CyberProof®
A UST Company

2022 CYBER DEFENDERS PLAYBOOK

REAL-LIFE EXAMPLES OF HOW SECURITY TEAMS CAN COLLABORATE TO MITIGATE CYBER THREATS

CONTENTS

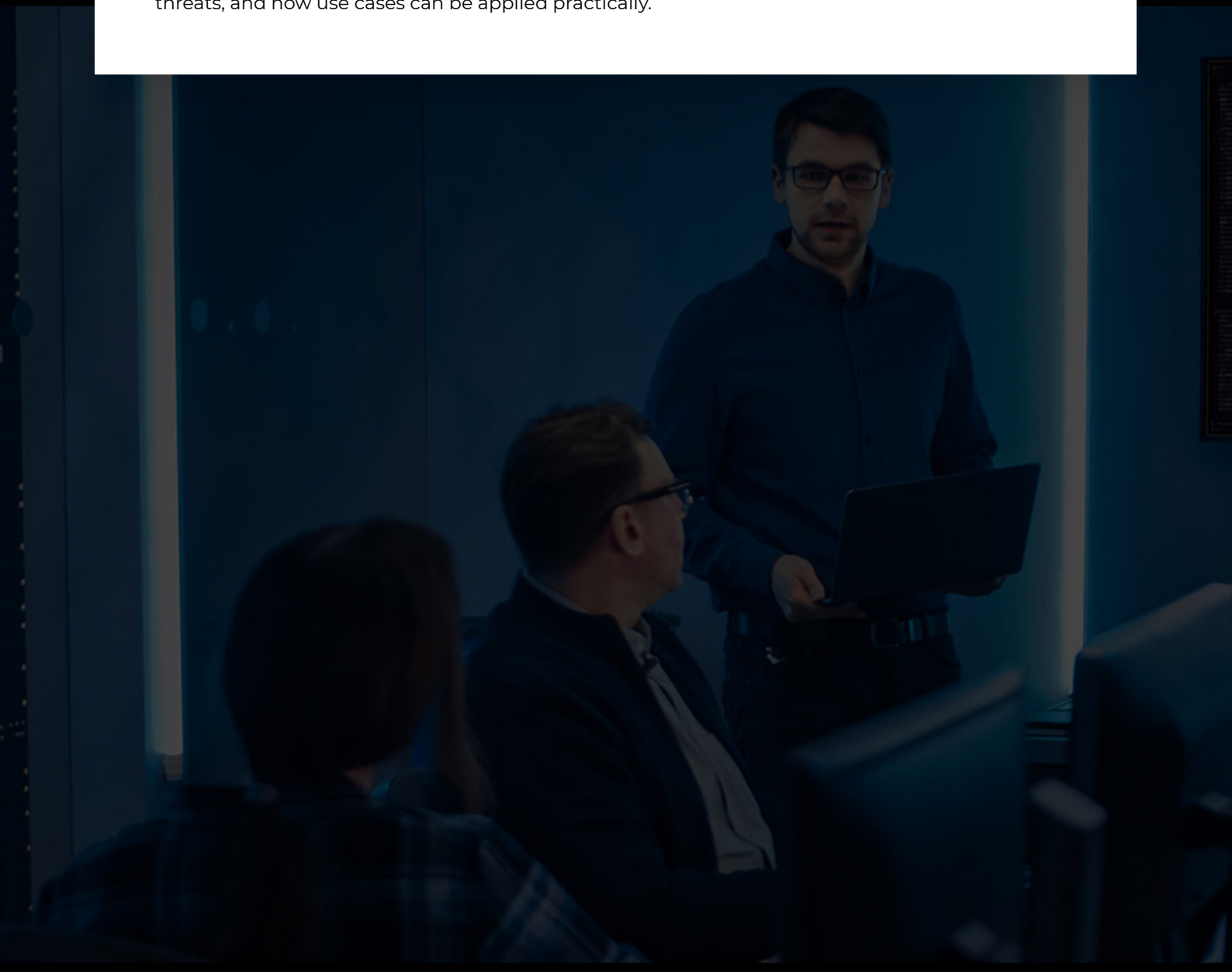
FIGURES

WHY READ THIS REPORT

You've probably encountered numerous threat intelligence reports outlining top attack campaigns in the past year. These reports are helpful in that they provide insight into common attacker behaviors and methods, but most of them fail to help you to apply this insight or include examples of the mitigation steps taken by defenders.

The aim of the report is to take those steps and turn them into a blueprint for the future.

This playbook provides the mitigation steps taken by cyber defenders. Using six scenarios depicting how individual teams within CyberProof worked together – including Level 1 and 2 SOC analysts, SIEM engineers, Digital Forensic and Incident Response (DFIR) specialists, threat hunters, vulnerability management experts and Cyber Threat Intelligence (CTI) analysts – this report illustrates how to detect and respond to some of the most persistent attacks in 2021. You'll learn from the highlighted techniques how different teams can collaborate effectively to mitigate threats, and how use cases can be applied practically.



SCENARIO 1
ICEDID FAMILY INFECTION INVOLVING A DATA EXFILTRATION ATTEMPT

CyberProof's L1 team detected an Endpoint Detection & Response (EDR) alert for command-and-control (C&C) malicious activity and potential shellcode execution. Collaboration between different teams – L1, L2, CTI, Threat Hunting, and DFIR – successfully remediated the threat, which turned out to be a data exfiltration attempt by means of an IcedID infection.

CYBERPROOF TEAMS INVOLVED

Cyber Threat Intelligence (CTI) team

- Deep & Dark Web Research
- IOC Analysis & Expansion

Threat Hunting team

- Data Collection
- YARA Rule Development
- SOC Feedback

L1 analysts

- Initial Response & Triage

L2 analysts

- Incident Response
- Further Investigation

Digital Forensics & Incident Response (DFIR) team

- Malware Analysis

1 **L1 Initial Response & Triage –** An EDR alert for C&C malicious activity and potential shellcode execution was detected by the L1 team on an employee's machine. The L1 team received the alert in the CyberProof Defense Center (CDC) platform, prioritized it, and opened an incident. The team initiated an investigation, then escalated it to the L2 analysts.

The L1 team identified several injected processes – including a suspicious query for domain admins using the net command. They shared their findings with the L2 team, who continued gathering and investigating related user activity.

2 **L2 Incident Response & Further Investigation –** The L2 team isolated the infected machine. They detected a user of the ADfind tool, who was querying the Active Directory (AD). The ADFind tool is a free command-line query tool that can be used for gathering information from Active Directory.

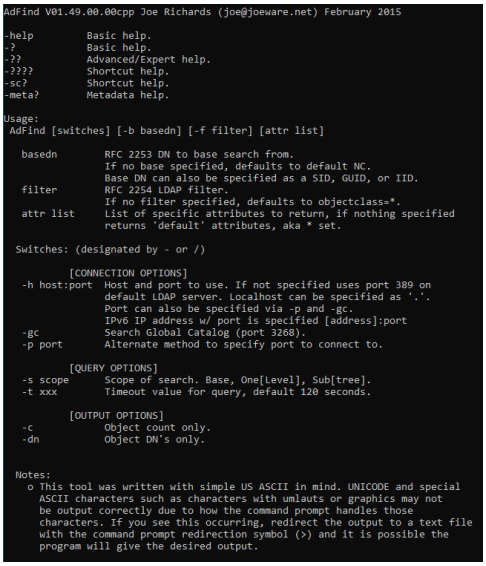


Figure 1: Detecting Malicious Use of The ADFind Tool

The L2 team dynamically executed the malicious document in the Red Lab environment to collect additional indicators. The information that was gleaned was forwarded to the CTI team so that they could assist in identifying the campaign.

```
adfind.exe -f "(objectcategory=person)" > ad_users.txt
adfind.exe -f "objectcategory=computer" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

Figure 2: Obfuscated Script

3 **CTI Research –** The CTI team searched for any exposed data that may have been gathered by the attacker on the dark and deep web and on underground forums. They then discovered IOCs (Figure 3) which included a malicious domain with two subpages.

2021-05-25 16:53:01	https://fimlubindu.top/news/	IcedID
2021-05-25 16:53:01	https://vindurualeg.top/news/	IcedID
2021-05-25 16:53:01	https://esaquell.website/news/	IcedID
2021-05-25 16:53:01	https://extrimefigim.top/news/	IcedID
2021-05-25 16:52:38	fimlubindu.top	IcedID
2021-05-25 16:52:38	vindurualeg.top	IcedID

Figure 3: Detection of Malicious Domains

The CTI team took the list of IPs that the injected processes communicated to. They ran these IPs through a custom-built script that analyzed the IPs using a variety of open sources. The team discovered that one of the IPs that was freshly reported in open communities was an IcedID Infra Server used by the threat actor known as TA551 or Shathack. The investigation revealed that this IP was used for data exfiltration, which was stopped by the machine isolation initiated by the L2 team.

4 **Threat Hunting –** The attack vector was revealed to be an attachment in a private email box. The Threat Hunting team examined the suspicious email and confirmed that this was a known attack. Delivering a malicious payload via private emails to corporate machines is a known technique to overcome enterprise email security – because no checks are carried out by the email gateway for private emails. The team looked for additional evidence that would help clarify whether the attack had moved laterally to other hosts. The Threat Hunting team verified that the IOCs connected to the incident did not exist in the environment.

The Threat Hunting team then identified a communication to one of the servers associated with the attacker TA551, which might have been indicative of data exfiltration. They recommended blocking relevant IPs. Finally, the Threat Hunting team performed a comprehensive hunt on the client's environment to make sure no malicious artifacts were left. As part of their recommendations, the Threat Hunting team developed YARA rules and recommended reimaging the infected host.

/2021 19:09:56 (UTC)	NTFS $MFT ...B $FILE_NAME	\ProgramData\ad_computers.txt
/2021 19:09:56 (UTC)	NTFS $MFT ...B $FILE_NAME	\ProgramData\ad_ous.txt
/2021 19:09:56 (UTC)	NTFS $MFT ...B $FILE_NAME	\ProgramData\trustdmp.txt
/2021 19:09:56 (UTC)	NTFS $MFT ...B $FILE_NAME	\ProgramData\subnets.txt
/2021 19:09:56 (UTC)	NTFS $MFT ...B $FILE_NAME	\ProgramData\ad_group.txt

Figure 4: File System Forensic Analysis

5 **DFIR Response –** The DFIR team initiated forensic analysis and verified that data had not been exfiltrated.

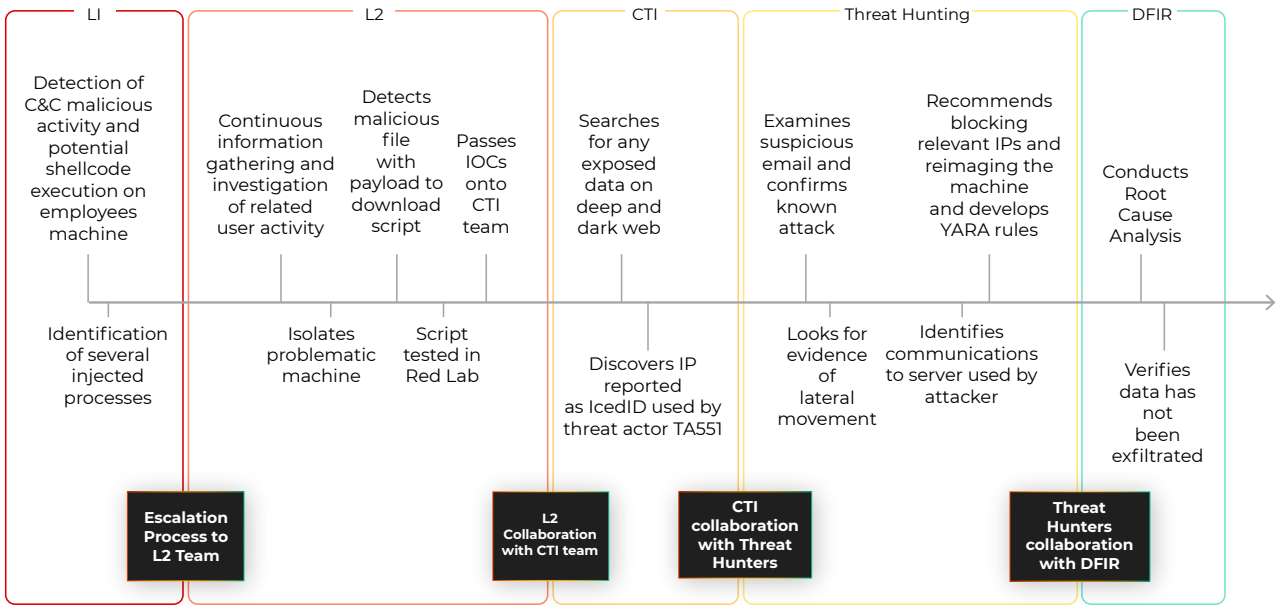


Figure 5: Summary of Steps Taken Against IcedID Data Exfiltration Threat

SCENARIO 2
DETECTION OF TYPOSQUATTING EXPOSES POTENTIAL DATA LEAKAGE

The CyberProof CTI team assisted one of its clients using several intelligence-gathering tools to compile a list of recently registered domains that either resembled the official domain name of the organization or were similar to the official domain name but had a typo. This information prompted an investigation that helped the client avoid the potential danger of data leakage.

CYBERPROOF TEAMS INVOLVED

CTI team
- CTI Research
- Data Leakage Monitoring
- Deep & Dark Web Research

SIEM engineers
- Query Development
- SIEM Logic Deployment/Testing

L1 analysts
- Initial Response & Triage

L2 analysts
- Further Investigation
- Incident Response

1 **CTI Research** – By gathering, on a regular basis, recently registered domains that were typosquatted and/or potentially malicious, the CTI team identified twenty potentially malicious domains that had been registered in the preceding two weeks and resembled the organization's official domain. The list also included all relevant data about these domains, including: registration date, registrar and associated DNS records.

2 **Initial Response & Triage** – The incident was escalated to the L2 team who in turn instructed the L1 team to scan the organization's logs for indications of traffic to or from any of the domains in the list provided by the CTI team. The L1 team did not find any evidence of such traffic.

3 **L2 Further Investigation** – Based on information provided by the CTI team, the L2 team knew that this domain had a Mail Exchanger (MX) record registered – meaning that the server could receive emails. A potential attacker could establish a mail server using the typosquatted domain – and it could register email addresses that mimicked the client's real email addresses. The potential attacker would then receive all emails sent to the fake, typosquatted email addresses.

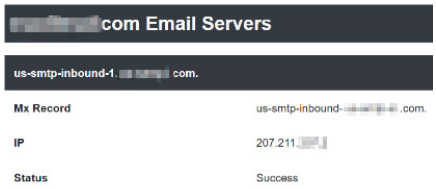


Figure 6: Evidence of MX Record

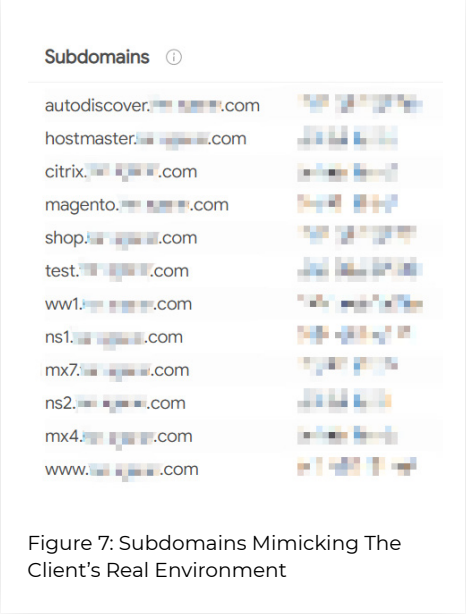


Figure 7: Subdomains Mimicking The Client's Real Environment

Predefined subdomains were found that mimicked the client's real environment. Together with CyberProof's security analysts, the L2 team searched for the users responsible for sending emails to the typosquatted addresses. The team's main goal was to assess the severity of the potential data leak by gaining more information about the type of information and documents that were being sent outside the organization. The analysts found multiple emails sent by the same sender to a variety of recipients, all of whom shared the same typosquatted domain.

After further investigation, CyberProof's security analysts concluded that this was a mailbox used to send automatic notifications for Purchase Orders and orders to multiple users. If a user's email address was added to the mailing list with a typo, every email sent to that address would not reach its intended destination. Instead, it went to an external user's mailbox. This was indeed the problem: typos entered by employees by mistake led to emails being sent externally.

4 **SIEM Engineering** – The L2 team asked the SIEM Engineering team to update the list of typosquatting domains in predefined rules to detect any connection, email, or alert related to one of the typosquatting domains in the list. Within a day, the team had identified a large number of outbound emails that had been sent to one of the typosquatted email domains.

5 **On-Site L2 Incident Response** – When the client understood the severity of the incident and the potential threat that typosquatting domains represent, they blocked the typosquatted domain in question in the email gateway. Other typosquatted domains that appeared on the list shared by the CTI team also were blocked, as a precaution.

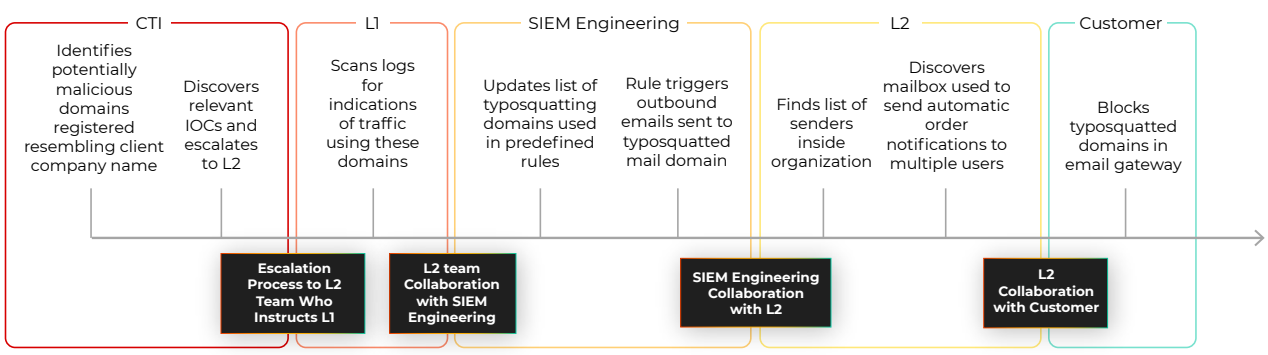


Figure 8: Summary of Steps Taken Against Typosquatting Threat

SCENARIO 3
MULTI-STAGE RANSOMWARE ATTACK WITH COBALT STRIKE INJECTIONS

CyberProof assisted a client in dealing with a multi-stage ransomware attack that involving both automation and human-operated techniques, which was detected by their EDR platform. CyberProof's CTI team identified the attack as a GootLoader campaign. With the assistance of our Threat Hunting team, SIEM engineers, and EDR engineers, the L2 analysts were able to remediate the attack.

CYBERPROOF TEAMS INVOLVED

CTI team
- CTI Investigation & Response
- Threat Actor Tracking

SIEM & EDR engineers
- SIEM Logic Deployment/Testing
- IOC Implementation

Threat Hunting team
- Data Collection
- Retro-hunting
- SOC Feedback

L1 analysts
- Initial Response & Triage

L2 analysts
- Incident Response
- Root Cause Analysis

1 **Initial Response & Triage** – The L1 team detected the malicious activity of a Cobalt Strike DLL injection. The L1 team initiated the investigation, identifying a Ping command potentially loaded with Cobalt. A floating module beacon was found in the Ping command process. The L1 team detected that a Rundll32.exe process was executed by the Ping and communicated to a malicious IP related to a server known to host Cobalt Strike. They also detected SMB connections to internal IPs. The L1 team turned to the L2 team, to carry out further investigation.

2 **L2 Incident Response –** The L2 team isolated the machine, investigated the known IP related to the known Cobalt Strike more deeply, and found a script related to a Cobalt payload.

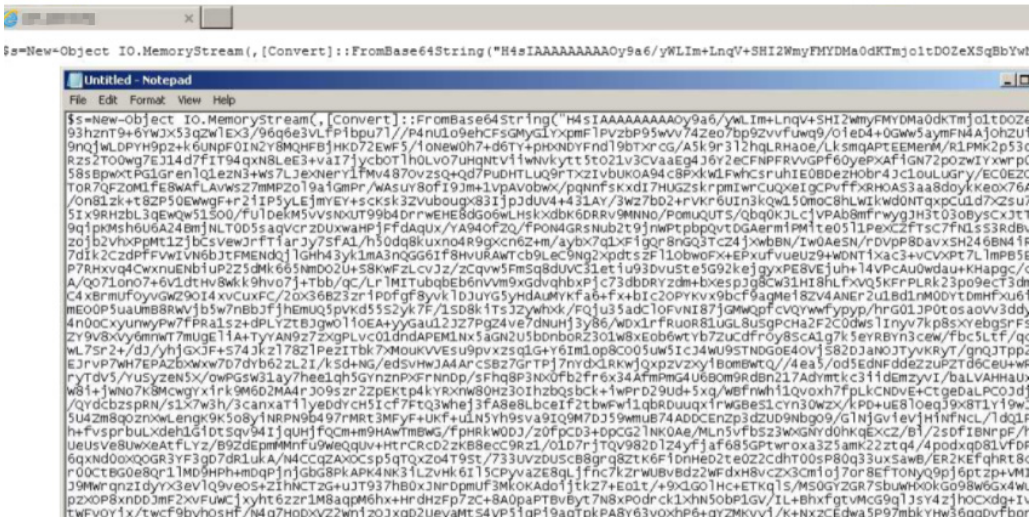


Figure 9: Cobalt Strike Payload Script

3 **L2 Investigation and Root Cause Analysis** – The L2 team was able to trace the appearance of a suspicious JavaScript execution, which later executed PowerShell and Ping. The infection started when a user visited a website compromised by a "waterhole" that included a link to download a ZIP archive with a malicious JavaScript. When the JavaScript was executed by the user, a PowerShell was downloaded from another compromised website that delivered the PowerShell script to execute a memory DLL injection. The first attack concluded by opening a door to the attacker via the Cobalt Strike C&C.

An EDR alert was detected, this time for a Cobalt Strike injection from the Ping process into the "Rundll32.exe" process. The CyberProof team believed this was done because of the greater capabilities "Rundll32" offers. The attack continued with the threat actor scanning the network over ports 137 and 445 with the objective of enumerating the environment (discovery phase). As soon as the threat actor found a Domain Controller (DC), they started a connection over LDAP protocol to pull Active Directory information.

The initial vector was a zipped document. A search in the email gateway logs revealed nothing, but when the browsing history was analyzed, the team found the source of the file download. This information (together with other indicators like domains) was provided to the CTI team to facilitate campaign identification.

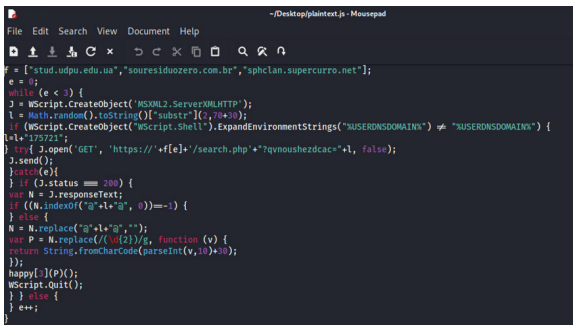


Figure 10: Malicious JavaScript Code

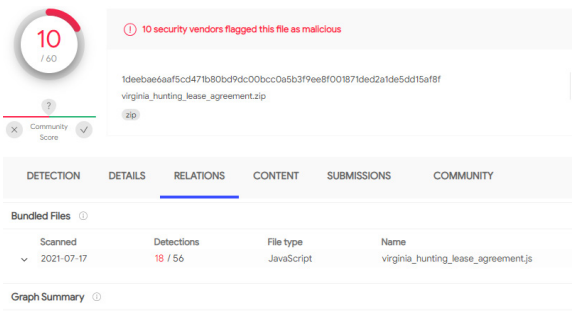


Figure 11: Analysis of Downloaded Malicious Zip File in Virus Total

4 **CTI Research** – The CTI team discovered that the IOCs probike[.]com and meenajewel[.]com were associated with a GootLoader campaign as well as with BlueCrab/Sodinokibi ransomware. The payloads of these two types of malware are distributed via SEO poisoning, a social engineering technique in which threat actors compromise legitimate and highly trafficked websites. They edit the content to improve Search Engine Optimization (SEO), and add ZIP files named with terms that they expect will appeal to their targets. The ZIP files contain malware that website visitors then download. For this reason, there was no detection of phishing emails in the email security gateway.

The GootLoader malware operates in the model of "Initial-Access-as-a-Service" (Figure 8). After successfully compromising an enterprise network, it sells access to other threat actors to further the attacks, usually to ransomware groups.

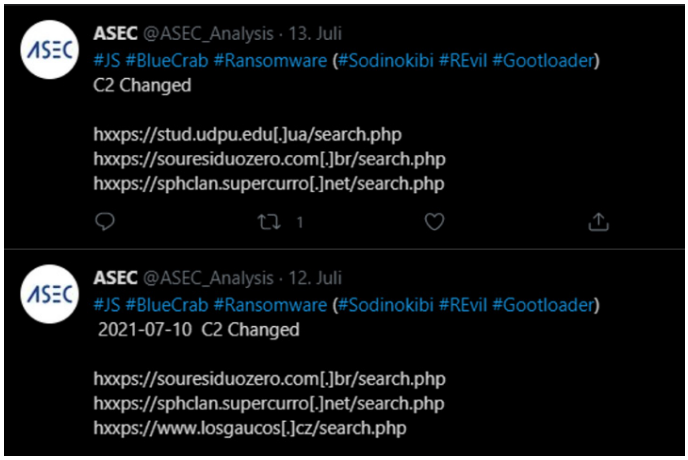


Figure 12: Gootloader IOCs Published in Twitter

5 **Threat Hunting** – The Threat Hunting team gathered IOAs for malicious behavior and used EDR and SIEM platforms to verify that this threat had not spread or infected other hosts. In this way, the team was able to limit the scope of the alert and prove that the rest of the network was not infected. Furthermore, the Threat Hunting team investigated the malicious files (e.g., JavaScript, the PowerShell script, and additional linked executables found online) using sandbox and file analysis and added these IOCs to the gathered IOC list provided by the CTI team.

The Threat Hunting team executed retro-hunts for these indicators within the EDR and SIEM logs and found no indication of infection. They recommended that the customer reset all credentials for domain administrators and other privileged accounts.

6 **SIEM and EDR Engineering** – The SIEM and EDR engineering teams implemented the IOCs and the L1 team searched for IOCs in the environment.

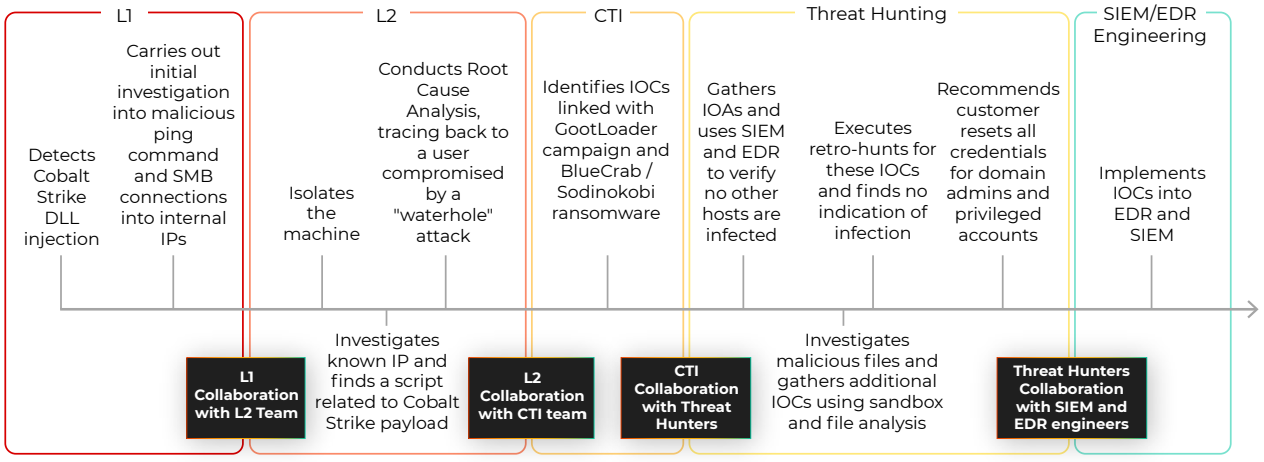


Figure 13: Summary of Steps Taken Against Multi-Stage Ransomware Attack

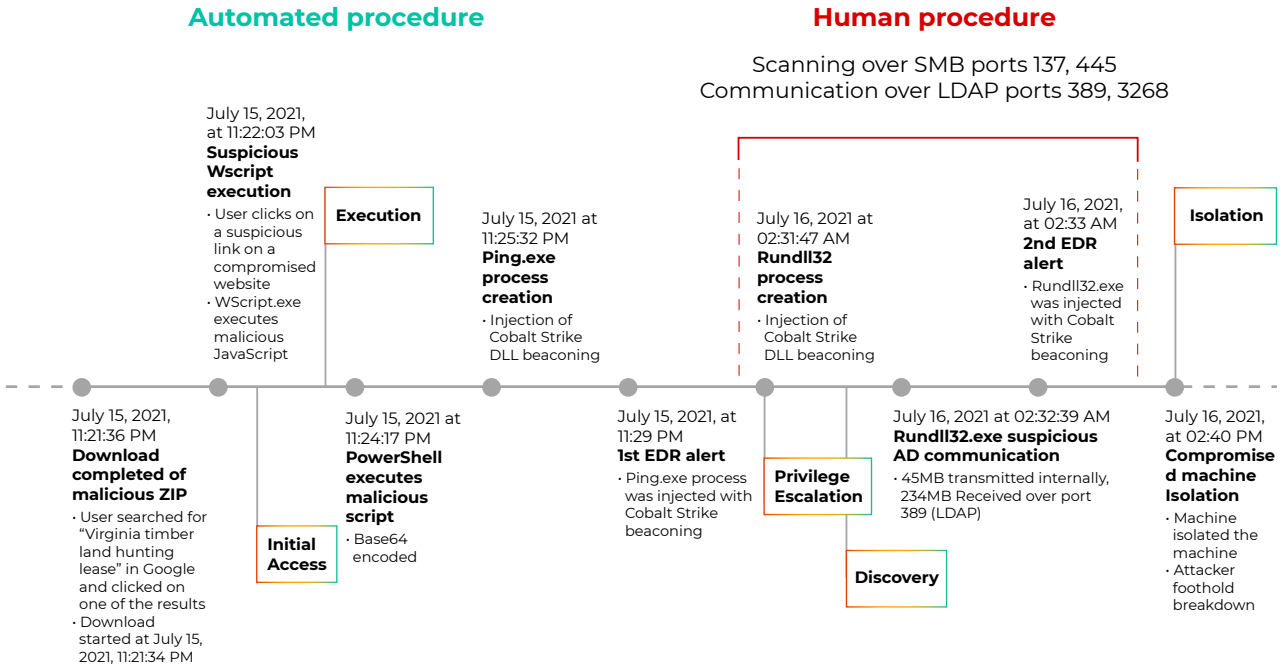


Figure 14: Multi-Stage Ransomware Attack Timeline

SCENARIO 4
CROSS-SITE SCRIPTING (XSS) ATTACK EXPLOITING A VULNERABLE WEB SERVER

CyberProof's CTI analysts noticed random strings of content on a client's website - the result of an XSS attack. CyberProof's CTI team, Vulnerability Management team, and L1 & L2 analysts worked together to learn more about the attack and assist the client in restoring its web servers to their original states.

CYBERPROOF TEAMS INVOLVED

CTI team
- Vulnerability Intelligence
- CTI Research

Vulnerability Management team
- Vulnerability Mapping
- Comparing CTI's Data to VM reports
- Patching Relevant Servers

L1 analysts
- Initial Response & Triage

L2 analysts
- Further Investigation
- Incident Response
- Root Cause Analysis

HERE ARE THE STEPS WE TOOK:

1 **Initial Response & Triage –** Unusual content was found on a client's website. The content consisted of two random strings – in two different HTML tags – on one of the pages of the client's website. Having recognized this as potentially malicious activity, the CTI team escalated to the L1 team to follow up. After initial investigation, the L1 team found the source of the exploit. They discovered that the appearance of the random strings on the client's website resulted from a vulnerability scan of the client's web applications that had a US-located source IP. The L1 team escalated the incident to the L2 team via the CDC platform to validate and conduct root cause analysis.

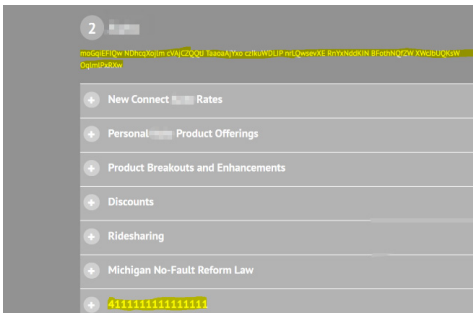


Figure 15: Website Snip

2 **L2 Further Investigation and Root Cause Analysis –** The L2 team validated the findings and established the scope of the attack – they determined that a single web server was affected. They revealed that multiple types of attack were exposed by the vulnerability scan, including: SQL injection, XSS, Remote File Inclusion, and more. The team identified these strings in the Web Application Firewall (WAF) logs and concluded that this was an XSS attack exploiting a vulnerability in the Oracle ColdFusion app, which was installed on the Internet Information Services (IIS) server, the most common Microsoft Web server. The L2 team escalated the incident to the CTI team, via the CDC platform – to obtain additional information.

3 **CTI Research –** The CTI team located the relevant vulnerabilities that were recently referenced – on clear web sources – to the ColdFusion app, and shared the information with the L2 team.

4 **L2 Incident Response –** The L2 team consolidated all information, drew conclusions, formulated recommendations, and escalated the incident to the onsite lead and the Vulnerability Management team. The on-site L2 lead was responsible for validating the response actions, includes restoring and patching the target server.

5 **Vulnerability Management –** CyberProof's Vulnerability Management team conducted internal vulnerability mapping and compared the information from the CTI team to VM reports. This allowed them to draw a clearer picture of the situation, which gave our client the ability to patch the vulnerable servers. The web servers were restored to their original state before the attack.

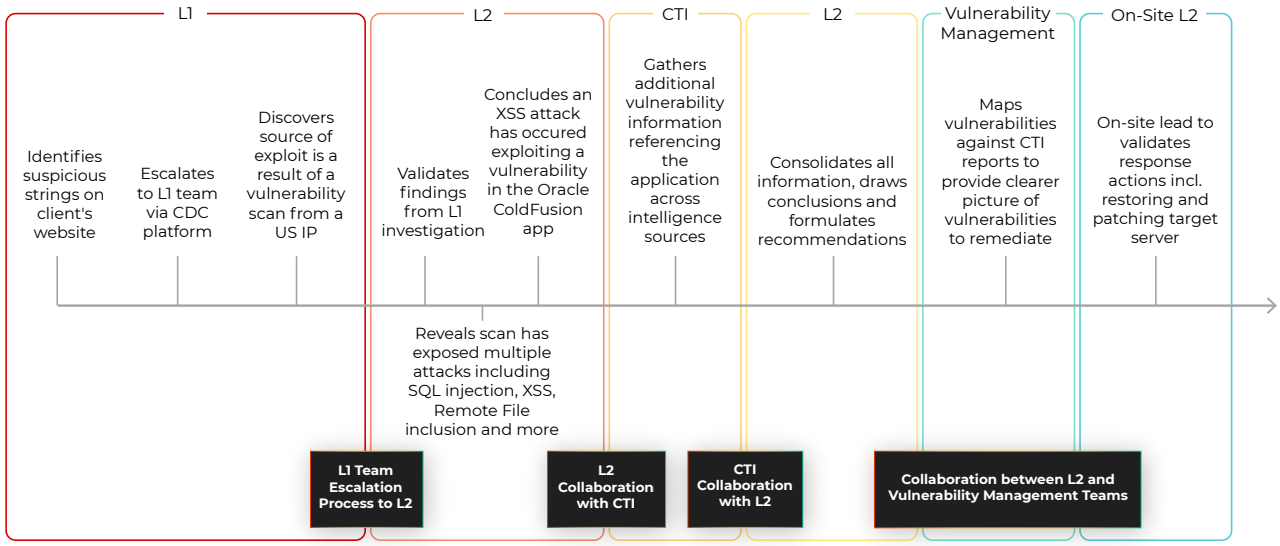


Figure 16: Summary of Steps Taken Against Cross-Site Scripting Threat

SCENARIO 5
PRINT NIGHTMARE VULNERABILITY LEADING TO REMOTE PRIVILEGE ESCALATION

Print Nightmare has been one of the most frequently discussed cyber security discoveries of the last year. It presents a serious vulnerability in the Print Spooler service that can lead to remote privilege escalation on every system in which the service is active. Cyberproof's CTI, SIEM, Threat Hunting, L1 and L2 teams worked proactively to mitigate this risk for our clients.

CYBERPROOF TEAMS INVOLVED

CTI team
- Vulnerability Intelligence

SIEM Engineering
- Log Validation
- Query Development
- SIEM Logic Deployment/Testing
- Alert Creation

Threat Hunting
- Data Collection
- Retro-hunting
- Mitigation Advice

L1 analysts
- Alert Monitoring

L2 analysts
- Incident Response

HERE ARE THE STEPS WE TOOK:

1 **CTI Vulnerability Intelligence –** The CTI team identified IOCs for the Windows Print Spooler Remote Code Execution vulnerability and provided each of our clients with the official Microsoft mitigation – which involved disabling the print service when it was not required. However, in situations where the servers could not be disabled, such as print servers, the official mitigation did not resolve the issue and further work was required.

2 **Threat Hunting –** The Threat Hunting team collaborated with the CTI team to gather external sources of information on which the hunt was based. The Threat Hunting team then proceeded to investigate by:

- Categorizing the hunt according to the type of platform (SIEM or EDR) in which the indicators would need verification.
- Searching for logs or events that could indicate an exploitation of this vulnerability, such as: execution of Remote Procedure Call (RPC); addition of a new printer driver; suspicious process execution tree; creation of suspicious DLL files spawned in a dedicated folder; or execution of a printer process with the Process Integrity Level "SYSTEM."
- Identifying mitigation steps and other hardening policies – such as disabling inbound remote printing through Group Policy and restricting the installation of new, unsigned printer drivers.

3 **L2 Incident Response –** The Threat Hunting team shared its findings with the L2 team and SIEM engineers, who were involved in the response process. The L2 team coordinated with each client to implement the necessary workarounds. They conducted research to identify means of mitigating the risk for servers that could not be patched – and shared the logic they uncovered with the SIEM engineers.

4 **SIEM Engineering –** The SIEM engineers validated the logs required for creating the logic in the SIEM. They provided logging requirements (where needed), developed a query for each SIEM system used by our clients, deployed the logic in the SIEM, tested this logic, and created alerts.

5 **L1 Alert Monitoring –** The L1 team continues to monitor and investigate the alerts fired by the new rules that have been developed.

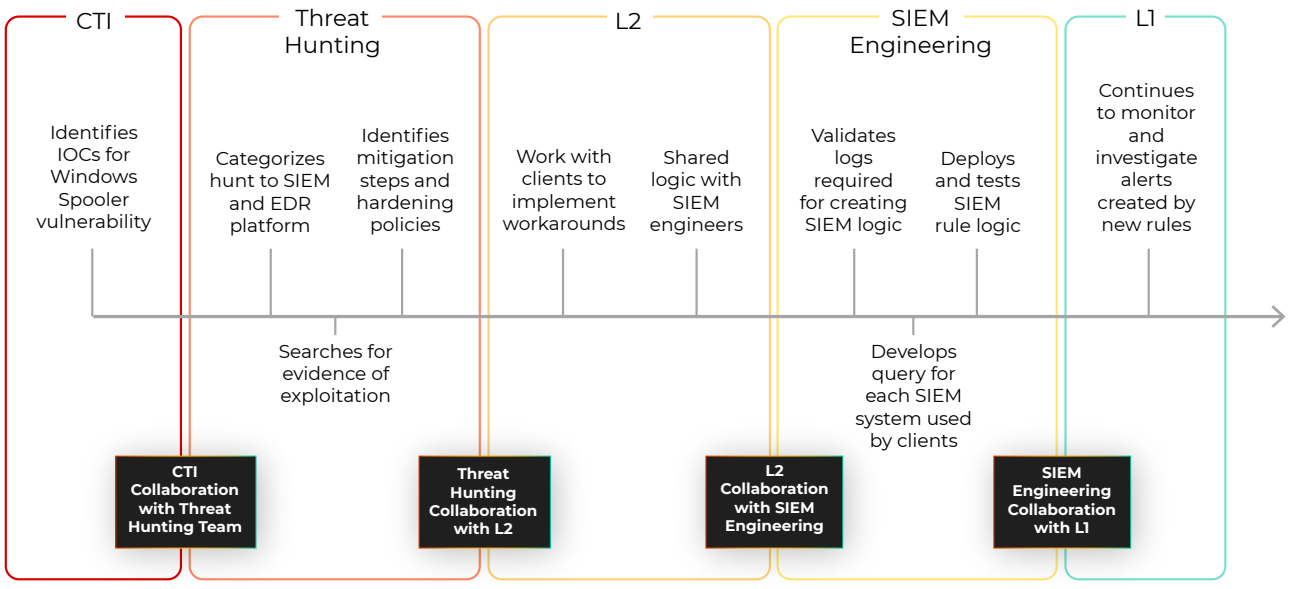


Figure 17: Summary of Steps Taken Against Print Nightmare Vulnerability

SCENARIO 6
EMAIL-BASED MALWARE DISTRIBUTION CAMPAIGN LEADS TO URSNIF INFECTION

Ursnif is one of the most common banking trojans. CyberProof's team revealed that this attack was linked to TA551 (Threat Actor ID 551), a financially motivated threat group that has been active at least since 2018, and helped the client remediate the attack.

CYBERPROOF TEAMS INVOLVED

CTI team
- CTI Research

L1 analysts
- Initial Response & Triage

L2 analysts
- Further Investigation
- Root Cause Analysis
- Incident Response

HERE ARE THE STEPS WE TOOK:

1 **Initial Response & Triage –** An alert was received by the L1 team from a Microsoft Office application. The alert involved a suspicious execution tree; winword.exe which was observed to be spawning cmd.exe.

The L1 team received the alert via the CDC platform, triaged it, and opened an incident. Having carried out an initial investigation, the L1 team decided to escalate it to the L2 team.

2 **L2 Further Investigation and Root Cause Analysis –** The L2 team validated the findings and gleaned additional details about the attack. The victim had received a phishing email with a weaponized macro document, which contained a command to download a malicious .hta script from a Microsoft domain and run it with cmd.exe.

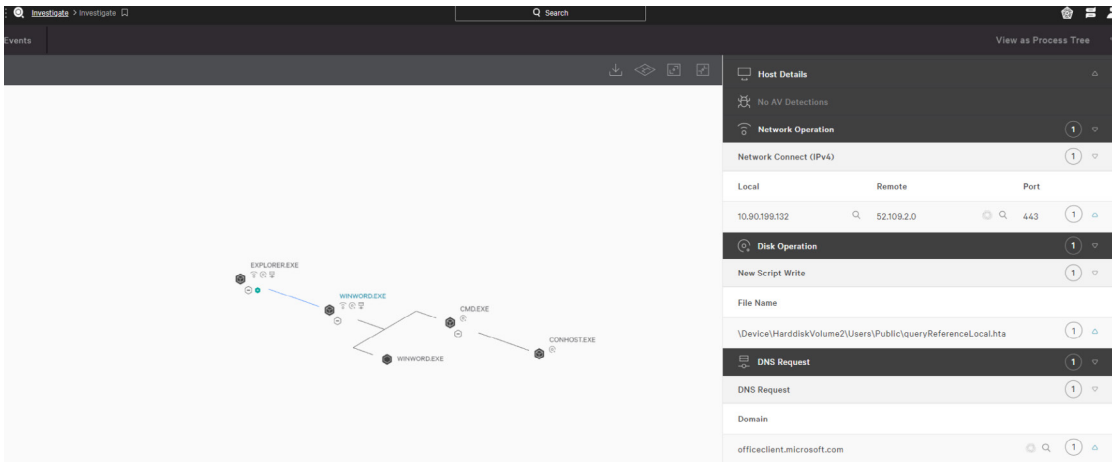


Figure 18: Suspicious Execution Tree

While pulling the script from the compromised host, the L2 team found obfuscated visual basic script blacklisted on many engines in VirusTotal.

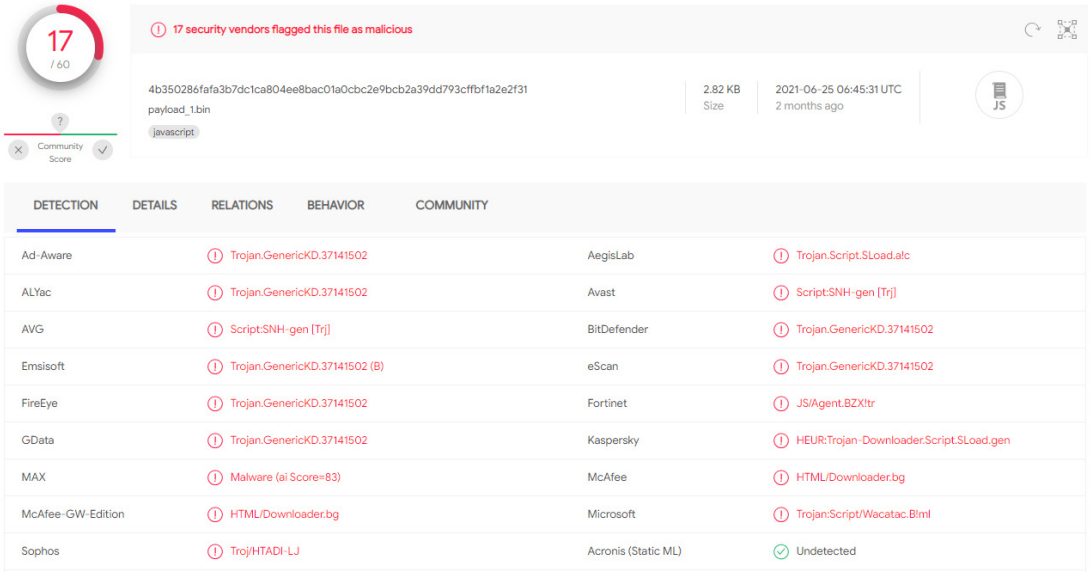


Figure 19: .HTA Dropper Script Analysis in VirusTotal

After deobfuscation, it was discovered that the script attempted to download the final payload from the C2 server and run it with regsvr.exe:

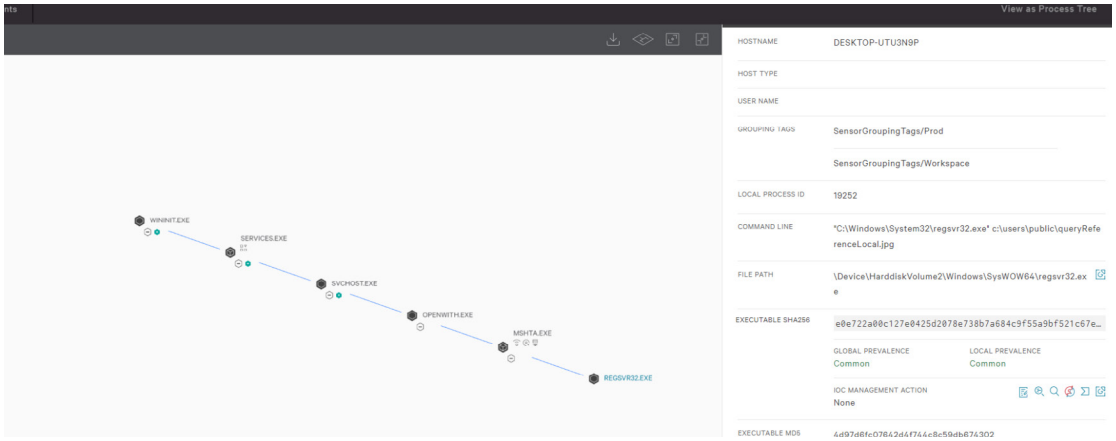


Figure 20: Attempted Process by Attacker to Execute Payload

The destination file was masqueraded as a .JPG file but seemed to be the target DLL payload file. The attempt to download the final payload from the C2 server was blocked by the firewall geolocation enforcement, which ended the execution chain.

3 **CTI Research –** The CTI team conducted further research about the campaign, confirmed the analysis of the L2 team and identified IOCs to check for further compromise. They revealed that this attack was linked to TA551 (Threat Actor ID 551), a financially-motivated threat group that has been active at least since 2018 and primarily targets English, German, Italian, and Japanese speakers through email-based malware distribution campaigns. The current campaign was researched by Palo Alto Unit 42, who observed that the final payload of IcedID malware was replaced with Ursnif malware – just days before this attack was first seen in the customer environment. All the indicators matched those of the attack CyberProof were dealing with at this point in time (see tweets/2021-06-21-TA551-IOCs-for-Ursnif.txt at master · pan-unit42/tweets · GitHub).

4 **L2 Incident Response –** The on-site lead coordinated the remediation steps – deleting the malicious email, isolating the host, implementing network restrictions, and raising the risk related to the use of personal mailboxes, as a lesson learned from this incident.

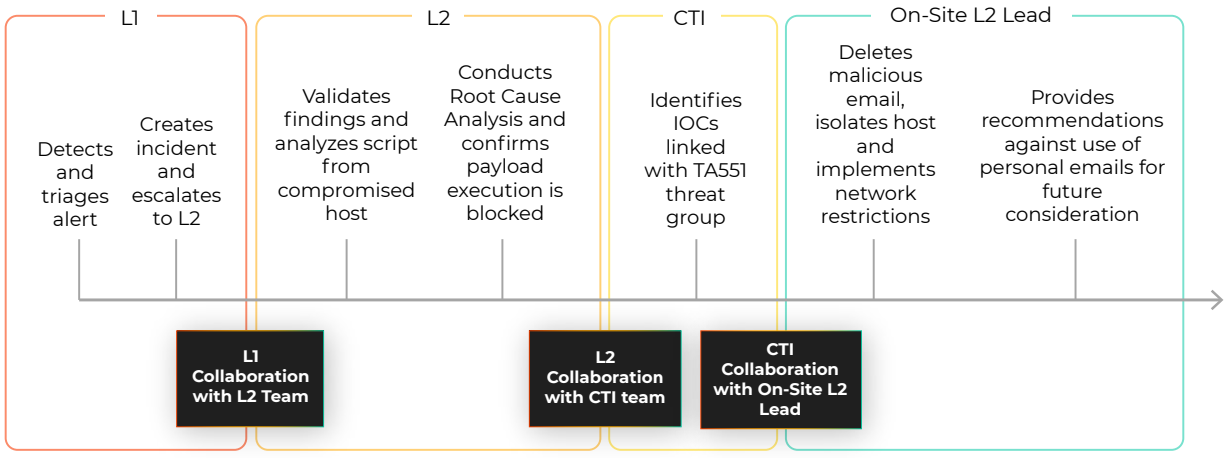
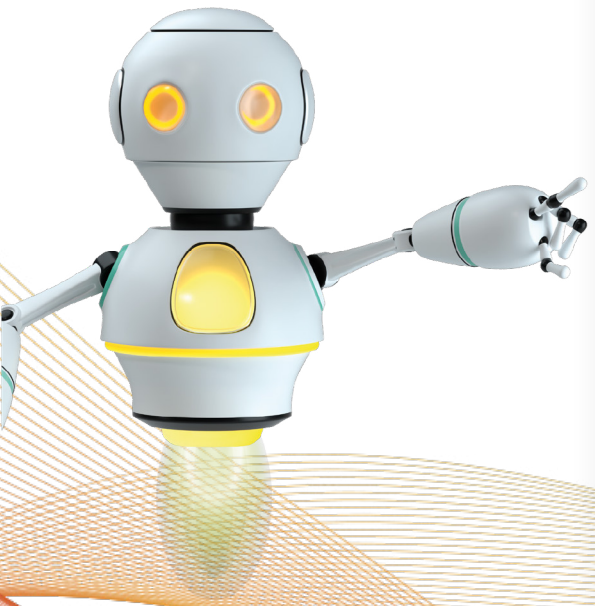


Figure 21: Summary of Steps Taken Against Ursnif Infection

KEY TAKEAWAYS

Our goal in describing these scenarios is to highlight best practice processes and techniques that can be adopted to improve the efficiency of security operations in any organization. By working together and focusing on collaborative approaches to problem-solving, security teams can increase the speed of detection & response – thereby reducing the potential impact of an attack.

Some of the key elements mentioned in this report, which contributed to successfully mitigating these attack scenarios, include:



- **Having a CTI team on hand to conduct research across the open, deep and dark web on IOCs –** Throughout these scenarios, the CTI team was vital in helping the various experts within the SOC to understand if any of the IOCs discovered in the network were being used as part of attack campaigns. Without this rapid collaboration with a CTI team, the SOC would have been unable to anticipate the next steps of the attacker. Similarly, without the input of the CTI team, Threat Hunters would have been unable to obtain the information they needed to search for evidence of these attacks in hidden areas of the network.

- **Using a proven Threat Hunting methodology –** We've seen that the scope of Threat Hunting goes way beyond the actual hunting itself. CyberProof's Threat Hunters played a critical role not only in searching across the client's environment to find evidence of compromise, but also in providing feedback to the SOC that improved the client's security posture. What's important is having a defined methodology in place that covers the following phases:
  - Conducting data collection from the network, endpoint, cloud instances, email gateway and more
  - Acquiring leads from threat intelligence or incident reports
  - Forming an actionable hypothesis
  - Executing the hunt using live and historic data
  - Validating the identified events
  - Providing feedback for improving future security procedures

- **Using a centralized SOC delivery platform –** Having a single SOC platform such as the CyberProof Defense Center (CDC) platform, which is integrated with existing security technology, enabled each of our teams to collaborate in real time capturing relevant data and orchestrating response actions quickly.

ABOUT CYBERPROOF

CyberProof is a security services company that helps organizations to intelligently manage incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact.

SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats.

We collaborate with our global clients, academia, and the tech ecosystem to continuously advance the art of cyber defense.

CyberProof is part of the UST family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services. For more information, see: www.cyberproof.com

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum