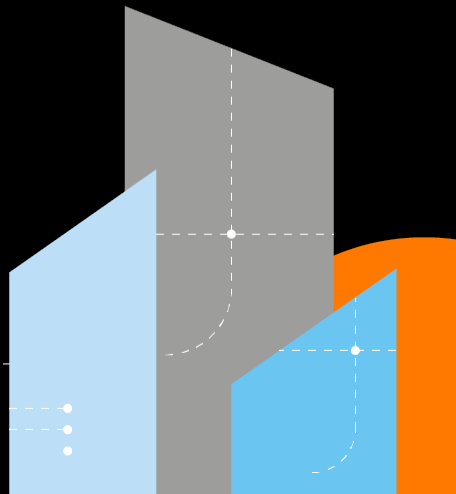
Orange
Cyberdefense

Incident Response – War Stories and Learnings

Bjørn Sverre Svendsen / Hampus Glantz

Malmö 18.04.2023



Our CSIRT, part of the Orange Cyberdefense CERT

- Operating since 2003
- Collaborating with Orange internal CERT
- 300+ incident response missions in 2022

- 105+ experts globally in the CERT
- CSIRT team available 24x7 with 25+ incident responders, dispersed geographically across Europe
- A wide range of skills and years of experience
- Member of industry-recognised bodies for CERT activities including CREST, TF-CSIRT, FIRST, …
- Partnerships established with vendors / editors, access to private lists, specific communication channels with police and intelligence departments all over the world, specific agreements with internet and Security global organizations (Verisign, Public Internet Registry, ICANN,…)

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CREST
PHISHING INITIATIVE France
VISA DE SÉCURITÉ PRIS ACCREDITED

Excecutive Summary: “BlackAxe”

“Drive By” Download

Root cause

Successful Enterprise Network Intrusion

Cobalt Strike used throughout the attack for lateral movement and persistence

Domain administrator privileges gained

No evidence of Data Exfil

Firewall logging provided contains no evidence of data exfiltration via file transfer protocols

Cobalt strike has limited exfiltration capability

Recovery

Domain controllers rebuilt – all compromised devices to be rebuilt

EDR monitoring on all servers

Account deletion and network wide password reset (including KRBTGT)

Timeline of events

APR 26 20:30

INITIAL USER ACTIVITY:

User browses Google in search of "is a handwritten recepit legal"

APR 26 20:40

INITIAL ATTACK VECTOR:

User clicks a link in the Google search results which uses "SEO Poisoning". It redirects to a fake forum.

APR 26 20:45

INITIAL MALWARE EXECUTION:

User downloads a .ZIP file "is a handwritten receipt legal.zip" and opens it, which results in a malicious JavaScript being executed.

APR 26 20:48

PERSISTENCE AND FOOTHOLD:

For malware persistence, a scheduled task is created along with an encoded PowerShell script in the autorun registry key, which loads each time the user logs on.

APR 26 20:50

REMOTE ACCESS TOOL:

After a series of events, the infamous commercial penetration testing tool “Cobalt Strike” is deployed to the user’s laptop.

Timeline of events

APR 26 21:00

INITIAL RECONNAISSANCE:

Just 20 minutes after the malware infection, the well-known recon tool “Bloodhound” is executed by the attacker.

APR 27 14:30

ABUSE OF PRIVILEGED SERVICE ACCOUNT:

After the recon phase, the attacker leverages an un-monitored Service Account called "bluecoat" to disable Windows Defender Antivirus on a Domain Controller server and install Cobalt Strike.

APR 27 20:00

LATERAL MOVEMENT AND PIVOTING:

Further movement inside the network is done through the Remote Desktop Protocol to several critical servers, disabling Windows Defender and deploying Cobalt Strike along the way.

APR 27 – MAY 4

CONTINUED RECONNAISSANCE:

Utilizing common tools such as ADTimeline, PowerSploit and Advanced IP Scanner, the attacker continues to conduct recon activities which in turn creates a considerable amount of noise.

MAY 4 13:00

DISCOVERY AND CONTAINMENT:

A third party of the client alerted the IT staff to potential Command & Control traffic emanating from 3 servers; two Domain Controllers and a File Server.

The traffic was swiftly blocked at the perimeter firewall and no further malicious activity was identified past this point.

Response timeline

MAY 6 13:30

CSIRT engaged

Customer contacted Orange Cyberdefense CSIRT

MAY 6 16:16

Collection and EDR deployment started

Started deployment of CSIRT tooling into customer network and started collection.

MAY 6 21:13

Collection and EDR deployment complete

Logs from 53 servers collected, processed and ingested into Splunk for analysis

MAY 06 22:30

Cobalt Strike beacons extracted

MAY 7 13:20

Patient Zero confirmed

Orange
Cyberdefense

Thanks

Hotline: +46 40 66 88 188

csirt-se@orangecyberdefense.com

Malmö 18.04.2023 / Göteborg 20.04.2023 / Sundsvall 03.05.2023

www.orangecyberdefense.com/se