Anatomy of a Breach: Identifying Potential Hazard Points in your Security Platform

Dustin McCreight and Lenny Zeltser
NCR Corporation

Modern cyber-adversaries are professionals with financial objectives and specialized expertise.

Many have teammates and managers.

Consider your environment. How might someone attack it? What weaknesses would they target?

Learn from your experience and public breach details. Find the paths of least resistance.

Remote Access

Intruders can steal logon credentials using phishing techniques. They trick people into revealing usernames and passwords.

It can be hard to tell whether an email about your password or service is legitimate.

More at: PhishLabs, Phishing Trends & Intelligence Report

Attackers often misuse legitimate remote access tools to log into targeted systems.

Attackers took advantage of password reuse to access LogMeIn, TeamViewer, VNC, etc.

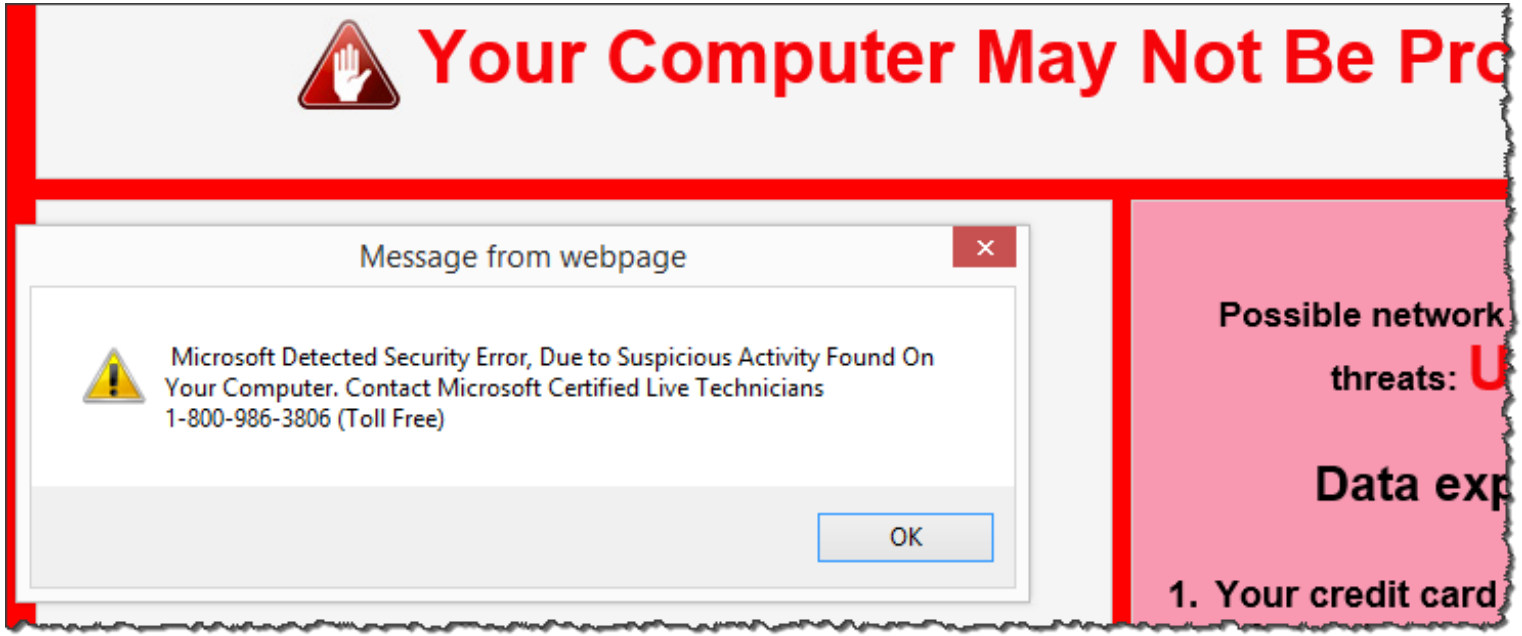
More at: LogMeIn, Password Reuse Issue Affecting Some LogMeIn Users
More at: TeamViewer, Statement on Potential TeamViewer Hackers

Attackers also brute-force logon credentials of legitimate users.

People often select common, easy-to-guess passwords and recovery questions.

More at: IW3C2, Secrets, Lies, and Account Recovery
More at: The Guardian, Passwords are not broken, but how we choose them sure is

People are sometimes social-engineered to grant unauthorized remote access.



More at: SANS, Who Develops Code for IT Support Scareware Websites?

Safeguards for Remote Access

Restrict

Restrict who can access what in your environment

Authenticate

Employ two-factor authentication

Review

Log and review access to detect misuse

Exploits

Exploit kits planted on compromised web servers target visitors to infect internal systems.

These are commercial attack tools, which are sometimes sold “as a service.”

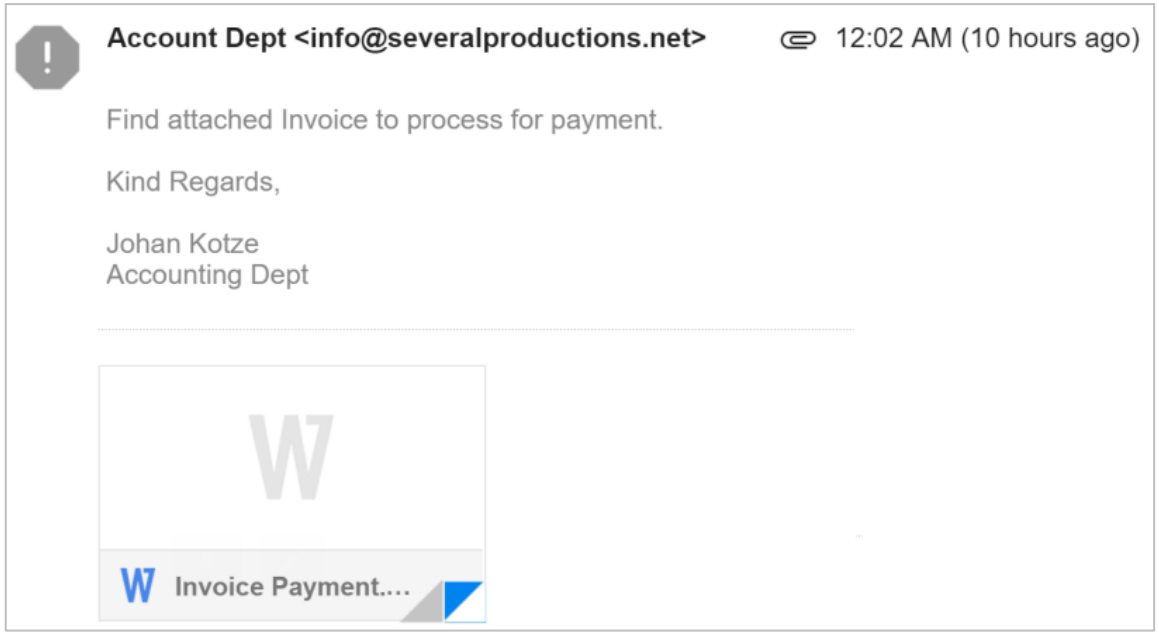
More at: Checkpoint, Inside Nuclear’s Core

Sometimes systems are attacked using malicious banner ads.

This means the infection might occur even after visiting a trusted website.

More at: Bromium, Endpoint Exploitation Trends

Attackers can also deliver exploits in the form of malicious document attachments to email.



More at: Sophos, The Rise of Document-based Malware

Client-side software vulnerabilities are gateways into the employee's system.

Though zero-day threats are possible, patches are often available for targeted vulnerabilities.

More at: Trend Micro, Evolution of Exploit Kits

Safeguards for Exploits

Web

Web activity oversight

Files

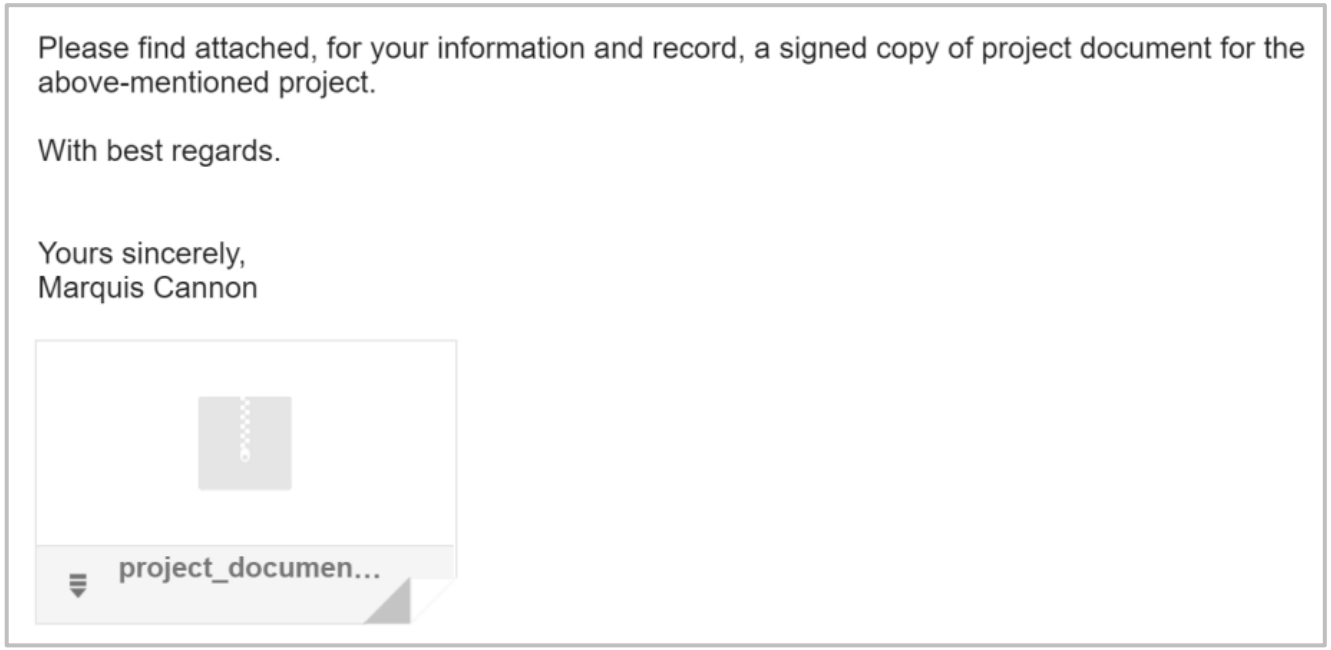
Scrutinize email attachments and downloads

Patch

Patch client-side vulnerabilities

Malware

Malicious software often spreads via exploits and can also arrive as an email attachment.



More at: US-CERT, Using Caution with Email Attachments

Malware can take the form of a keylogger to obtain credentials for accessing other systems.

For instance, PoSeidon deleted cached LogMeIn credentials to force users to retype them, so it could capture them.

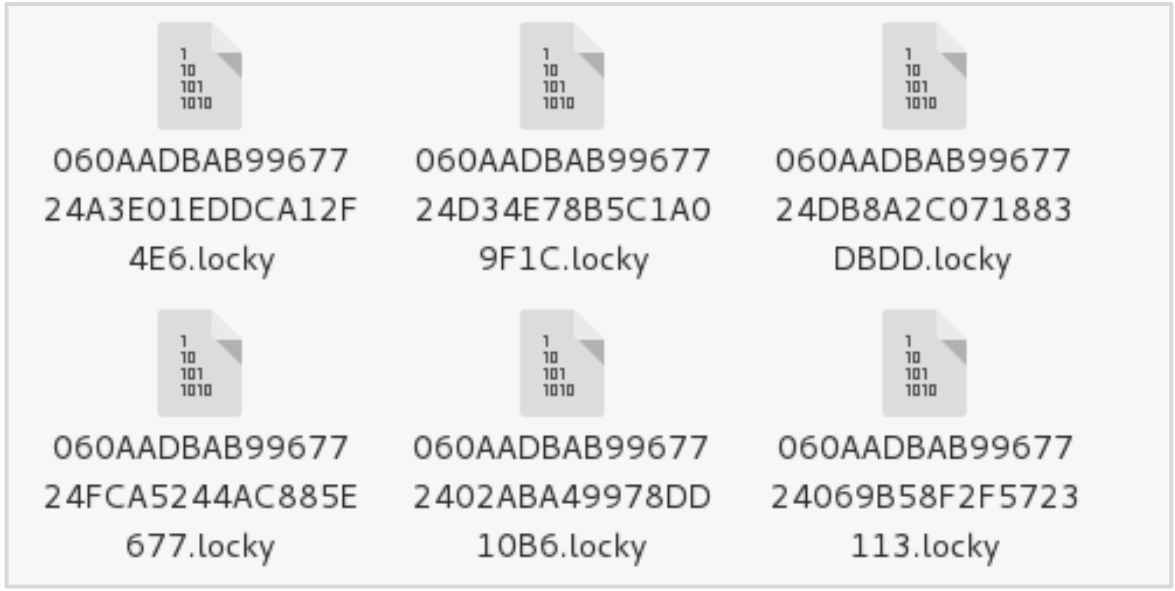
More at: Cisco, PoSeidon - A Deep Dive Into Point of Sale Malware

Attackers can use malware for remote access, memory scraping, webcam spying, etc.

```
*(_DWORD *)off_40708C = sub_40349C(&v7, "StartVNC");
*(_DWORD *)off_40707C = sub_40349C(&v7, "StopVNC");
*(_DWORD *)off_407084 = sub_40349C(&v7, "StartWebcam");
*(_DWORD *)off_407070 = sub_40349C(&v7, "StopWebcam");
*(_DWORD *)off_40709C = sub_40349C(&v7, "DeleteKeylog");
*(_DWORD *)off_407078 = sub_40349C(&v7, "GetKeylog");
*(_DWORD *)off_40705C = sub_40349C(&v7, "StopKeylog");
*(_DWORD *)off_40704C = sub_40349C(&v7, "QueryScreen");
```

More at: TrendLabs, NewPosThings Has New PoS Things

Ransomware has become a major threat to business operations.



More at: US-CERT, Ransomware and Recent Variants

Safeguards for Malware

Antivirus

Modern, up-to-date antivirus as the baseline

Whitelisting

Application whitelisting for comprehensive control

Network

Malware scanning at the network, not just the endpoint

Network

An infected system on one of your networks could offer access to a more sensitive network.

Adversaries might infect a corporate workstation and use it to target your retail environment.

More at: NCR, Segment Your Network to Protect Data

Attackers could access your environment by going through your vendors or suppliers.

It can be hard to control security of third parties that need to have access to your network.

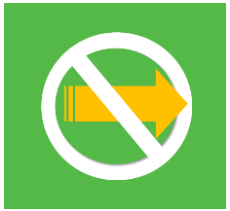
More at: Forbes, Digital Supply Chain Security

Stolen data can be transmitted out of your environment using the open protocols you allow.

Outbound HTTP, HTTPS and even DNS traffic can be used for such exfiltration.

More at: TrendMicro, Data Exfiltration in Targeted Attacks

Safeguards for Network

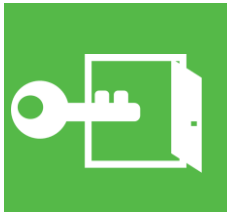


Outbound

Restrict access to specific destinations & protocols

Segment

Segment internal network to dampen attackers' movement



Third Parties

Control access to your environment from third parties

How do you address these threat vectors?

Remote Access	Exploits	Malware	Network
▪ Access restrictions ▪ Two-factor authentication ▪ Activity logging and review	▪ Web activity oversight ▪ Downloads and attachments ▪ Software patching	▪ Modern and up-to-date antivirus ▪ Application whitelisting ▪ Network-based malware scans	▪ Outbound restrictions ▪ Internal segmentation ▪ 3rd-party access controls

Keep learning about attack trends.

- PhishLabs, Phishing Trends & Intelligence Report
  https://info.phishlabs.com/pti-report-download
- More at: LogMeIn, Password Reuse Issue Affecting Some LogMeIn Users
  https://blog.logmeininc.com/password-reuse-issue-affecting-logmein-users
- TeamViewer, Statement on Potential TeamViewer Hackers
  https://www.teamviewer.com/en/company/press/statement-on-potential-teamviewer-hackers
- IW3C2, Secrets, Lies, and Account Recovery
  http://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43783.pdf
- The Guardian, Passwords are not broken, but how we choose them sure is
  https://www.schneier.com/essays/archives/2008/11/passwords_are_not_br.html
- SANS, Who Develops Code for IT Support Scareware Websites?
  https://isc.sans.edu/forums/diary/Who+Develops+Code+for+IT+Support+Scareware+Websites/19489
- Checkpoint, Inside Nuclear's Core
  https://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf
- Bromium, Endpoint Exploitation Trends
  https://www.bromium.com/sites/default/files/rpt-bromium-threat-report-2015-us-en.pdf

Keep learning about attack trends. (2)

- Sophos, The Rise of Document-based Malware
  https://www.sophos.com/en-us/security-news-trends/security-trends/the-rise-of-document-based-malware.aspx
- Trend Micro, Evolution of Exploit Kits
  https://trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf
- US-CERT, Using Caution with Email Attachments
  https://www.us-cert.gov/ncas/tips/ST04-010
- Cisco, PoSeidon - A Deep Dive Into Point of Sale Malware
  http://blogs.cisco.com/security/talos/poseidon
- TrendLabs, NewPosThings Has New PoS Things
  http://blog.trendmicro.com/trendlabs-security-intelligence/newposthings-has-new-pos-things
- US-CERT, Ransomware and Recent Variants
  https://www.us-cert.gov/ncas/alerts/TA16-091A
- NCR, Segment Your Network to Protect Data
  http://www.ncr.com/company/blogs/hospitality/segment-network-protect-data-avoid-inconvenience
- Forbes, Digital Supply Chain Security
  http://www.forbes.com/sites/davelewis/2014/07/30/digital-supply-chain-security-partner-networks
- TrendMicro, Data Exfiltration in Targeted Attacks
  http://blog.trendmicro.com/trendlabs-security-intelligence/data-exfiltration-in-targeted-attacks/

SYNERGY 2016
EXPERIENCE 2020

Thank you

Please remember to take the brief session survey in the mobile app.
Your feedback is very valuable to us!

Check-in on the Synergy app to earn points!

0115