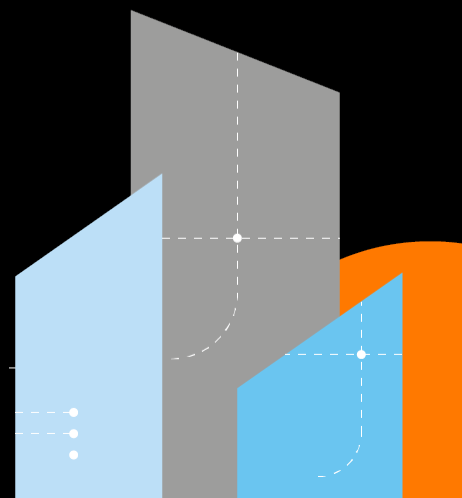


Orange
Cyberdefense

Incident Response – War Stories and Learnings

Hampus Glantz/ Daniel Bohwim

Sundsvall 03.05.2023



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,...)



PHISHING
INITIATIVE
France



Executive 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

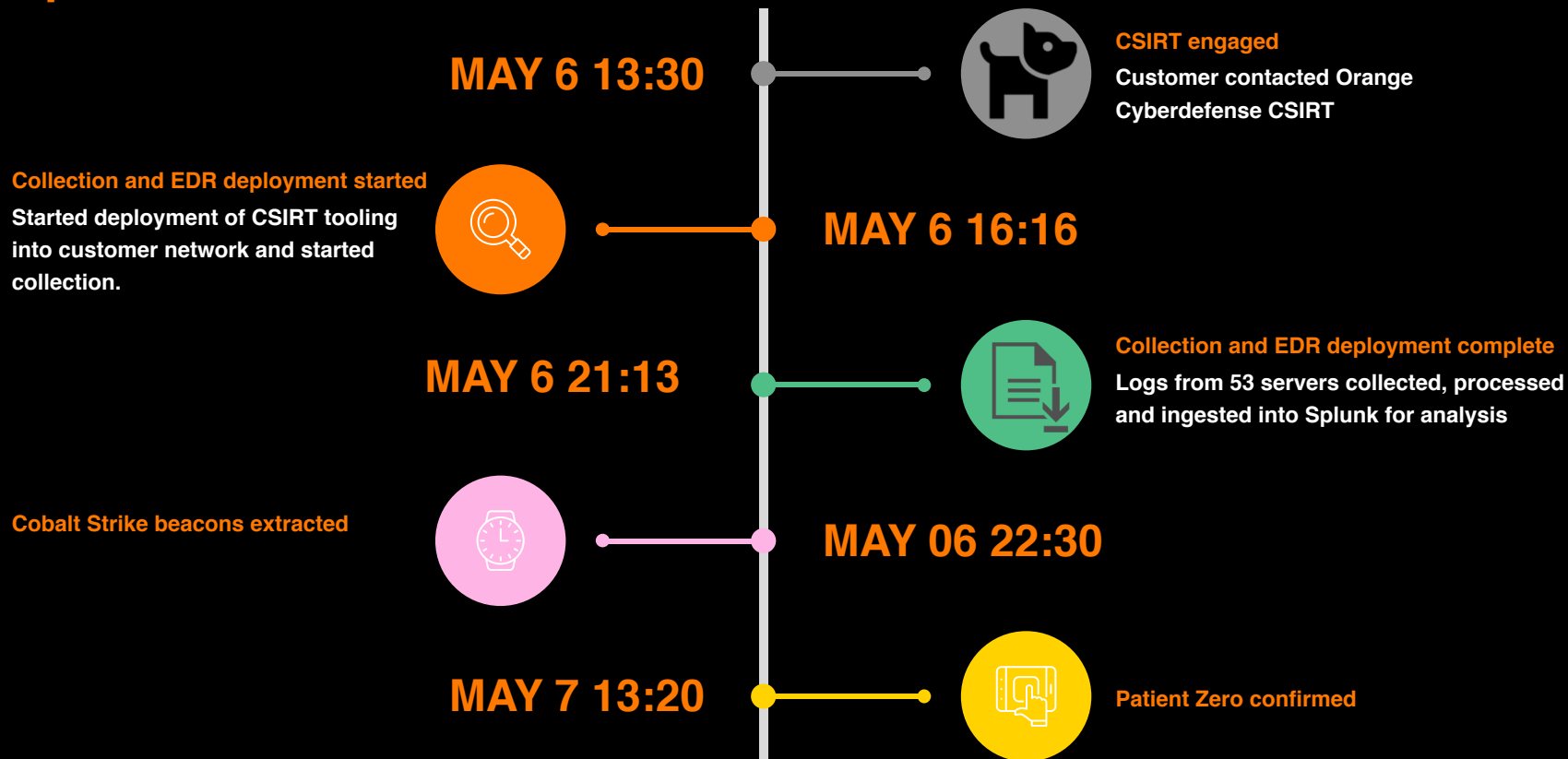
Recovery

Domain controllers rebuilt – all compromised devices to be rebuilt

EDR monitoring on all servers

Account deletion and network wide password reset (including KRBTGT)

Response timeline



Timeline of events, user activity

INITIAL ATTACK VECTOR:

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

PERSISTENCE AND FOOHOLD:

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 20:30



INITIAL USER ACTIVITY:

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



APR 26 20:40

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 20:45



APR 26 20:48

REMOTE ACCESS TOOL:

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

APR 26 20:50



Google search: «is a handwritten receipt legal»

The screenshot shows a Google search page in a Mozilla Firefox browser. The search query is "is a handwritten receipt legal". The page displays approximately 2,050,000 results in 0.48 seconds. A featured snippet from Informi.co.uk states that a receipt can be issued on paper or electronically and can be handwritten or typed. Below this, there is a "People also ask" section with four questions: "Are handwritten invoice acceptable?", "Do I have a legal right to a receipt?", "How do I write a receipt for cash?", and "What is a valid receipt?". The first result is from Yoder Results, dated February 28, 2022, which states that handwritten contracts are legal if written correctly.

is a handwritten receipt legal - Google Search - Mozilla Firefox

is a handwritten receipt | x +

https://www.google.com/search?q=is+a+handwritten+receipt+legal&source=hp&ei=SrKLYtXQMIG

Google is a handwritten receipt legal Sign in

All Images Shopping News Videos More Tools SafeSearch on

About 2,050,000 results (0.48 seconds)

A receipt can be issued on paper or electronically. **It can be handwritten or typed.**

https://informi.co.uk > business-administration > how-do-i...
How do I write a receipt? | Informi

About featured snippets Feedback

People also ask

- Are handwritten invoice acceptable?
- Do I have a legal right to a receipt?
- How do I write a receipt for cash?
- What is a valid receipt?

Feedback

https://www.yoderresults.com > is-a-handwritten-receipt...
Is a Handwritten Receipt Legal | Yoder Results

28 Feb 2022 — The short answer is yes. **Handwritten** contracts are a bit handy if you could just type them in, but they're completely **legal** if written correctly ...

Drive-by download

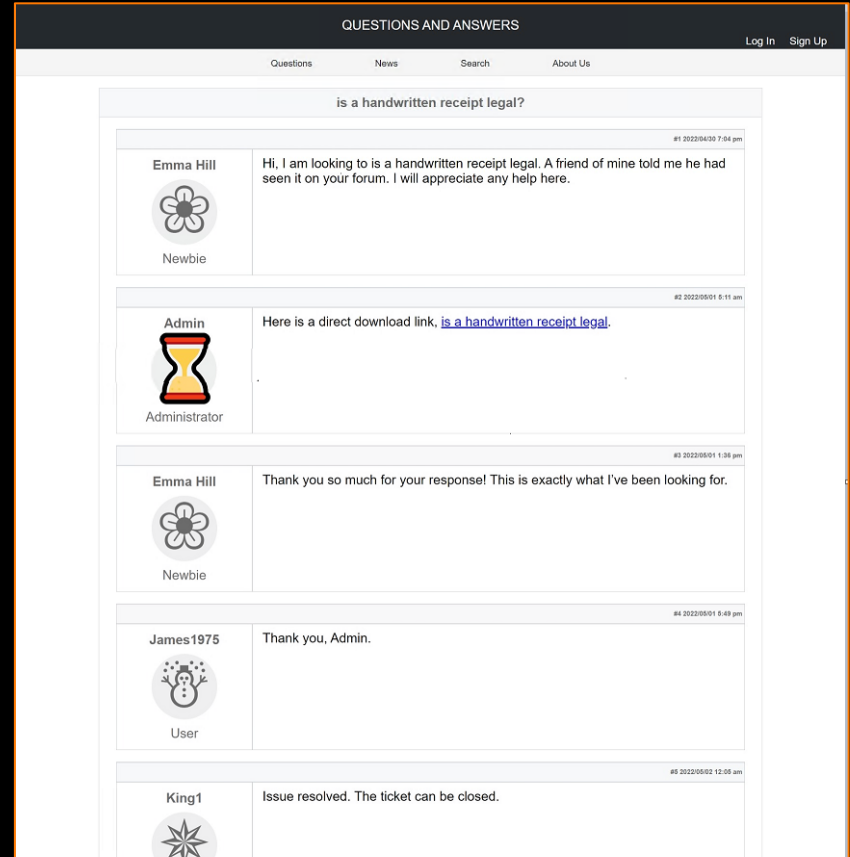
- Infected site checks victim

-• Target country
-• Hasn't visited previously
-• Type of Browser etc

- If any of these conditions are met you are redirected to a legitimate site

-• Related to the search you entered

- If not, you are directed to this forum:



The screenshot shows a forum page titled "QUESTIONS AND ANSWERS" with navigation links for "Questions", "News", "Search", and "About Us". The thread title is "is a handwritten receipt legal?".

Post #1 (7:04 pm):
User: Emma Hill (Newbie)
Text: "Hi, I am looking to is a handwritten receipt legal. A friend of mine told me he had seen it on your forum. I will appreciate any help here."

Post #2 (9:11 am):
User: Admin (Administrator)
Text: "Here is a direct download link, [is a handwritten receipt legal](#)."

Post #3 (1:38 pm):
User: Emma Hill (Newbie)
Text: "Thank you so much for your response! This is exactly what I've been looking for."

Post #4 (9:49 pm):
User: James1975 (User)
Text: "Thank you, Admin."

Post #5 (12:05 am):
User: King1
Text: "Issue resolved. The ticket can be closed."

Timeline of events, user activity

INITIAL ATTACK VECTOR:

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

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 20:30



INITIAL USER ACTIVITY:

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



APR 26 20:40



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 20:45



APR 26 20:48



REMOTE ACCESS TOOL:

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

APR 26 20:50

Timeline of events, attacker activity

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.

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.

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



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 20:00



APR 27 – MAY 4

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.

MAY 4 13:00



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



Orange
Cyberdefense

Thanks

Hotline: +46 40 66 88 188

csirt-se@orangecyberdefense.com

Sundsvall 03.05.2023

www.orangecyberdefense.com/se

