INFS 5115 Security Principles

Cyber Intrusions

University of South Australia

School of
Information Technology
and Mathematical Sciences

Cyber Intrusions

- In this seminar we will review the concept of cyber intrusions, including:
  - how they occur, based on real life case studies;
  - contemporary techniques used by adversaries; and
  - a brief discussion of mitigation strategies.

Cyber Intrusions

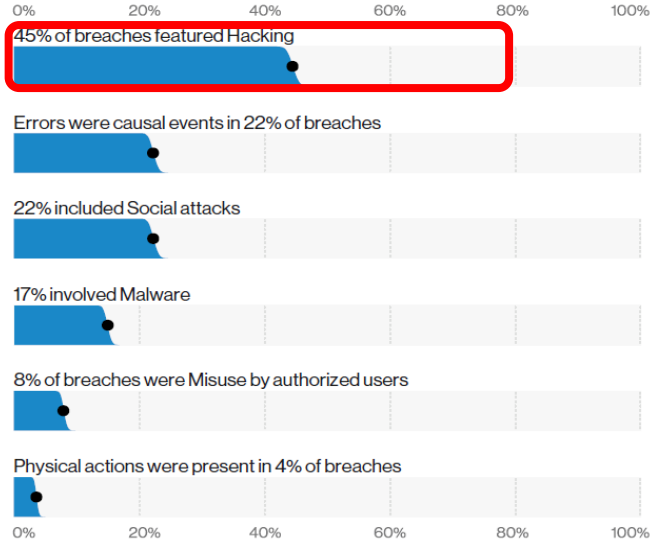
Definition

- *Intrusion*
  - *Unauthorised act of bypassing the security mechanisms of a system.*[1]

[1] CNSSI-4009 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

Verizon's Data Breach Investigations Report

Figure 2. What tactics are utilized? (Actions)



Verizon 2020, *2020 Data Breach Investigations Report*, Verizon, p. 7, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Cyber Intrusions

- The following slides outline a selection of actual cyber intrusions that have affected a range of organisations and industries.
- They serve as illustrative examples of the wide range of intrusions that occur on an ongoing basis.

Intrusion Case Study 1

Source: Australian Broadcasting Corporation 2016, 'Bureau of Meteorology target of 2015 cyber attack, Prime Minister Malcolm Turnbull confirms, http://www.abc.net.au/news/2016-04-21/australia-admits-it-can-launch-cyber-attacks-turnbull/7343620

University of South Australia
School of Information Technology and Mathematical Sciences

ABC NEWS

Just In | Australia | World | Business | Sport | Science | Arts | Analysis | Fact Chec

Print | Email | Facebook | Twitter | More

Bureau of Meteorology target of 2015 cyber attack, Prime Minister Malcolm Turnbull confirms

By political editor Chris Uhlmann

Updated 21 Apr 2016, 2:08pm

The Federal Government has confirmed for the first time the Bureau of Meteorology was the target of a cyber attack.

Last year, the ABC uncovered a state-based intrusion into the Bureau of Meteorology that infected its entire computer network.

The threat is persistent, aimed at stealing information, and will cost hundreds of millions of dollars to fix.

The bureau has a direct link to the Defence Department and officials have told the ABC they believe the attack was launched from China.

Prime Minister Malcolm Turnbull today confirmed the attack.

"I can confirm reports that the Bureau of Meteorology suffered a significant cyber intrusion which was first discovered early last year, and the Department of Parliamentary Services suffered a similar intrusion in recent years," he said.

"Those organisations have worked hard with the experts at the Australian Cyber Security Centre to understand and fix the vulnerabilities."

PHOTO: Malcolm Turnbull walks through a door replicating the Tardis, from Dr. Who, after holding a press conference about the Federal Government's Cyber Security. (AAP: Dean Lewins)

RELATED STORY: China blamed for 'massive' cyber attack on BoM computer

Case Study 1

Government

- A 2015 attack on the Australian Bureau of Meteorology (BoM) was widely reported by the media.
- The ACSC 2016 threat report provides an overview of the event.
- Suspicious activity was initially detected by the Australian Signals Directorate (ASD).
- The ASD located a type of remote access malware commonly associated with state-sponsored adversaries.
- They also detected other malware associated with cybercrime.

Australian Cyber Security Centre 2016, ACSC Threat Report, Commonwealth of Australia. p. 11.

Case Study 1

Government

- The ASD determined that the adversary was attempting to locate and exfiltrate documents from the BoM.
- They recovered a ‘password dumping utility’ and determined that at least one *domain administrator* account had been used maliciously.
- The adversary attempted to access at least six additional hosts, including *domain controllers* and *file servers*.
- These facts suggested that all passwords on the BoM network were compromised by the time of the investigation.

Australian Cyber Security Centre 2016, ACSC Threat Report, Commonwealth of Australia. p. 11.

Case Study 1

Government

- Evidence suggesting the use of network scanning and time stamp modification tools was also identified.
- These tools may have been used to map the network and hide the adversary's tracks.
- The ACSC attributed the primary compromise to a foreign intelligence service.
- However, the security controls were insufficient to protect the network against even more common cybercrime.

Australian Cyber Security Centre 2016, ACSC Threat Report, Commonwealth of Australia. p. 11.

The Essential Eight

- The ACSC report recommends the implementation of security controls as outlined in *ASD's Strategies to Mitigate Cyber Security Incidents*.
- These include the '*Essential Eight*':
  - *Application control/whitelisting*
  - *Configure Microsoft Office macro settings*
  - *Daily backups*
  - *Multi-factor authentication*
  - *Patch applications*
  - *Patch operating systems*
  - *Restrict administrative privileges*
  - *User application hardening*

Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents', https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents, viewed 24/03/2021
Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents', https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model , viewed 24/03/2021

Strategies to Mitigate Cyber Security Incidents

UPDATED FEBRUARY 2017
First published February 2010

Suggested Mitigation Strategy Implementation Order
(start with the threats of most concern to the organisation)

Targeted cyber intrusions (advanced persistent threats) and other external adversaries who steal data:

1. Implement "essential" mitigation strategies to:
   a. prevent malware delivery and execution
   b. limit the extent of cyber security incidents
   c. detect cyber security incidents and respond.
2. Repeat step 1 with "excellent" mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Ransomware and external adversaries who destroy data and prevent computers/networks from functioning:

1. Implement "essential" mitigation strategies to:
   a. recover data and system availability
   b. prevent malware delivery and execution
   c. limit the extent of cyber security incidents
   d. detect cyber security incidents and respond.
2. Repeat step 1 with "excellent" mitigation strategies.
3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note that 'Hunt to discover incidents' is less relevant for ransomware that immediately makes itself visible.

Malicious insiders who steal data:

1. Implement 'Control removable storage media and connected devices' to mitigate data exfiltration.
2. Implement 'Outbound web and email data loss prevention'.
3. Implement "essential" mitigation strategies to:
   a. limit the extent of cyber security incidents
   b. detect cyber security incidents and respond.
4. Repeat step 3 with "excellent" mitigation strategies.
5. Implement 'Personnel management'.
6. If employees are likely to have hacking skills and tools, implement "essential" mitigation strategies to prevent malware delivery and execution, and repeat step 3 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note that technical mitigation strategies provide incomplete security since data could be photographed or otherwise copied from computer screens or printouts, or memorised and written down outside of the workplace.

Malicious insiders who destroy data and prevent computers/networks from functioning:

1. Implement "essential" mitigation strategies to:
   a. recover data and system availability
   b. limit the extent of cyber security incidents
   c. detect cyber security incidents and respond.
2. Repeat step 1 with "excellent" mitigation strategies.
3. Implement 'Personnel management'.
4. If employees are likely to have hacking skills and tools, implement "essential" mitigation strategies to prevent malware delivery and execution, and repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Relative Security Effectiveness Rating	Mitigation Strategy	Potential User Resistance	Upfront Cost (staff, equipment, technical complexity)	Ongoing Maintenance Cost (mainly staff)
Mitigation Strategies to Prevent Malware Delivery and Execution:				
Essential	**Application whitelisting** of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Medium	High	Medium
Essential	**Patch applications** e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with "extreme risk"[1] vulnerabilities within 48 hours. Use the latest version of applications.	Low	High	High
Essential	**Configure Microsoft Office macro settings** to block macros from the Internet, and only allow vetted macros either in "trusted locations" with limited write access or digitally signed with a trusted certificate.	Medium	Medium	Medium
Essential	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	Medium	Medium	Medium
Excellent	**Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is identified e.g. network traffic, new or modified files, or other system configuration changes.	Low	High	Medium
Excellent	**Email content filtering**. Whitelist allowed attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.	Medium	Medium	Medium
Excellent	**Web content filtering**. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.	Medium	Medium	Medium
Excellent	**Deny corporate computers direct Internet connectivity**. Use a gateway firewall to require use of a split DNS server, an email server, and an authenticated web proxy server for outbound web connections.	Medium	Medium	Low
Excellent	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Low	Low	Low
Very Good	**Server application hardening** especially Internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive/high-availability) data.	Low	Medium	Medium
Very Good	**Operating system hardening** (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD.	Medium	Medium	Low
Very Good	**Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.	Low	Low	Low
Very Good	**Control removable storage media and connected devices**. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G devices.	High	High	Medium
Very Good	**Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use "hard fail" SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain.	Low	Low	Low
Good	**User education**. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.	Medium	High	Medium
Limited	**Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.	Low	Low	Low
Limited	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.	Low	Low	Low
Mitigation Strategies to Limit the Extent of Cyber Security Incidents:				
Essential	**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	Medium	High	Medium
Essential	**Patch operating systems**. Patch/mitigate computers (including network devices) with "extreme risk"[1] vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.	Low	Medium	Medium
Essential	**Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.	Medium	High	Medium
Excellent	**Disable local administrator accounts** or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.	Low	Medium	Low
Excellent	**Network segmentation**. Deny traffic between computers unless required. Constrain devices with low assurance e.g. BYOD and IoT. Restrict access to network drives and data repositories based on user duties.	Low	High	Medium
Excellent	**Protect authentication credentials**. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Credential Guard. Change default passphrases. Require long complex passphrases.	Medium	Medium	Low
Very Good	**Non-persistent virtualised sandboxed environment**, denying access to important (sensitive/high-availability) data, for risky activities e.g. web browsing, and viewing untrusted Microsoft Office and PDF files.	Medium	Medium	Medium
Very Good	**Software-based application firewall, blocking incoming network traffic** that is malicious/unauthorised, and denying network traffic by default e.g. unneeded/unauthorised RDP and SMB/NetBIOS traffic.	Low	Medium	Medium
Very Good	**Software-based application firewall, blocking outgoing network traffic** that is not generated by approved/trusted programs, and denying network traffic by default.	Medium	Medium	Medium
Very Good	**Outbound web and email data loss prevention**. Block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words or data patterns.	Medium	Medium	Medium
Mitigation Strategies to Detect Cyber Security Incidents and Respond:				
Excellent	**Continuous incident detection and response** with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.	Low	Very High	Very High
Very Good	**Host-based intrusion detection/prevention system** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Low	Medium	Medium
Very Good	**Endpoint detection and response software** on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.	Low	Medium	Medium
Very Good	**Hunt to discover incidents** based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.	Low	Very High	Very High
Limited	**Network-based intrusion detection/prevention system** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Low	High	Medium
Limited	**Capture network traffic** to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.	Low	High	Medium
Mitigation Strategies to Recover Data and System Availability:				
Essential	**Daily backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	Low	High	High
Very Good	**Business continuity and disaster recovery plans** which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.	Low	High	Medium
Very Good	**System recovery capabilities** e.g. virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.	Low	High	Medium
Mitigation Strategy Specific to Preventing Malicious Insiders:				
Very Good	**Personnel management** e.g. ongoing vetting especially for users with privileged access, immediately disable all accounts of departing users, and remind users of their security obligations and penalties.	High	High	High

Activity 1

Suggest solutions to the BOM cyberattack

Using the Essential 8 suggest what solutions the BOM could implement on their network to prevent further attacks.

Case study 2: Background

Industrial Parts Manufacturer

- Verizon's 2016 Data Breach Digest outlines a scenario involving a US-based industrial parts manufacturer.

- The company believed there was a ‘possible’ breach of their payroll system, but was unable to find evidence.

- It appeared that for the last two payroll cycles, members of senior management had not received their payment via direct deposit.

Verizon 2016, ‘Data Breach Digest’, https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

Case study 2: Investigation

Industrial Parts Manufacturer

- The IT security team reviewed the HR payment database, interviewed payroll staff and reviewed firewall logs, but found no evidence of a breach.

- Verizon's investigation team asked questions to understand how employees accessed the payroll system.

Verizon 2016, 'Data Breach Digest', https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

Case study 2: Investigation

Industrial Parts Manufacturer

- The company used an HR portal that could be accessed via the internet, which authenticated users based on their Social Security Number and a six digit PIN.

- Further discussions revealed that the application was ten years old, the original developer had left some time ago and the system had not been updated or scanned for vulnerabilities.

Verizon 2016, 'Data Breach Digest', https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

Case study 2: Hypothesis

Industrial Parts Manufacturer

- The investigators suspected an *SQL injection* attack at this point.

Example:

Username: john **Password:** P@ssw0rd1

SELECT * FROM users WHERE username = 'john' AND password = 'P@ssw0rd1'

Username: admin' -- **Password:** foo

SELECT * FROM users WHERE username = 'admin' -- ' AND password = 'foo'

Verizon 2016, 'Data Breach Digest', https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

[1] Tracy, M, Jansen, W, Scarfone, K and Winograd, T 2007, 'Guidelines on Securing Public Web Servers', National Institute of Standards and Technology, SP 800-44, p. 6-9.

Case study 2: Findings

Industrial Parts Manufacturer

- A scan revealed that the HR website was vulnerable to SQL injection attacks.
- Apart from the logon system, a non-authenticated “help” form allowed employees to submit messages.
- The form was leveraged to interact with the database.
- Initially the attacks focused on mapping the underlying database and system.

Verizon 2016, ‘Data Breach Digest’, https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

Case study 2: Findings

Industrial Parts Manufacturer

- The attackers then manipulated the database to download additional tools via the internet.
- Once they had admin access to the database, they modified the direct deposit information for the executives they had identified as part of their initial reconnaissance.
- The IT security team were unable to locate the modified records as, after the payroll run was complete, the attackers would modify the deposit details back to their original values.

Verizon 2016, 'Data Breach Digest', https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

Case study 2: Actions

Industrial Parts Manufacturer

- The company decommissioned the HR platform and replaced it with a new, and internal only, product.
- This vulnerability was likely due to poor implementation of the technology, rather than a vulnerability in the database or web hosting software itself.
- Mitigation of these types of attacks involves secure software development practices, auditing of existing applications and improved incident detection capabilities.

Verizon 2016, 'Data Breach Digest', https://www.maritimecyprus.com/wp-content/uploads/2016/03/verizon_data-breach-digest_en-1.pdf

Advanced Persistent Threats

Definition

- APT's are defined by Tankard as "*a new breed of insidious threats that use **multiple attack techniques and vectors** and that are conducted by **stealth** to **avoid detection** so that hackers can **retain control** over target systems **unnoticed** for **long periods of time***"[1].

[1] Tankard, C 2011 'Advanced Persistent threats and how to monitor and deter them', Network Security, vol. 2011, no. 8, p. 16.

Advanced Persistent Threats

- Tankard outlines the ‘Operation Aurora’ APT (one of the first), which involved[1]:
  - Advanced social engineering
  - Malicious JavaScript code which exploited a zero-day vulnerability in Internet Explorer
  - Several types of malware
  - Encryption to obfuscate the attacker’s actions
  - Communication with Command and Control servers over TCP 443
  - ‘Pivoting’ to explore protected intranets for IP and other vulnerabilities

[1] Tankard, C 2011 'Advanced Persistent threats and how to monitor and deter them', Network Security, vol. 2011, no. 8, pp. 16-17.

Advanced Persistent Threats

Identification

- Brewer describes techniques for identifying the existence of an APT within a network.
- This is achieved by reviewing the log and audit trails for each of the five phases Brewer outlines in the APT lifecycle:
  - Reconnaissance
    - Firewall port scanning logs.
    - Adding IPs to watch lists if they meet certain criteria.
    - Real time analytics should be used, including rules to detect internal reconnaissance.

Brewer, R 2014, 'Advanced persistent threats: minimising the damage', Network Security, vol. 2014, no. 4, pp. 5-9.

Advanced Persistent Threats

- Compromise
  - Spear phishing campaign logs (e.g. email, IDS, AV, processes crashing).
  - Behavioural anomaly detection to determine if traffic is abnormal.
- Maintaining access
  - Use suspicious IP watchlist to detect potential RATs (remote access toolkits).
  - Behavioural analytics for user web browsing activity.
- Lateral movement
  - Check for credentials being used in two separate geographic locations simultaneously.

Brewer, R 2014, 'Advanced persistent threats: minimising the damage', Network Security, vol. 2014, no. 4, pp. 5-9.

Advanced Persistent Threats

- Data exfiltration
  - Behavioural anomaly detection that identifies any network activity that deviates from the normal for further examination.
  - For example, a normal workstation that suddenly starts sending substantial data to a single IP address on a regular basis could be considered suspicious.
  - Analysis of web traffic can also help to detect stenographic techniques.

Brewer, R 2014, 'Advanced persistent threats: minimising the damage', Network Security, vol. 2014, no. 4, pp. 5-9.

Case study 3

- In 2011 RSA, a well known cybersecurity technology company and developer of SecurID two-factor authentication tokens, was the victim of a cyberattack.
- They describe the attack in a blog post entitled ‘Anatomy of an Attack’, summarised in the following slides.
- They identify the attack as being conducted by an ‘advanced persistent threat’, commonly known as an APT.

RSA FraudAction Research Labs 2011, ‘Anatomy of an Attack’, https://blogs.rsa.com/anatomy-of-an-attack/

Case study 3

- In the RSA case, the attacker sent two different phishing emails over two days.
- The targets were two small groups of employees, with nothing obviously high profile or high value about the targets.
- The email subject was “2011 Recruitment Plan”, and one of the spearphishing victims opened the attached Excel spreadsheet.
- The spreadsheet contained a zero day Adobe Flash vulnerability and the attacker used the vulnerability to install a RAT.

RSA FraudAction Research Labs 2011, ‘Anatomy of an Attack’, https://blogs.rsa.com/anatomy-of-an-attack/

Case study 3

- The attacker then collected credentials from the compromised users (including user, domain admin and service accounts).
- They escalated their privileges within non-admin users and targeted more valuable users such as process experts and server admins.
- The attacker accessed servers of interest, moved data to internal staging servers where it was aggregated, compressed and encrypted ready for exfiltration.
- FTP was used to transfer encrypted RAR files from the staging server to an outside compromised machine used as an external staging server.

RSA FraudAction Research Labs 2011, ‘Anatomy of an Attack’, https://blogs.rsa.com/anatomy-of-an-attack/

Case study 3

- This case study shows that even organisations who specialise in IT security can be affected by advanced persistent threats.

- RSA note that they did detect the attack while it was occurring, which may have substantially limited the scope of the attack, in comparison to the traditional operation of APTs, where the attacker tries to remain stealthy for as long as possible.

RSA FraudAction Research Labs 2011, 'Anatomy of an Attack', https://blogs.rsa.com/anatomy-of-an-attack/

Case study 4

IT Security Industry

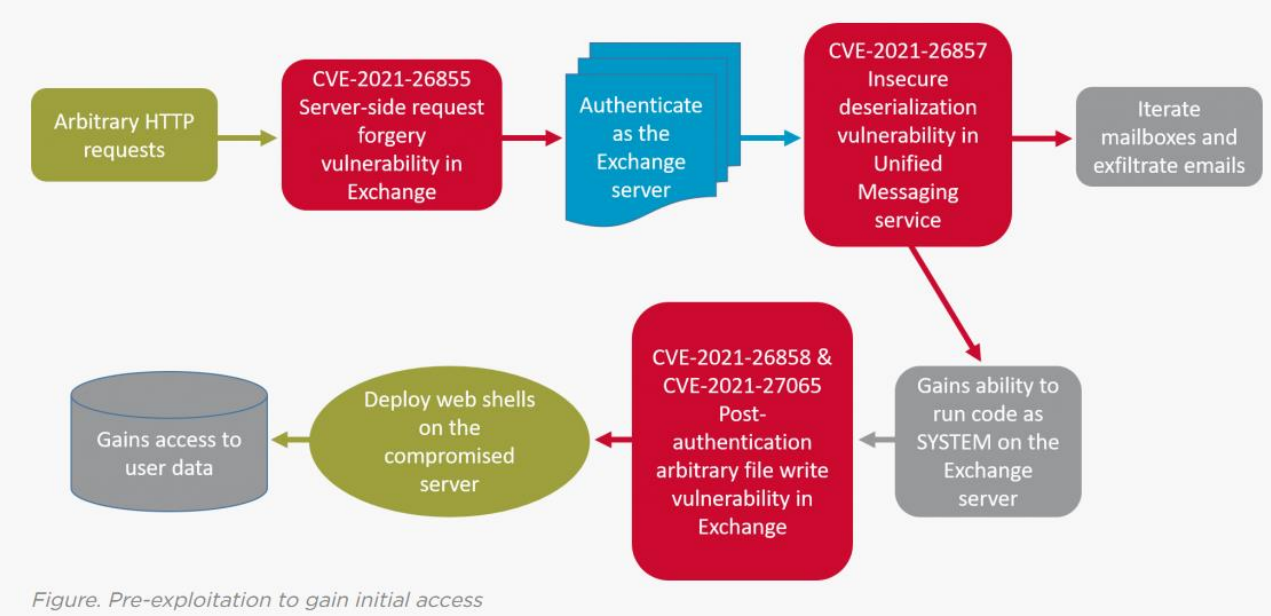


Figure. Pre-exploitation to gain initial access

Symantec Enterprise Blogs, 'How Symantec Stops Microsoft Exchange Server Attacks', https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/microsoft-exchange-server-protection viewed 27/03/2021

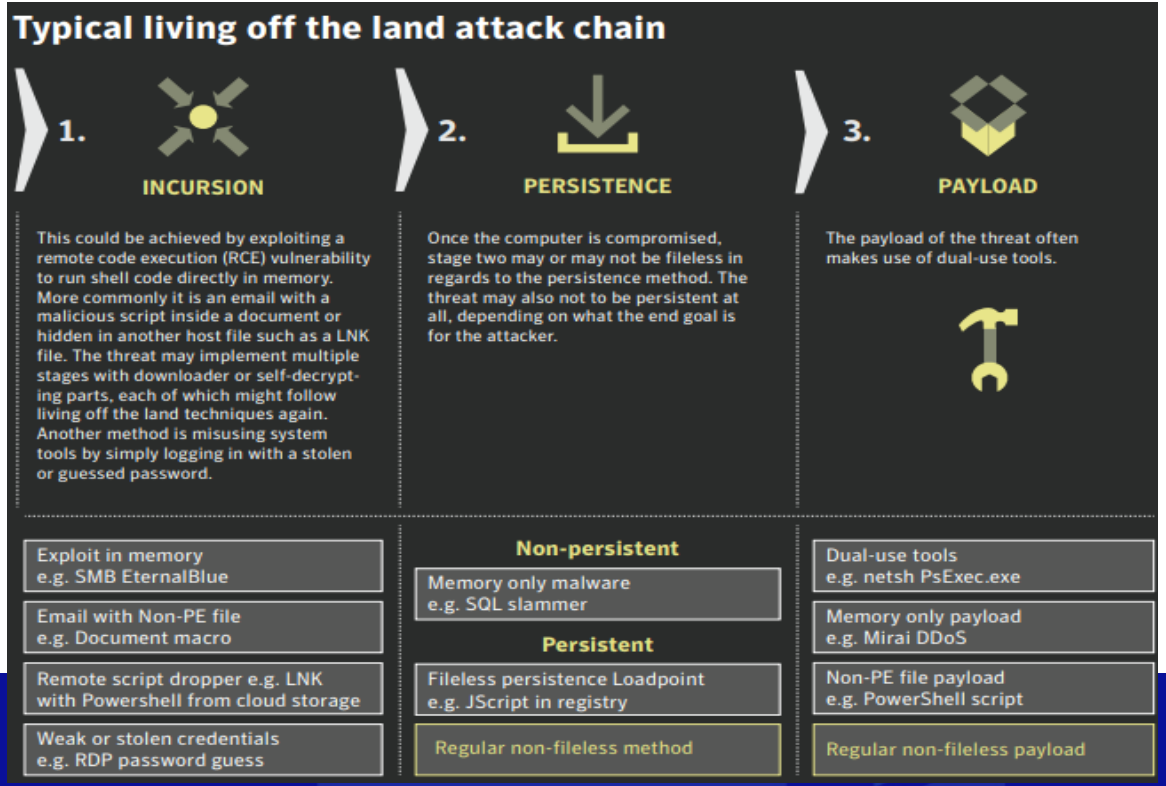
Cyber Intrusions

- In 2017, Symantec released a threat report to describe the trend of attackers ‘living off the land’ when conducting contemporary cyber intrusions.
- Living off the land describes the use of preinstalled and/or trusted off-the-shelf tools (generally used for system administration) being used as part of cyber attacks.
- This change in attacker behaviour may be due in part to increased difficulty in locating and successfully exploiting zero day vulnerabilities.

Wueest, C and Anand, H 2017, ‘Living off the land and fileless attack techniques’, Symantec Internet Security Threat Report, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf

Cyber Intrusions

Trends



Wueest, C and Anand, H 2017, 'Living off the land and fileless attack techniques', Symantec Internet Security Threat Report, p. 8.

Cyber Intrusions

- The ACSC July 2019 to June 2020 Threat Report indicates an increase scale, sophistication and frequency of malicious cyber activity[1].
- Ransomware has become one of the most significant threats to business operations and government.

- The 2020 Verizon Data Breach Investigations Report also highlights that attacks on cloud-based data are on the increase[2].

[1] Australian Cyber Security Centre July 2019 – June 2020, ACSC Threat Report, Commonwealth of Australia.
[2]Verizon 2020, *2020 Data Breach Investigations Report*, Verizon, p. 7, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Cyber Intrusions

- Adversaries will continue to adapt to bypass traditional security defence techniques.

- Organisations will need to ensure that they maintain cybersecurity best practices, and continue to evolve these practices, as adversary methodologies change.