processes, steal credentials, and disable local firewalls.	RAT

RATS!

The use of publicly available malware in targeted attacks is increasing.

THE TAKEAWAY

Classifying incidents involving publicly available tools and malware as minor issues can be risky. Take advantage of anti-virus tools' alerts on publicly available malware to uncover potential larger issues. Look for trends and anomalous patterns in these alerts and investigate as appropriate.

mergers & acquisition and compromise

M&A IS BEING SERVED WITH A SIDE OF COMPROMISE

Organizations are buying and selling compromise during merger & acquisition activity.

2011 was the busiest year for global merger & acquisition activity since the recession of 2008.[4] Based on Mandiant's experience, it was also the busiest year for the acquisition and divestiture of APT compromises. We responded to a record number of targeted intrusions that were discovered while the victimized organizations were in the process of integrating into their new parent organizations.

THE TAKEAWAY

Organizations with a mature security program understand that incident detection and response is a continuous business process, not an isolated exercise. Defeating persistent threats requires technical, repeatable, and automated scrutiny of business units, acquisitions, divestitures, partners, suppliers, and outsourcers.

UNIVERSITY OF Southampton

SOME ASSEMBLY REQUIRED

Attackers are targeting companies that collaborate within a supply chain in order to assemble a comprehensive intellectual property portfolio.

Over the last year, Mandiant identified a distinct trend of related organizations being targeted because they partnered on a specific project or because their technology was complementary to a targeted technology. Advanced attackers have learned that in order to gain full visibility into complex projects, data is required from all of the companies that partnered to design or build the targeted project.

THE TAKEAWAY

Defensive-minded enterprises recognize that their organization could be part of a targeted ecosystem and remain vigilant for intruders who steal and integrate intellectual property, business intelligence, methods, and other information assets from victims in other parts of their supply chain. Frustrating threat actors requires recognizing that no organization is too small for compromise as long as the data it possesses is important.

IT PAYS TO BE PERSISTENT

Financially motivated attackers are shifting toward longer-term presence on victim networks.

Financially motivated attackers have historically relied on relatively simple tools, tactics, and procedures (TTPs) to steal payment card data. These attacks were known as “smash and grab” compromises — the attacker would steal targeted data and never return to the victim organization. Maintaining persistent access was not considered essential. If access was necessary again, they would leverage the same exploit they used initially. This strategy simplified their operations as they did not need to deploy backdoors or maintain command-and-control networks.

THE TAKEAWAY

Financial organizations are as much a target of persistent attackers as the defense industrial base and government organizations. The financial industry can benefit from real-time threat intelligence and by continuing to improve their ability to detect and respond to targeted threats.

case studies (1)

CASE STUDY

ELECTRONICS MANUFACTURER
THE PARTNER ORGANIZATION

Coordinated attack to several apparently unrelated victims

It was only by connecting the dots between the two victims that the attacker's goal was clear: rather than targeting a single company for a particular technology, they had been tasked to acquire the more advanced, broader technology.

case studies (2)

CASE STUDY

FINANCIAL INSTITUTION
PERSISTENT ORGANIZED CRIME

Initial compromise through misconfigured web server administrative interface.

Once the foothold was established, they moved laterally in the environment, taking advantage of misconfiguration created several admin accounts.

It was then easy to install several backdoors to guarantee persistent presence and start on their real objective: search for financial information (eg credit card numbers)

Eventually the attacker installed backdoors on 80 systems, dumped password for all users, compromised 5 user accounts stole data from systems with no malware on.

This long-term access would ensure the attacker enjoyed continued, unfettered access to the environment to continually steal more data.

CASE STUDY

DEFENSE INDUSTRIAL BASE
INTEGRATING COMPROMISED COMPANIES

The attack began with a phishing email containing a malicious PDF attachment. Prior to sending the email, the attacker had performed enough reconnaissance to uncover the name of an individual at a competing organization with whom the victim user had previously corresponded.

When the victim opened the attachment, a dropper malware was extracted and executed, installing the publicly available RAT known as GhOst to establish the attacker's foothold in the environment. The attacker leveraged this initial backdoor to move laterally throughout the environment, dropping other backdoors along the way. The attacker extracted password hashes from Active Directory, cracked some of the domain administrator account passwords, and cracked the local administrator account password. **The attacker then proceeded to move freely throughout the environment using legitimate credentials and a combination of "net use," scheduled tasks, and PsExec.**

This tool silently captured usernames and passwords of all users authenticating to the system.

Targeted attackers frequently use the C:\RECYCLER directory as a staging area for data theft because the contents of this directory are not visible to casual observers. Ultimately, the attacker succeeded in stealing over 50,000 files.

UNIVERSITY OF Southampton

1 POSTURING STEPS

Consider these activities prior to beginning remediation of an incident.

- Enable comprehensive logging of DNS, DHCP, VPN, and Windows security events
- Increase password complexity
- Reduce cached credential storage
- Disable the use of LANMAN hashes
- Implement aggressive patch management
- Develop end-user security training

2 REMEDIATION EVENT

Consider these activities to aggressively remove the attacker's access to your network.

- Pull entire enterprise off of the internet until the remediation event steps are completed
- Block known attacker C2 domains and IP addresses
- Block dynamic DNS providers
- Change all compromised passwords (if Active Directory has been compromised, this means changing all Active Directory passwords)
- Rebuild or replacing systems on which the attacker has installed malware or utilities
- Deny "uncategorized" web traffic at web proxy
- Reconnect environment to the internet
- Validate that key applications are working appropriately

3 STRATEGIC PLANNING

Consider these activities to ensure long-term success combatting targeted threats.

Improve Network Architecture

- Document and understand critical applications' network data flows
- Periodically validate network device rulesets
- Implement network segmentation
- Implement web application firewalls to reduce the risk of web application vulnerabilities
- Implement web proxies for all users, restricting access to "uncategorized" web sites
- Build restricted, high security zones for critical data and applications

Create Investigation-Ready Environment

- Create inventory of systems that store sensitive data and designate a business and IT point of contact for each
- Define the IR team's structure and responsibilities
- Define an IR plan
- Aggregate log sources into a SIEM tool
- Record and preserve logs for at least one year
- Tune host-and network-based intrusion prevention systems to alert on anomalies that indicate potential attacker activity
- Augment monitoring mechanisms with a threat-based monitoring service
- Conduct tabletop exercises to test the IR plan

Enhance Authentication and Authorization

- Upgrade workstations to Windows 7 which implements User Account Control
- Remove local administrator rights from the majority of users
- Reduce the number of privileged domain-wide service accounts
- Implement a set of accounts designed for use during an incident response. These accounts are normally disabled
- Implement multi-factor authentication

Invest in People

- Build or outsource a dedicated security team
- Structure roles to provide the team time to focus on investigating suspicious events on a daily basis

4 GOING FORWARD

Enact immediate containment measures at first sign the attackers have regained access.

more trends (2013)

1 **OUTSIDE IN**

Attackers are increasingly using outsourced service providers as a means to gain access to their victims.

2 **"X" MARKS THE SPOT**

Attackers are using comprehensive network reconnaissance to help them navigate victims' networks faster and more effectively.

3 **ONCE A TARGET ALWAYS A TARGET**

Advanced Persistent Threat (APT) attackers[1] continue to target industries that are strategic to their growth including aerospace, computer software, high-tech manufacturing, and energy.

4 **OLD SCHOOL DRIVE-BYS WITH A TWIST**

Targeted attackers are adapting Internet drive-by attacks and stepping them up a notch to compromise victims and gain a foothold in their networks.

Advanced attack groups are increasingly taking advantage of outsourcing relationships to gain access to the organizations they are targeting.

Attackers can steal data faster when they know what the want

Observable relationship between strategic priorities of some states, their state-owned enterprises, and data stolen thru cyber intrusion

Attackers shift from spear phishing attacks to exploits on websites used by targets, to install malware and gain access to systems

compromise via outsourced service prov

1

OUTSIDE IN

Attackers are increasingly using outsourced service providers as a means to gain access to their victims.

1 OSP has access to client network through site-to-site VPN tunnel. Limited access restrictions are in place.

Outsource Serivce Provider — Client Network

2 Attacker compromises OSP.

3 Attacker leverages site-to-site VPN tunnel and compromises client from OSP network.

THE TAKEAWAY Your network is only as secure as your outsourced service provider. Make sure your organization understands the security posture of these providers, and apply as stringent policies to their access as you would to your own employees.

items attackers steal for reconnaissance

UNIVERSITY OF Southampton

2

"X" MARKS THE SPOT

Attackers are using comprehensive network reconnaissance to help them navigate victims' networks faster and more effectively.

ITEM STOLEN	HOW THE ATTACKERS USE INFORMATION
 **Network Infrastructure Documentation Including Schematics and Configuration Files**	Understand firewall and other IDS configurations and where vulnerabilities that can be exploited exist.
 **Organization Chart**	Establish individuals to target in spear-phishing campaigns or to target for email and data theft.
 **Systems Documentation**	Identify where targeted systems existing within a victim network.
 **VPN Configuration Files**	Identify what VPN users have access to within a victim's network and target VPN credential data to steal.

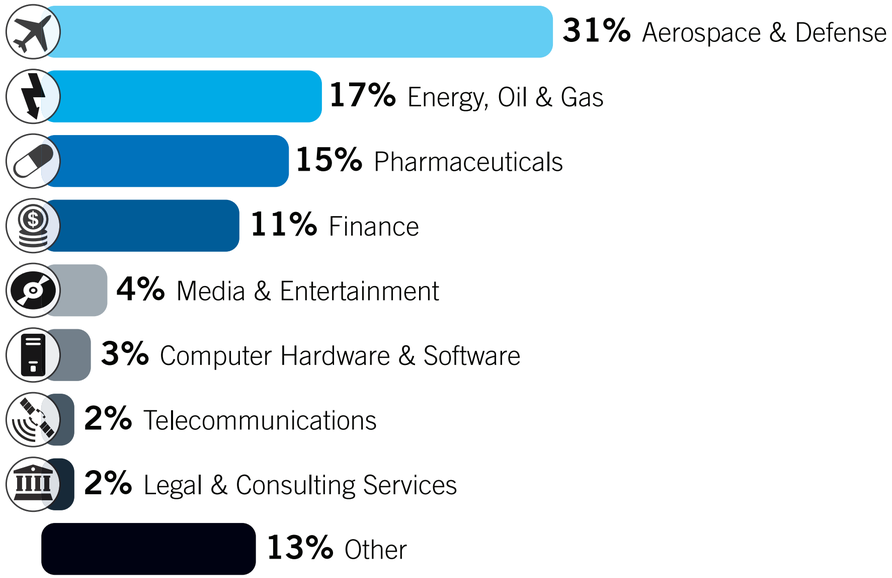
THE TAKEAWAY Information about your networks, systems, and organization provide a road map for attackers to quickly find what they are searching for. Apply the appropriate data classifications to such information and secure it accordingly.

repeated attacks by industry

3

ONCE A TARGET ALWAYS A TARGET

Advanced Persistent Threat (APT) attackers continue to target industries that are strategic to their growth including aerospace, computer software, high-tech manufacturing, and energy.



THE TAKEAWAY Attackers with an objective of economic espionage have specific goals and will return until their mission is complete. Treat incident detection and response as a consistent business process — not just something you do reactively. Constant vigilance and rapid response is necessary to keep an organization secure.

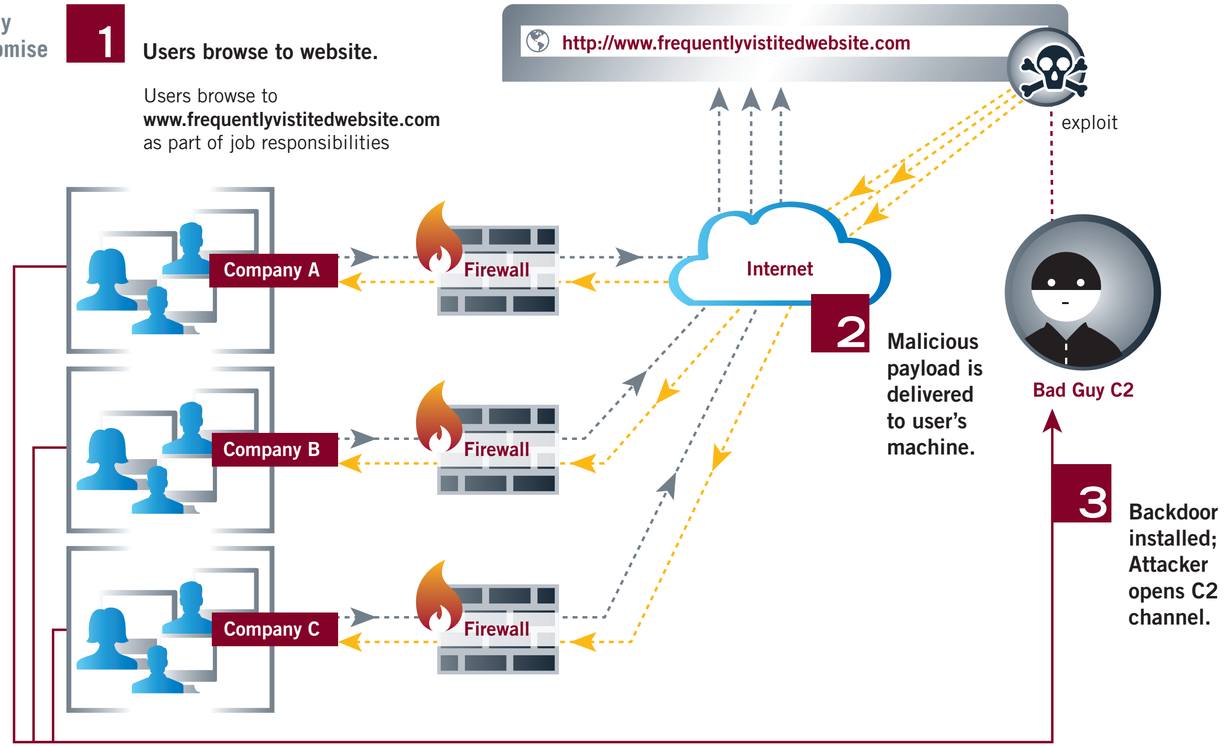
how strategic web compromise works

UNIVERSITY OF Southampton

4

OLD SCHOOL DRIVE-BYS WITH A TWIST

Targeted attackers are adapting Internet drive-by attacks and stepping them up a notch to compromise victims and gain a foothold in their networks.

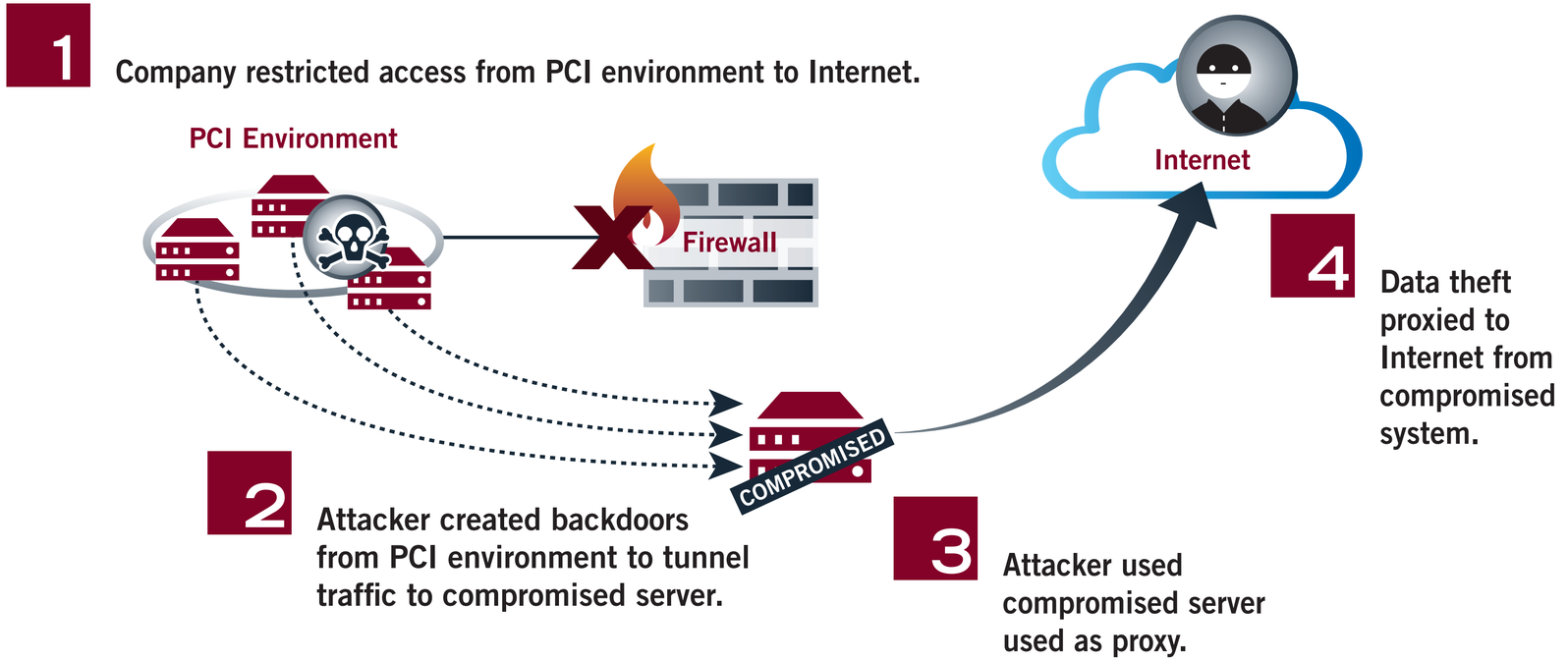


THE TAKEAWAY Advanced attackers are no longer relying solely on vulnerable Web applications and phishing emails to gain access to targeted companies. They are targeting individuals, conducting reconnaissance, and are willing to lie in wait while a user acts to compromise themselves. Ensure that your security operations incorporate data from intelligence services to identify when domains are compromised — and use this information to evaluate proxy or DNS logs for signs of access to these sites.

case study (4): global financial institution

The card processing environment restricted outbound Internet access for security.

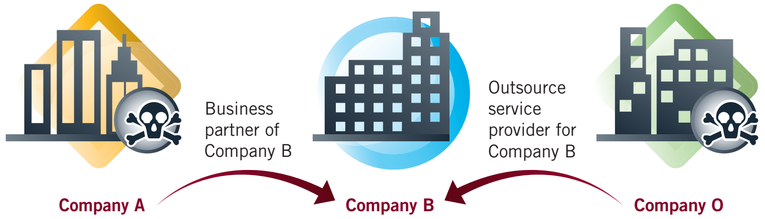
ATTACKER PLACED TUNNELING MALWARE ON COMPROMISED SERVER

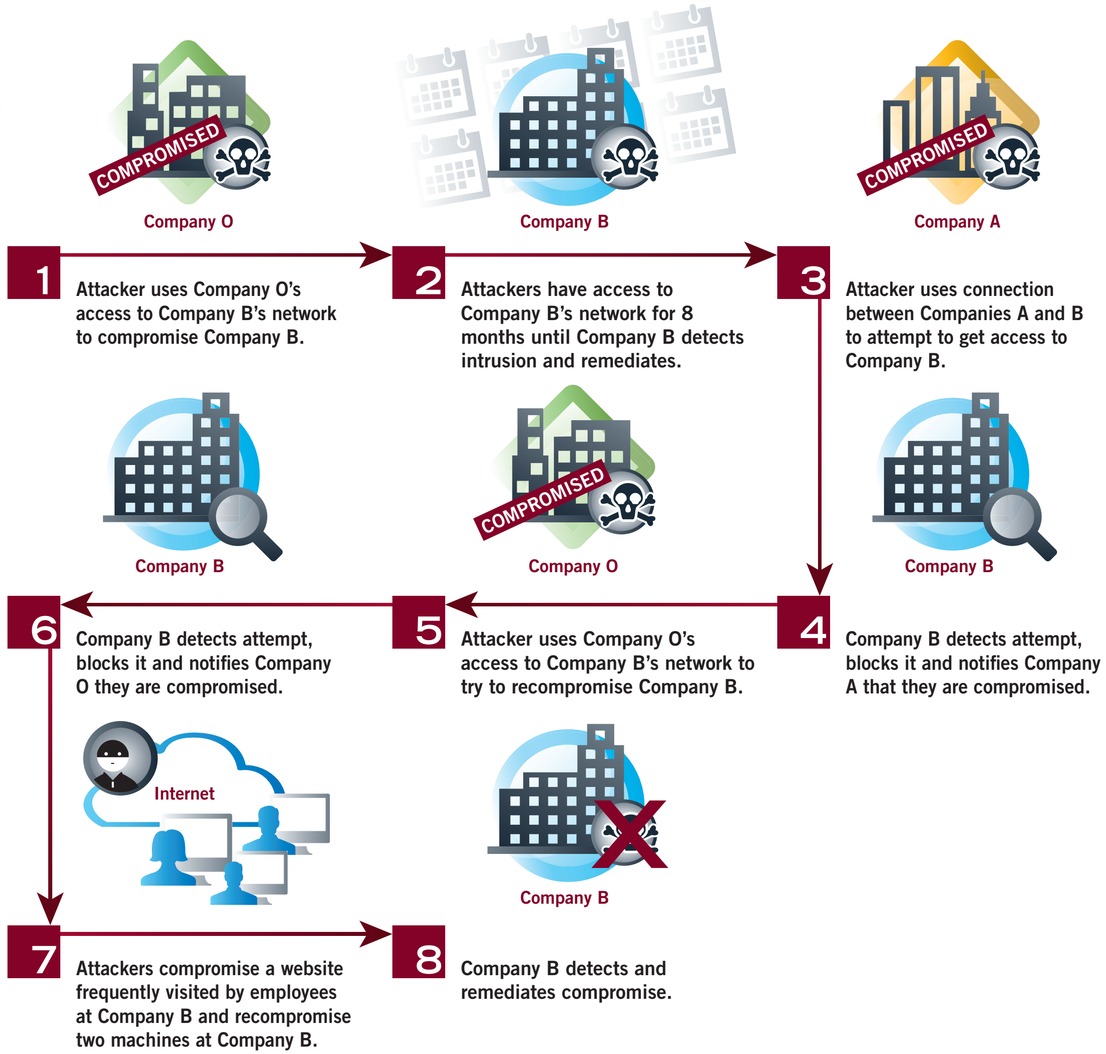


case study (5): energy company

RELATIONSHIPS

Attacker is at two places: Company A and Company O

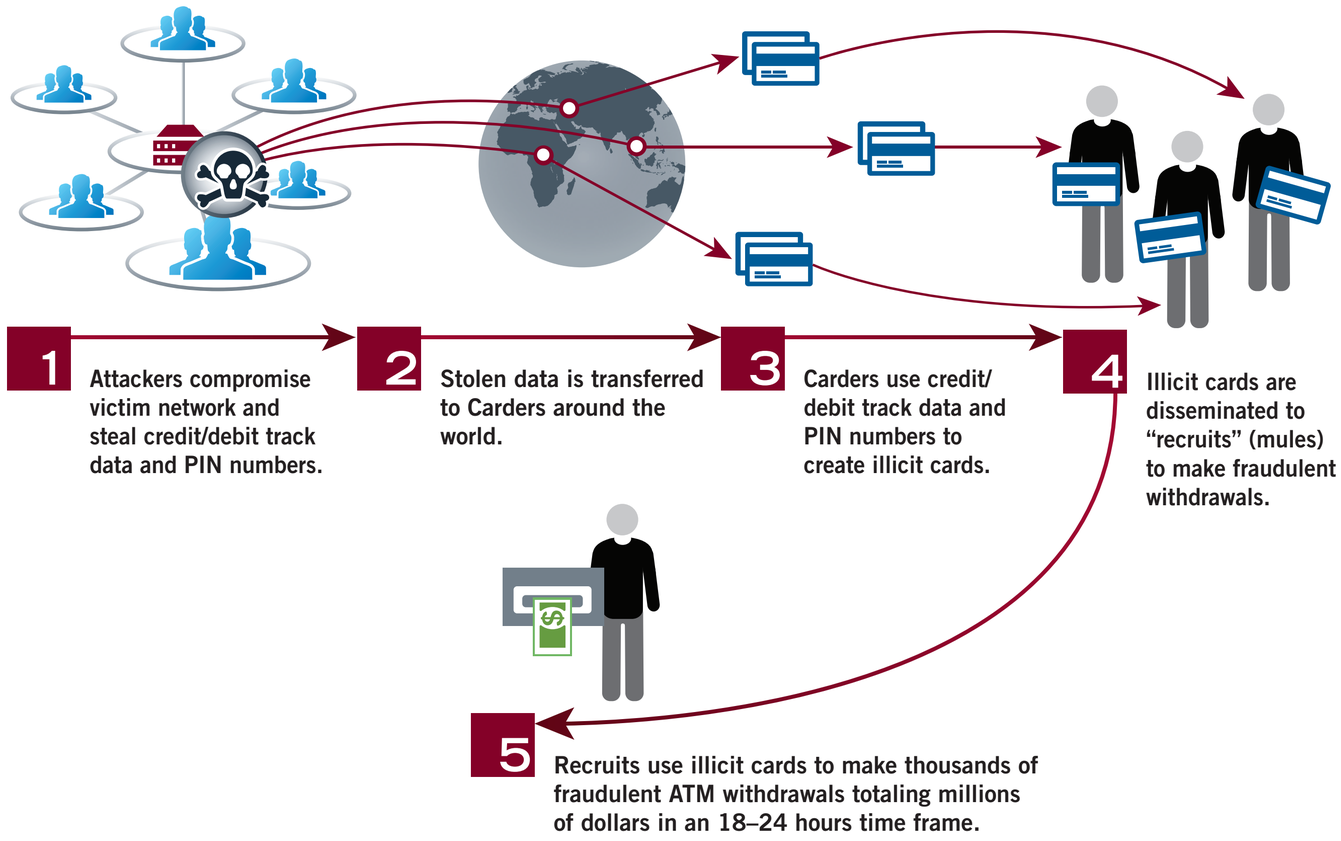




case study (6):banking industry

Compromise bank management application and use access to identify accounts with large sums; then disable two-factor authentication, reset password and access as legitimate users. You can then wire funds away or steal credit car/pin info to run a “money mule” op like below.

HOW A “MONEY MULE” INFRASTRUCTURE OPERATES



best practice for targeted organisation

1. employ dedicated “cyber incident” handler team — even if one person only!— whose full time job is to chase intruders.

2. equip the team with tools to collect and analyse network data.

3. understand that this is a daily job, count the number of incidents, measure the response time.

4. establish “incident team” partnership with other relevant organisations.