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

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

<table>
<thead>
<tr>
<th></th>
<th>Web</th>
<th>Files</th>
<th>Patch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Web activity oversight</td>
<td>Scrutinize email attachments and downloads</td>
<td>Patch client-side vulnerabilities</td>
</tr>
</tbody>
</table>
Malware
Malicious software often spreads via exploits and can also arrive as an email attachment.

Please find attached, for your information and record, a signed copy of project document for the above-mentioned project.

With best regards.

Yours sincerely,
Marquis Cannon

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.

```c
*(_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

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>Restrict access to specific destinations &amp; protocols</td>
</tr>
<tr>
<td>Segment</td>
<td>Segment internal network to dampen attackers’ movement</td>
</tr>
<tr>
<td>Third Parties</td>
<td>Control access to your environment from third parties</td>
</tr>
</tbody>
</table>
How do you address these threat vectors?

<table>
<thead>
<tr>
<th>Remote Access</th>
<th>Exploits</th>
<th>Malware</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Access restrictions</td>
<td>- Web activity oversight</td>
<td>- Modern and up-to-date antivirus</td>
<td>- Outbound restrictions</td>
</tr>
<tr>
<td>- Two-factor authentication</td>
<td>- Downloads and attachments</td>
<td>- Application whitelisting</td>
<td>- Internal segmentation</td>
</tr>
<tr>
<td>- Activity logging and review</td>
<td>- Software patching</td>
<td>- Network-based malware scans</td>
<td>- 3rd-party access controls</td>
</tr>
</tbody>
</table>


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

- IW3C2, Secrets, Lies, and Account Recovery

- 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?

- Checkpoint, Inside Nuclear’s Core

- Bromium, Endpoint Exploitation Trends
Keep learning about attack trends. (2)


- Trend Micro, Evolution of Exploit Kits

- 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

- 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

- Forbes, Digital Supply Chain Security

- TrendMicro, Data Exfiltration in Targeted Attacks
Thank you

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

Dustin McCreight
Product Manager
Network & Security Services
14770 Trinity Blvd
Fort Worth, TX 76155
dustin.mccreight@ncr.com

Lenny Zeltser
Director, Product Management
Network & Security Services
250 Greenwich St
New York, NY 10007
lenny.zeltser@ncr.com