

Cyber 2024 Defender's Playbook

Cl0p ransomware

Real-life examples that will empower
your security teams

cyberproof.com





Table of Contents

Why read this report	3
CI0p Ransomware	4
Teams involved	4
The role of the L1 and L2 SOC analysts	5
The role of the DFIR team	5
The role of the Managed EDR team	5
The role of the advanced threat hunting team	6
The role of the tailored threat intelligence team	7
Our recommendations	8
Appendix	10
CyberProof's security services	11
About CyberProof	14

Why read this report

It's likely that you have encountered numerous threat intelligence reports outlining top attack campaigns. These types of reports provide insight into attacker behaviors and methods – but most of them don't 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 to help you in handling future incidents.

How do our clients discover if they have been attacked?

There are many ways that we help our clients identify potential attacks. In the scenario outlined in this report, the CyberProof Cyber Threat Intelligence (CTI) team shared weekly reports with the client describing campaigns that include new Incidents of Compromise (IOCs). The client – who is being monitored through the CyberProof Defense Center (CDC) platform – may detect these IOCs, indicating a possible attack.

This report outlines how our team works together internally as well as with the client team to cut incident response time and mitigate the potential risk to the business.

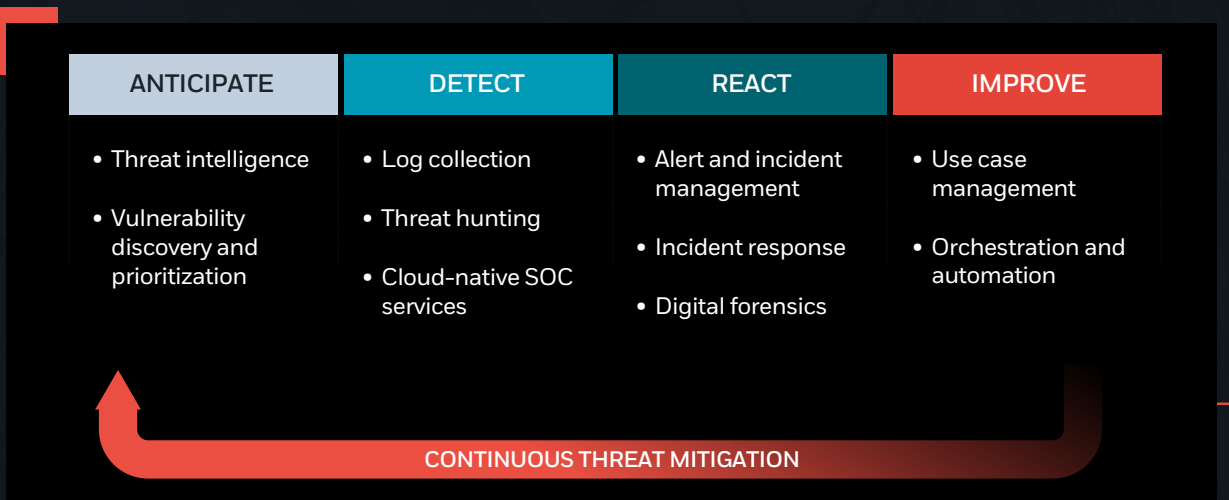
When the client detected an CIOp ransomware IOC, CyberProof's experts collaborated to assess and minimize and prevent damage to the client's network and data.

What is CIOp?

CIOp ransomware is a form of malicious software designed to encrypt files on a victim's computer, rendering them inaccessible until a ransom is paid. It is associated with a larger cybercrime group that primarily targets large organizations to maximize potential payouts. CIOp is known for its tactic of double extortion, where attackers threaten to release stolen data publicly if the ransom is not paid, increasing pressure on victims to comply.

How does CyberProof mitigate attacks?

CyberProof offers better security, together – slashing incident response time and mitigating risk by augmenting the client's in-house team, leveraging best-of-breed technologies, and collaborating internally with focused teams of experts.



Note: This report is written in the past tense to simplify and clarify the description and definition of our activities. However, it is a theoretical attack that is being described here, rather than a real attack on one of CyberProof's clients.



CI0p Ransomware

The CI0p ransomware attack on our client was facilitated by exploiting a zero-day vulnerability in the GoAnywhere MFT admin console, enabling the CI0p group to compromise approximately 130 victims rapidly. CI0p operates as a Ransomware as a Service (RaaS) and is notable for its evolutionary nature, regularly updating and varying its attack methods. Historically linked with other ransomware families like CryptoMix, CI0p has adapted over time, enhancing its effectiveness through new tactics.

One of CI0p's hallmark strategies is "double extortion," where it not only encrypts the victim's files but also exfiltrates sensitive data prior to encryption. The group then threatens to leak this data unless the ransom is paid, significantly increasing the urgency and pressure on victims to meet their demands.

Teams involved

The following teams at CyberProof took part in the process of mitigating the CI0p ransomware attack:

Team	Description
 CTI	<ul style="list-style-type: none">▪ Insights and enrichment▪ OSINT and WEBINT▪ IOC collection & analysis
 EDR	<ul style="list-style-type: none">▪ Add Incidents of Attack (IOAs) as behavior rules
 Threat hunting	<ul style="list-style-type: none">▪ Identify additional infected assets▪ Leverage IOAs to locate infection
 L1 analysts	<ul style="list-style-type: none">▪ Initial response & triage▪ Monitor security perimeters and CDC alerts
 L2 analysts	<ul style="list-style-type: none">▪ Incident response▪ Advanced incident investigation▪ Orchestration of team activities
 DFIR	<ul style="list-style-type: none">▪ In-depth Investigation and Resolution

The role of the L1 and L2 SOC analysts

The SOC team's L1 and L2 analysts detected this attack via an alert on the SIEM platform which was viewed by CyberProof's team using the CyberProof Defense Center platform.

The following initial steps were taken:

- Isolating the endpoint to prevent the attack from spreading further
- Reviewing user activity and user behavior analysis
- Checking outbound communication and searching for abnormal traffic

During the initial triage, analysts studied "Patient Zero" – the endpoint where the infection was first identified – and collected all potential evidence, including the file path of the detected ransomware and the C2 communication attempt. The analysts also searched for the possibility of encrypted files, abnormal file extensions (specifically, .clop), and notifications regarding ransomware encryption. They communicated with the

client throughout the incident response period, providing notifications and updates.

The role of the DFIR team

The DFIR team remained on-hand and prepared to handle any indications of ransomware spreading further across the client network, and to assist with incident handling including containment and eradication.

The role of the Managed EDR team

The MEDR team supported the incident handling process by fine-tuning policies. Their work was based on the information that they received from the SOC analysts.

Using EDR detection rules, they did the following fine-tuning:

- **The file-based detection rule looked as follows:**

```
bash Copy code
rule detect_clop_ransomware {
  strings:
    $magic = { 0x43 0x4C 0x4F 0x50 } // Detects the "CLOP" magic bytes
  condition:
    $magic
}
```

Example of EDR file-based detection rule

- **The behavioral detection rule looked as follows:**

```
vbnet Copy code
title: Clop Ransomware Behavior Detection
description: Detects behaviors associated with Clop ransomware
detection:
  - ImageLoad:
    Image: '*\clop.exe'
```

Example of EDR file-based detection rule

- **The network traffic rule looked as follows:**

```
css Copy code
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"Clop Ransomware C2 Commu
```

Example of network traffic rule

The role of the advanced threat hunting team

The threat hunting team received a lead from the SOC team about the existence of ransomware activity. By investigating EDR logs, they were able to identify the infected endpoints that were not yet encrypted. The threat hunting team conducted endpoint-based hunting:

1. To identify ransomware and malware delivery, we hunted for suspicious execute trees starting with a mailing process such as outlook.exe or thunderbird.exe deploying suspicious LOLBAS processes such as: wscript.exe, cscript.exe, cmd.exe, powershell.exe, rundll32.exe, etc. The threat hunting team used Generative AI to transform logic hunting steps into a hunting query, and identify the relevant data sources that would produce the corresponding hunting query.

You're a cybersecurity expert working as a threat hunter. You identified a chain of three processes. An outlook.exe process spawning as a child process a malicious cmd.exe which opens another child process a powershell.exe process that has an encoded command line. The execution tree is outlook.exe -> cmd.exe -> powershell.exe (with encoded command line). You were given the task of hunting for this behavior in your Microsoft Defender EDR. Please write a hunting query for this corresponding behavior that can be executed on Microsoft Defender. Explain the logic of the query and every field that you've used.

CyberProof CoWorker 9:26



Sure Brian, here is the Kusto Query Language (KQL) query to hunt for this behavior in Microsoft Defender Endpoint Detection and Response (EDR):

```
DeviceProcessEvents
| where (InitiatingProcessParentFileName == 'outlook.exe' and InitiatingProcessFileName
== 'cmd.exe' and FileName == 'powershell.exe' and ProcessCommandLine contains "-e")
| summarize Children = make_list(pack('ChildProcess', FileName, 'CommandLine',
ProcessCommandLine)) by DeviceId, DeviceName, InitiatingProcessParentFileName,
InitiatingProcessFileName, ProcessCommandLine, bin(Timestamp, 1m)
| where array_length(Children) > 1
| project DeviceName, Timestamp, InitiatingProcessParentFileName,
InitiatingProcessFileName, ProcessCommandLine, Children
```

This query works by:

1. Filtering the `DeviceProcessEvents` for those events where an `outlook.exe` process has initiated a `cmd.exe` process, which in turn has initiated a `powershell.exe` process with a "-e" flag in the command line. This flag is often associated with encoded and potentially malicious PowerShell scripts.
2. Summarizing the child processes (if any) for each combination of the fields `DeviceId`, `DeviceName`, `InitiatingProcessParentFileName`, `InitiatingProcessFileName`, `ProcessCommandLine` and the `Timestamp`.
3. Filtering for instances where there is more than one child process. This could indicate unusual or malicious behavior, as multiple PowerShell scripts are being initiated from a single `cmd.exe` process.
4. Finally, projecting or selecting the relevant fields that provide information about the device and the processes involved.

Fields explanation:

Using GenAI for endpoint-based hunting

- `DeviceId` : The unique identifier of the device on which the process events are taking place.
- `DeviceName` : The name of the device.
- `InitiatingProcessParentFileName` : The file name of the parent process that initiated the currently running process (in this case, 'outlook.exe').
- `InitiatingProcessFileName` : The file name of the process that initiated the currently running process (in this case, 'cmd.exe').
- `ProcessCommandLine` : The command line that initiated the current process. The "-e" flag indicates an encoded PowerShell script.
- `Children` : The list of child processes initiated by the `cmd.exe` process.
- `Timestamp` : The time at which the process event was logged.

With this query, you can track the specific behavior you are looking for (outlook.exe -> cmd.exe -> powershell.exe with encoded command line), and identify potential security threats on your network.

Using internal GenAI tools to obtain the query language and speed up the hunting process

Since ClOp Ransomware uses native PowerShell cmdlets, we hunted for the persistence performed by hunting PowerShell scripts containing well-known cmdlets –

`New-ScheduledTaskAction`, `New-ScheduledTask`, `Register-ScheduledTask`, `New-ScheduledTaskTrigger`, and more.

2. In most of the cases where ClOp Ransomware encrypted a machine, the APT group brought open-source and well-known tools into the infected host. These tools were essential for the attacker to use since they are very powerful and have low detection rates. The Threat Hunting team searched for common tools that the ClOp ransomware group is known to use in this attack, including Cobalt Strike, AdFind, Impacket and PsExec.

See the report Appendix for a list of common tools used by attackers, and how CyberProof's threat hunting team identifies them.

The role of the tailored threat intelligence team

The tailored cyber threat intelligence (CTI) team performed a search on the Clear, Deep and Dark Web to collect additional information such as:

- Propagation methods, encryption mechanisms, and communication with its C2 servers
- Any information about new ClOp ransomware campaigns that are being planned
- Targeted campaigns that could impact the client
- Zero-day vulnerabilities being exploited by ClOp ransomware

Root cause analysis reporting

All of the teams contributed to a root cause analysis (RCA) report which covered detection, incident response (containment and eradication), lessons learned, and all areas of decision-making.

This report was structured in a way that allowed both technical and non-technical stakeholders to understand the nature and impact of the ClOp ransomware incident. It also serves as a valuable resource for compliance, and future security planning.

Our recommendations

CIOp ransomware is a growing threat capable of delivering multi-layered ransomware extortion attacks at dangerous scales while bypassing security measures and account protections.

To navigate the threats posed by CIOp effectively, organizations are urged to implement a comprehensive defense strategy that specifically focuses on monitoring for ransomware, thorough investigative processes that unpack and counteract the threat.

This integrated approach, emphasizing proactive detection, detailed analysis, and the strengthening of authentication protocols, equips organizations to enhance their security posture and defend against the sophisticated tactics of CIOp, thus securing their assets against the dynamic spectrum of cyber threats.

To safeguard your organization, the following measures are recommended to prevent a ransomware attack:

The initial defense against ransomware involves ensuring that the ransomware doesn't enter your organization's digital infrastructure. Security teams must be aligned to ensure that threat actors do not have any access points to your organization. To do this:

- **Prevent initial access to your assets:** Limit access controls and administration rights. The increase of remote work has expanded the attack surface, as remote endpoints are more likely to use unsecured connections. These remote connections can serve as entry points for ransomware attacks, allowing unauthorized access to essential systems.
- **Update security products:** Keep endpoint and perimeter security products, such as email gateways and proxy caches, updated with the latest security patches. Validating and updating security products to protect against vulnerabilities can prevent malicious payloads from reaching the end-user.
- **Promote employee awareness:** By educating employees about potential threats and safe practices, organizations can significantly reduce the risk of successful attacks. Cybercriminals often distribute fake emails and other correspondence, and malicious links are rampant. Developing training programs on trusted sources and safe communication can help improve employee awareness.
- **Implement a Zero-Trust policy:** Any account can be compromised, and that means that strict policies must be implemented for all accounts across your organization. Across the organization, the principle of least privilege policy should be implemented, preventing ransomware actors from using a compromised account to move through your network. Only specific employees should be granted access to certain assets and privileges in line with business justifications, to prevent the proliferation of ransomware throughout your organization.

The following Managed Detection and Response (MDR) safeguards are recommended:

- Deploy an Endpoint Detection and Response (EDR) solution throughout your security infrastructure to enhance visibility and support both prevention and investigative efforts
- Implement an Intrusion Prevention System (IPS) to monitor all inbound, outbound, and internal network traffic
- Integrate all security log sources with the Security Information and Event Management (SIEM) system
- Proactively develop a comprehensive incident response plan
- Collaborate with a sophisticated Managed Detection and Response (MDR) provider to conduct simulation exercises



Appendix

CyberProof's threat hunting team's recommendations for identifying common tools used by attackers

The following is a list of four of the tools most commonly used by threat actors. The threat hunting team uses a range of different approaches to identify these tools including the following hunting methods:

1. Cobalt Strike - Cobalt Strike is a red teaming tool featuring covert communication, privilege escalation, and post-exploitation capabilities, essential for in-depth network defense assessments and security evaluations.

- We recommend hunting for cmd.exe or powershell.exe instances loading Cobalt Strike attributed DLL libraries such as beacon.dll. To do so, we can hunt for loaded modules or the process call stack.
- The team should also look for suspicious standard Cobalt Strike named pipes using the postex_* patterns with regex, such as; \postex_0c2a, \postex_e3dc, etc.
- Hunt for uncommon connections with rare port numbers from native windows processes, such as; rundll32.exe, svchost.exe, explorer.exe, etc.

2. AdFind - AdFind is a free tool used to retrieve information from the Active Directory (AD). The information gathered can be hosts and users, likely during the threat actor's reconnaissance phase, from the target network.

- To hunt for AdFind activity the hunters can search for file activity and process activity for AdFind.exe, however, in many cases the tool will be infiltrated with a random name and this approach won't work.
- The better approach would be hunting for process execution containing AdFind cmdlets, such as; "domainlist",

"dcmodes", "adinfo", "trustdmp", "computers_pwdnotreqd", "Domain Admins", "objectcategory=person", "objectcategory=computer", "objectcategory=*". And, the commandline also including the character ">" which is used to save the gathered information into the infected host.

3. Impacket - Impacket is an open-source collection of Python classes for working with network protocols, which is often used for network security audits and penetration testing to create and send network packets, and analyze responses.

- To detect Impacket activity, the Threat Hunting can look for known artifacts such as cmd.exe execution which the commandline contains;

"cmd.exe /C * > * 2>&1"

4. PsExec - PsExec is a lightweight telnet-replacement utility for Windows systems that lets system administrators execute processes on remote systems, offering full interactive use of the remote system's console. Threat actors also use this tools to perform lateral movement and remote code execution.

- PsExec, as default, generates a new service called PSEXESVC on the target machine, an activity that can be flagged in Windows service creation logs with Event IDs 7045 and 4697.
- Assuming telemetry data is accessible, the best approach would be to keep an eye on the specially named pipes that are generated during the process. The Threat Hunting team will hunt for Event ID 5145 containing "*-stdin" OR "*-stdout" OR "*-stderr"

CyberProof's security services

CyberProof, a UST company, delivers global enterprises fast, transparent, and fully managed cloud-native cybersecurity operations and services – keeping enterprises safe and secure as they transition to the cloud and beyond. Using an innovative combination of expert human analysts, virtual analysts, and automations in a fully transparent, platform-enabled service, CyberProof supports, extends, and continually optimizes cybersecurity operations, collaborating with internal security teams in real time.



BRAND
PROTECTION



FRAUD
PREVENTION



REPUTATION
SAFEGUARDING



DATA
PROTECTION



CAMPAIGN
ALERTING



VULNERABILITY
INTEL

CyberProof's advanced services combine expert resources, nation-state-trained security experts, and best-of-breed tools to assist with detailed investigations, root cause analysis, risk mitigation, and proactive threat management. In parallel, we continuously develop new threat detection content, workbooks, and dashboards and maintain existing content.

With CyberProof, you can:

- **Proactively mitigate threats** - CyberProof's **Managed Detection and Response (MDR) service** provides round-the-clock, 24x7 operational monitoring and prompt response by trained analysts, incident triage, in-depth investigations, and escalation of received security incidents to relevant stakeholders. CyberProof's security analysts collect and aggregate security event logs from various security data sources, analyzing new threats and proactively investigating events from on-premises, SaaS, and cloud-native IT infrastructures.
- **Integrate and automate threat intelligence** - Most security teams struggle to keep up with the volume of data that must be reviewed and absorbed. As time is short, threat intelligence reports should be integrated into security operations so that they can be viewed together with other perimeter and site alerts. CyberProof's **Tailored Threat Intelligence service** is fully integrated and provides accurate and actionable insights, enabling clients to better anticipate and react to the changing threat landscape and better manage risks.
- **Leverage threat hunting tools to improve detection and response** - CyberProof's **Advanced Threat Hunting service** proactively searches for and identifies malware and attackers hiding within client networks. Threat hunting strengthens the cybersecurity ecosystem by incorporating a more proactive approach while improving an enterprise's security posture by reducing the attack surface. The team has extensive experience with nation-state cybersecurity activities and a clear focus on threat investigation and isolation of suspicious behavior.
- **Streamlined platform monitoring** - CyberProof's **Security Platform Management service** includes comprehensive security monitoring and threat detection for your organization, offering both hybrid cloud and on-premises solutions where applicable. In addition to SIEM solutions including Sentinel, QRadar, and Splunk Enterprise, CyberProof provides platform monitoring services to help you proactively identify and respond to security incidents while also ensuring the health and performance of your infrastructure. The CyberProof team enhances incident response capabilities with automation and process streamlining for faster response times and more effective incident resolution.
- **Prioritize threats based on risk** - CyberProof's **Vulnerability Management service** is designed to identify, assess, and mitigate security vulnerabilities in an organization's systems and networks. These services involve regular scanning to discover potential weaknesses, followed by prioritization and remediation steps to minimize the risk. By proactively managing vulnerabilities, businesses can enhance their security posture and protect themselves from potential cyber threats.
- **Continuously adapt and optimize** - Your threat coverage and response actions should be continuously improved - by defining, testing, and tuning use cases to the latest threats, security sensors, and technology landscape. CyberProof's **Use Case Management service** evaluates the current threat detection coverage, assesses

the efficacy of deployed use cases, formulates threat detection rules and rapid response measures, and where possible, identifies automation opportunities. This proactive approach aims to mitigate cyber risks, minimize potential impact, and enhance the overall maturity of the company’s cyber defense capabilities, ensuring our clients remain proactive against continually evolving threats.

- **Maximize visibility and flexibility** – As organizations move to the cloud, they ingest ever-increasing volumes of data across an ever-increasing range of data sources. Using the MITRE ATT&CK security framework, CyberProof maximizes visibility and develops custom methods to identify unique threats and vulnerabilities of an organization. Security baselines and detection rules aligned with data sources allow CyberProof’s security teams to highlight gaps in security posture while continuously researching and identifying new threat tactics to update detection rules.



Fortify your enterprise with cloud security transformation. CyberProof, a UST company, helps enterprises migrate to cloud-native security operations with advanced Managed Detection & Response services that allow you to protect, detect, and respond to new and existing cyber threats faster and more effectively. Our team of nation-state trained experts together with our AI virtual assistant SeeMo challenge the status quo in the cybersecurity industry with a risk-based approach that helps mitigate the potential threat to your business. Our mission is to empower your organization to anticipate, adapt, and swiftly counter cyber threats – with our global security operations centers, in-depth expertise, and a portfolio of services including Tailored Threat Intelligence, Advanced Threat Hunting, Use Case Management, and more. See: www.cyberproof.com