

Cyber defenders playbook 2024

EvilProxy

Real-life examples that will empower
your security teams

cyberproof.com





Table of Contents

Why read this report	3
Mitigating an EvilProxy Attack	4
Teams involved	4
The role of the CTI team	4
The role of the Managed EDR team	5
The role of the Threat Hunting team	5
The role of L1 analysts	7
The role of L2 analysts	7
The role of the Digital Forensics and Incident Response (DFIR) team	7
Navigating EvilProxy effectively	9
Our recommendations	9
CyberProof's security services	10
About CyberProof	13

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.

When the client detected an EvilProxy IOC, CyberProof's experts collaborated to

assess, minimize, and prevent potential damage to the client's network and data. 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.

What is EvilProxy?

EvilProxy is a phishing-as-a-service (PhaaS) toolkit designed to bypass two-factor authentication (2FA) protections employed against online services. EvilProxy indicates that adversaries are upgrading their attack arsenal to orchestrate sophisticated phishing campaigns that can defeat existing security safeguards, including targeting public-facing code and package repositories to facilitate supply chain attacks.

How does CyberProof mitigate attacks?

CyberProof's *Better Security, Together* solutions allow you to slash incident response time. We help you mitigate risk by augmenting your 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.

Mitigating an EvilProxy Attack

Teams involved

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

Team	Description
 CTI	<ul style="list-style-type: none">▪ Insights and enrichment▪ OSINT and WEBINT▪ IOC collection and 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 and triage▪ Monitor security perimeters and alerts from client SIEM
 L2 analysts	<ul style="list-style-type: none">▪ Incident response▪ Advanced incident investigation▪ Orchestration of team activities
 Digital Forensics & Incident Response (DFIR)	<ul style="list-style-type: none">▪ In-depth investigation and resolution

The role of the CTI team

After we detected an EvilProxy IOC in one of our client's systems, our CTI team leveraged threat intelligence platforms to learn additional information about any indicators of compromise (IOCs) associated with the client's assets. We checked Reddit threads, other public forums, and social media platforms, looking for information that might have hinted at an attack on our client, and leveraged tools matching IOCs with live

intelligence feeds to enrich the data.

In parallel, we researched the latest vulnerabilities associated with EvilProxy attacks, joined chat rooms where cybercriminals are known to share information, and conducted a deep web search for the organization's data in leaked databases to ascertain if sensitive information was compromised.

Our CTI team leveraged information gleaned from previous EvilProxy attacks and extracted attack vectors, TTPs, and IOCs from a variety of sources and reports, to identify indicators in the organization's environment. We monitored dark web forums and marketplaces for any signs of the organization's data being traded or discussed – checking communications and announcements from known hacker groups who we believed might claim responsibility for the attack. An investigation was conducted to identify any custom malware or tools being distributed on the dark web, that were designed to facilitate EvilProxy attacks.

Our team's objective was to understand the threat posed by the EvilProxy tool and identify IOCs for proactive defense. Examples of relevant IOCs included:

Domain IOC

One abused domain in the attack flow was bs.serving-sys[.]com. This domain is notorious for redirecting users to undesired webpages.

Redirection Patterns

This is a malicious URL pattern that uses YouTube for redirection: [https://www.youtube\[.\]com/attribution_link?c=10570810&u=http://dseapps.web\[.\]app/pi2Pss****3RWO3BM2?id=com.google.android.apps.youtube.music](https://www.youtube[.]com/attribution_link?c=10570810&u=http://dseapps.web[.]app/pi2Pss****3RWO3BM2?id=com.google.android.apps.youtube.music)

Email Decoding

Attackers are known to encode user emails to evade automatic scanning tools. They utilize compromised legitimate websites to decode these emails, which then direct the user to a tailored phishing page.

Geographical Anomalies

Traffic from the IP addresses associated with the attack was redirected to legitimate pages, suggesting a potential origin or a deliberate avoidance strategy by the attackers.

The role of the Managed EDR team

Our EDR team leveraged the information obtained by the CTI team to identify the presence of EvilProxy and determine its scope and reach within the network and across endpoints. The team set up alerts and created and fine-tuned rules to detect unusual or unauthorized proxy server usage. By assessing the impact of EvilProxy on the network and evaluating data integrity, the EDR team performed relevant mitigation steps, where required.

The role of the Threat Hunting team

The threat-hunting team adopted a multi-layered hunt strategy. The team members invested their efforts in both email-based and identity-based hunting, and leveraged the information provided by the CTI team.



Email-based hunting included:

- **Hunting for evidence of suspicious inbox manipulation rules or suspicious email deletion activity:** The Threat Hunting team utilized GenAI capabilities to generate a list of relevant keywords appearing in suspicious emails. This was done because often, after the initial compromise, attackers create inbox rules to delete emails that contain certain keywords.
- **Detecting if the mailboxes of multiple users were configured to forward emails to the same destination:** The team checked for the existence of an attacker-controlled destination mailbox configured to collect mail from multiple compromised user accounts.

Identity-based hunting included:

- **Reviewing any impossible travel activities:** For example, identifying a successful user login from two different countries, within a two-hour period.
- **User identity-related activities from new locations:** For example, identifying activity from countries that are not typically part of the company's usual business interactions.
- **MFA-related information:** The team queried the SIEM to detect accounts that had signed in with a new MFA method, i.e., a method that had been added to the session's account within a timeframe of eight hours.
- **Unfamiliar sign-in properties:** The Threat Hunting team looked for unfamiliar sign-in properties including the ISP, user agent, user's time zone, multiple browsers, use of anonymizer services, and MFA methods. The team also utilized AI capabilities to explore more ideas about relevant fields and properties.

You're a cybersecurity expert working as a threat hunter. You were given the task of hunting for unfamiliar sign-in in azure. What are the properties or fields that you would consider relevant for this type of hunt? an example can be user agent, timezone, etc.

CyberProof CoWorker 7:36



In the process of hunting for unfamiliar sign-ins within an Azure environment, relevant fields that would be considered include:

1. **UserPrincipalName** : This field provides the name of the user attempting to log in. Unfamiliar or unusual usernames could indicate potential malicious activity.
2. **UserAgent** : As you've mentioned, the User Agent is critical. It reveals the software used by the entity attempting the sign-in. If a User Agent does not align with the standard patterns within your environment, it may indicate a potential threat.
3. **Location** or **IPAddress** : Unusual login attempts from unfamiliar locations or IP addresses could indicate potential unauthorized access.
4. **AuthenticationMethodsUsed** : This field specifies the methods used to authenticate during the sign-in process. An unusual authentication method could indicate a threat.
5. **DeviceDetail** : Information about the device used for sign-in can help identify unfamiliar sign-ins. Properties such as **DeviceId**, **OperatingSystem**, and **Browser** are worth checking.
6. **SuccessStatus** : This field indicates whether the sign-in was successful or failed. Repeated failed attempts could suggest potential malicious activities.
7. **Timezone** : The time zone from where the sign-in originates could be useful. If it doesn't align with normal working hours of the user, this could indicate a threat.
8. **ConditionalAccessStatus** : This shows whether a sign-in attempt passed or failed any conditional access policies. A failure could be a sign of an unfamiliar sign-in attempt.
9. **CorrelationId** : Correlation ID helps in aggregating and correlating multiple related events.
10. **ResourceDetails** : This field provides details of the resources that were accessed during the sign-in. Unusual resource access can be an indicator of a potential threat.

These properties can help in the process of threat hunting. However, each environment is unique, so the relevance of each field can vary. Make sure to tailor your hunting strategies to your specific environment and needs.

GenAI tool providing threat hunting direction

The role of L1 analysts

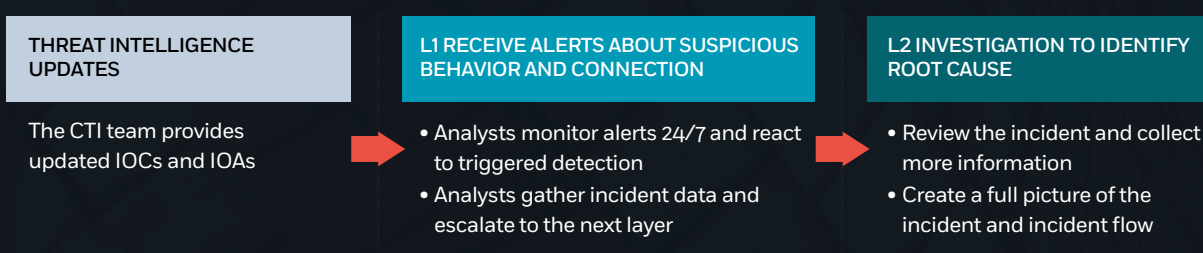
CyberProof's L1 analysts monitored the security perimeters of the client's organization, looking for unusual or suspicious activity such as a surge in phishing emails impersonating popular brands (a common tactic used by EvilProxy) or emails with embedded links that lead to unknown or suspicious domains. They reviewed unusual login attempts, unexpected redirections, or unusual account activities that could be connected to EvilProxy. They also monitored for increased use of TOR or other anonymizing services or unusual network traffic and looked for IOCs associated with EvilProxy, such as known malicious IP addresses, domains, and file hashes.

Our L1 team raised the flag and collaborated with relevant stakeholders in the client's information security team to provide assistance with email filtering - implementing stricter email filtering rules to block phishing emails impersonating popular brands, as observed in recent EvilProxy campaigns. They escalated the next step to the L2 Team.

The role of L2 analysts

The L2 analysts undertook the investigation phase, gathering further information and evidence. The team gathered pertinent data, logs, and network traffic associated with EvilProxy, documenting and preserving evidence to maintain the chain of custody for potential legal or investigative purposes. They utilized threat intelligence sources to enrich their investigation with relevant context and compared findings against known threat intelligence to determine if the incident was part of a broader attack campaign. The team collaborated with other SOC analysts, incident response teams, and external stakeholders to share information and communicate findings to management, stakeholders, and other teams within the organization. They documented findings and provided recommendations for preventing similar incidents in the future.

The L2 analysts recommended to the client team to raise security awareness by conducting regular training to educate employees about the latest phishing techniques used by EvilProxy and how to identify and report suspicious emails.



The role of the Digital Forensics and Incident Response (DFIR) team

CyberProof's DFIR team resolved key investigation questions related to the EvilProxy attack, conducting a thorough assessment of the incident's scope, impact, and criticality to determine the appropriate response level and resource allocation. A comprehensive investigation plan was formulated, outlining objectives, methodologies, and task assignments within our DFIR team.

The DFIR team analyzed phishing emails, identified compromised accounts, and removed malicious artifacts associated with the EvilProxy attack, including any injected

malicious code in widely used projects or reset login sessions to sterilize stolen tokens. Forensic images of affected systems were meticulously created for detailed analysis, preserving the original state of the evidence. Through careful reconstruction, we gained a comprehensive understanding of the incident, including the attack vector, entry point, lateral movement, and extent of compromise. Systems and data were then prioritized based on criticality and relevance to the investigation.

We actively assisted the client in implementing post-investigation remediation steps, such as patching vulnerabilities, enhancing security controls, and revising incident response plans, to fortify your organization's security posture and minimize future risks.

Our DFIR investigation revealed EvilProxy's mechanism of operation: EvilProxy operates by employing reverse proxies to relay authentication requests and user credentials between the target user and the legitimate service website.

Here is a step-by-step breakdown of how the attack works:

- 1. Phishing email:** The attack began with a phishing email sent to the target. The email impersonated popular brands and contained an embedded link.
- 2. Redirection:** When the victim clicked on the embedded link, they were redirected through an open redirection via other websites (e.g., YouTube or SlickDeals), followed by a series of subsequent redirections designed to lower the chances of discovery and analysis.
- 3. EvilProxy phishing page:** Eventually, the victim landed on an EvilProxy phishing page that reverses proxied the legitimate login page of the service being targeted, e.g., Microsoft 365. This phishing page also featured the victim's organization theme to appear authentic.
- 4. Credential harvesting:** As the phishing server proxied the legitimate login form, it stole authentication cookies as soon as a user logged into their account. The victim interacted with the phishing page, believing it to be legitimate, and entered their credentials and 2FA passcodes.
- 5. Bypassing Multi-Factor Authentication (MFA):** Since the user already had to pass MFA challenges when logging into an account, the stolen cookie allowed the threat actors to bypass multi-factor authentication. The attackers gained access to the user's account, just as if they had legitimately logged in.
- 6. Account takeover:** Once the account was compromised, the threat actors added their multi-factor authentication method (via Authenticator App with Notification and Code) to establish persistence in the account.

In this way, EvilProxy enabled cybercriminals to bypass 2FA protections, harvest credentials, and 2FA passcodes, and take over user accounts associated with various online services.

This ability to bypass security measures

and account protections makes EvilProxy a particularly dangerous threat, requiring organizations to adopt higher security awareness, stricter email filtering rules, and robust authentication methods like FIDO-based physical keys.

Navigating EvilProxy effectively

EvilProxy is a growing threat capable of delivering high-quality phishing at dangerous scales while bypassing security measures and account protections.

To navigate the threats posed by EvilProxy effectively, organizations are urged to implement a comprehensive defense strategy that specifically focuses on monitoring for phishing schemes, 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 EvilProxy, thus securing their assets against the dynamic spectrum of cyber threats.

Our recommendations

- ➡ Reinforce your security measures with advanced authentication technologies, such as FIDO-based physical keys.
- ➡ Perform security awareness employee training regularly.
- ➡ To identify suspicious behaviors, follow CTI leads and correlate them with environmental logs.
- ➡ With most companies embracing remote work, it is key to develop specific “impossible travel” detection rules to identify irregularities or anomalies in remote logins.
- ➡ Don't fully trust security products to contain all infections. Learn the behavior of an attack (all IOCs, all IOAs, all used tools, all MITRE techniques) and hunt for it throughout the rest of the environment. This helps identify additional infected endpoints and validates the environment's integrity.
- ➡ During an incident, make sure the threat actor did not tamper with security products.

CyberProof's security services

CyberProof, a UST company, delivers fast, transparent, and fully managed cloud-native cybersecurity operations and services to global enterprises 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



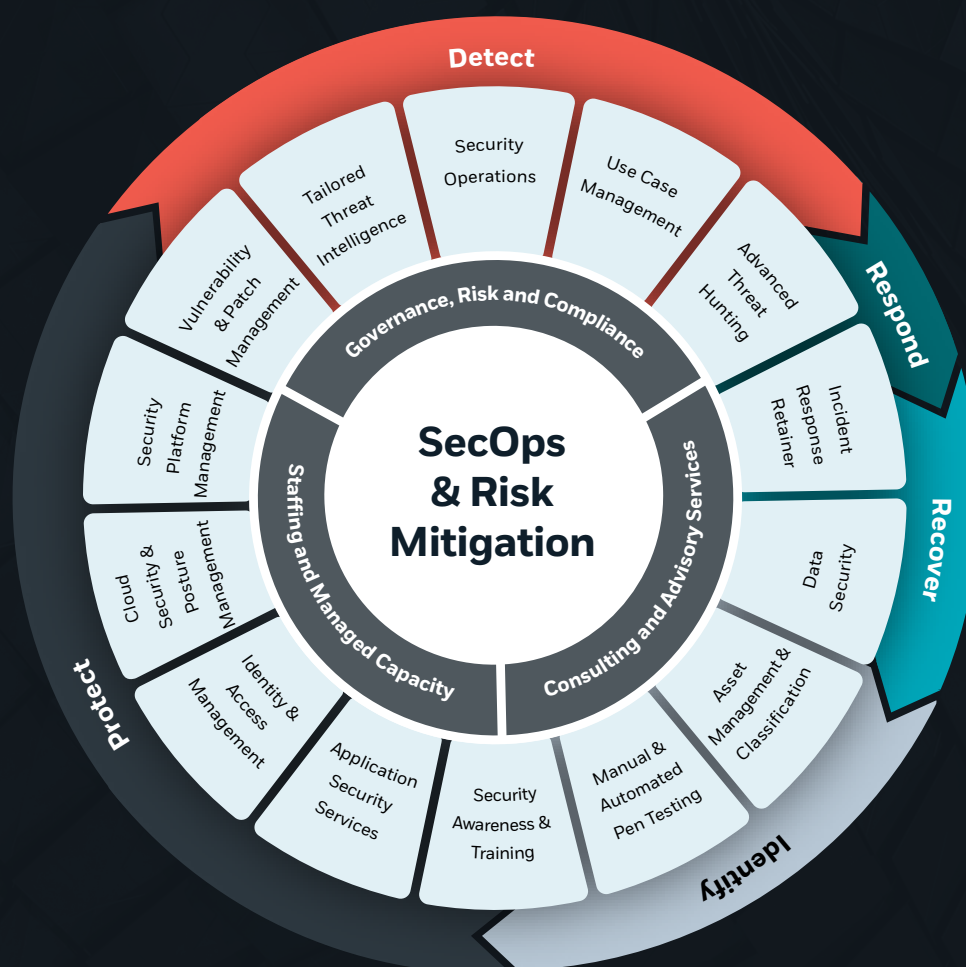
VULNERABILITY
INTEL

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