TIR-20250701 Oyster, Kepavll, and BHO.BJ – Malware to Watch

7/1/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

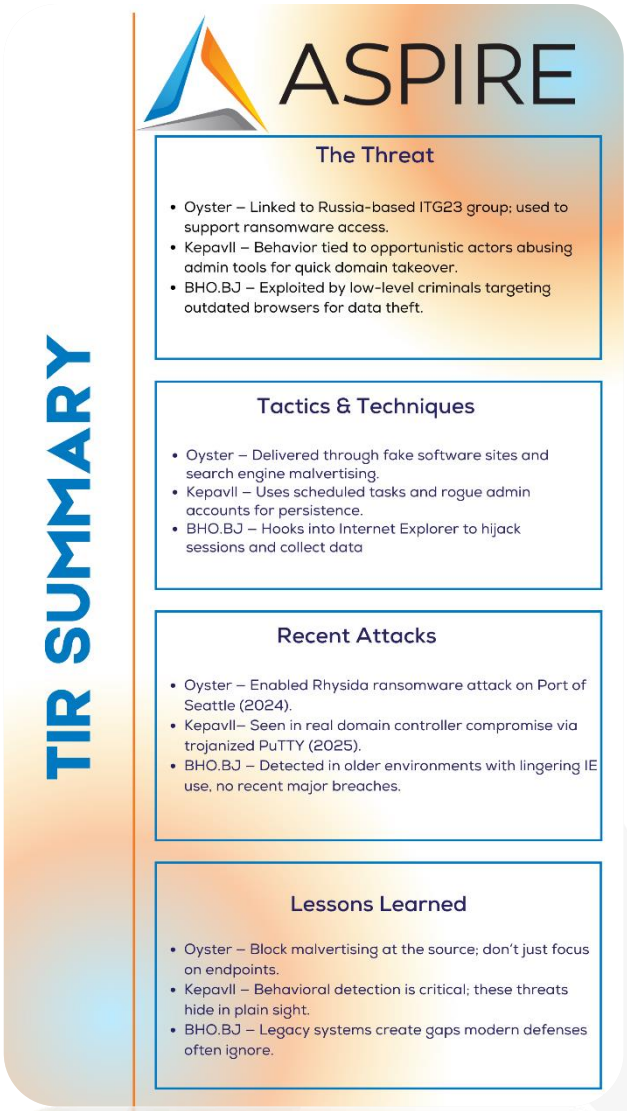
This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

TABLE OF CONTENTS

Executive Summary



In the last couple of years, lesser-known malware has quietly helped attackers break into networks and steal victim data. This report takes a close look at three malware families you might not be familiar with: Oyster, Kepavll, and BHO.BJ. Each works in different ways and has surfaced in different contexts, yet all bring risks that organizations need to take seriously.

Oyster, also known as *Broomstick* or *CleanUpLoader*, was first identified in late 2023 and has been linked to Russia based cybercrime operations, including ITG23 (known for TrickBot). It has been used to support ransomware attacks such as those carried out by the Rhysida ransomware group. Its primary distribution method involves trojanized installers for legitimate software, spread through **malvertising campaigns** that exploit search engine results.

Kepavll, sometimes flagged as Kepavll!rfn isn't a well-defined malware family. It's a label antivirus tools like Microsoft Defender use when they spot suspicious behavior - things like unauthorized software downloads, privilege escalation, or attempts to stay hidden on a system. There isn't much formal research on Kepavll; most of what we know comes from community discussions and

removal guides. What we do know is that it can be used to create unauthorized accounts, move laterally across a network, and stage data for potential theft

BHO.BJ is part of an older class of threats that still show up in systems running outdated technology. It takes advantage of **Browser Helper Objects in Internet Explorer** to hijack browser traffic and gather data. It isn't linked to any known group or campaign, but it's a reminder that legacy software like Internet Explorer can still expose organizations to threats. This report breaks down what we know about each of these threats. We will take a look at how they work, where they've been seen, and what steps you can take to protect your environment.

OYSTER

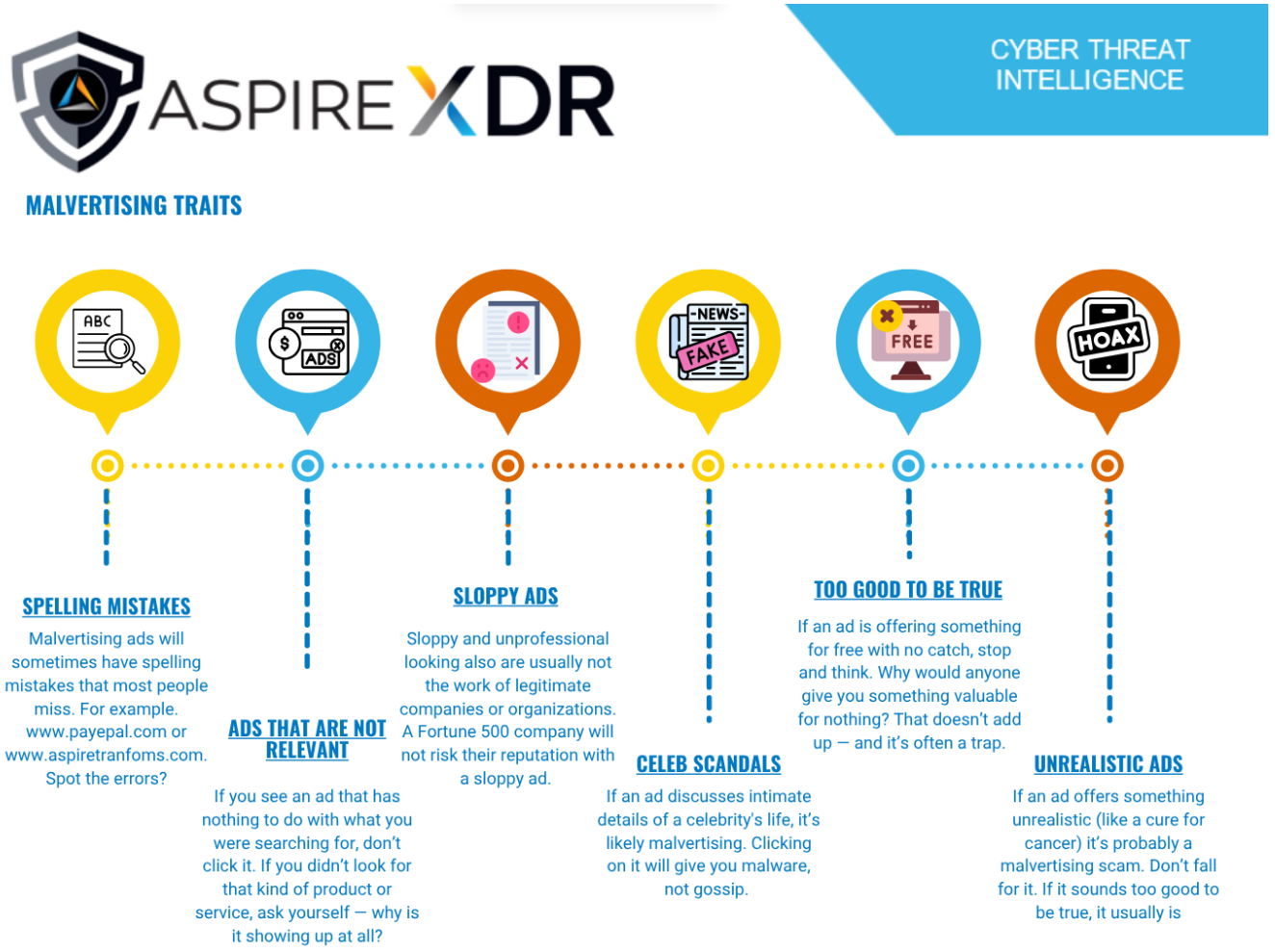
Oyster, also referred to as *Broomstick* or *CleanUpLoader*, was first discovered by IBM researchers in September 2023. It has been linked to the Russia-based ITG23 cybercrime group, which is infamous for developing and distributing TrickBot. Oyster is typically spread through malvertising campaigns that lure users into downloading trojanized installers for legitimate software, such as Microsoft Teams or Google Chrome.

What is Malvertising?

Malvertising is when attackers use online ads to spread malware. These ads can show up on legitimate websites or in search results, and they often look just like normal ads or download links. Visually, malvertising might look like a banner offering a free software download, a pop-up telling you your computer needs an update. It can also be a top search result that takes you to a fake website.

The threat is that it blends in and nothing about the ad itself looks harmful at first glance. But clicking on it can lead to a malicious file or site designed to infect your system. However, there are some tell-tale signs that will give a malvertising campaign away. Below is an example of what a malvertising ad might look like.

Image 1: Malvertising Traits



Oyster has been observed in opportunistic campaigns, with confirmed targeting of U.S. organizations, including the Port of Seattle in 2024, where threat actors used it to support a ransomware attack that disrupted airport operations and delayed flights.

Tactics and Techniques

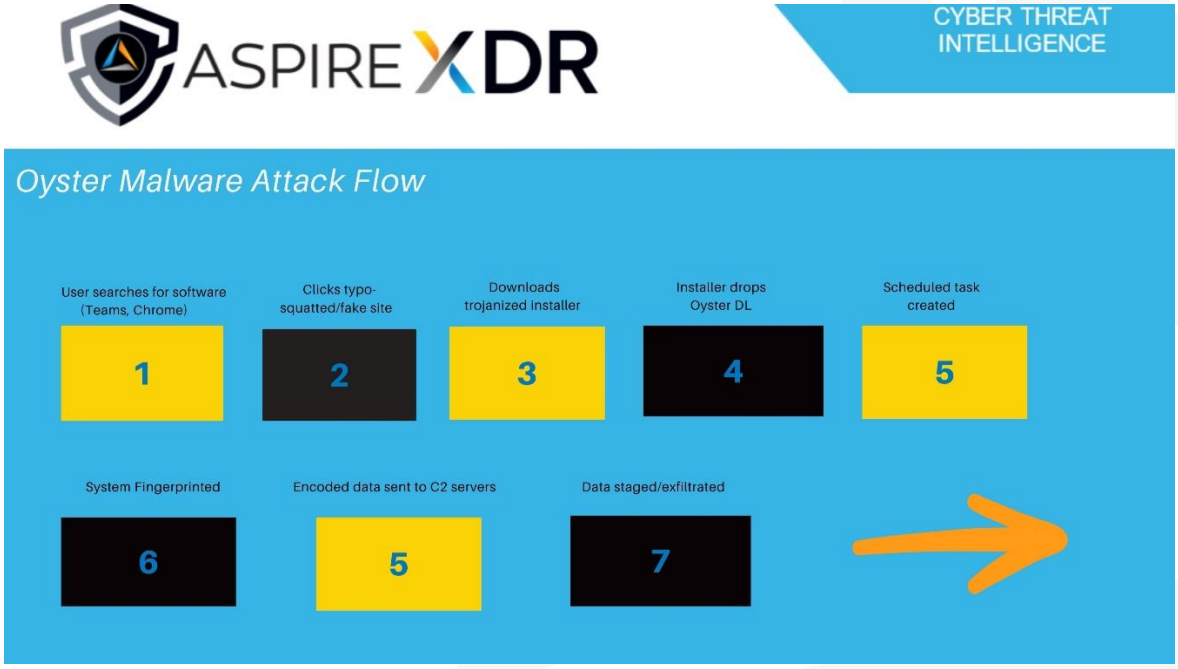
Oyster infections begin with users being tricked into visiting typo-squatted websites that mimic official download pages. These fake sites deploy malicious installers, which drop the Oyster backdoor. The malware achieves persistence by creating scheduled tasks, such as ClearMngs or Security Updater, that repeatedly execute malicious DLL files.

Oyster is capable of host enumeration, collecting information about the domain, user accounts, system configuration, and network settings. It uses encoded HTTP POST requests to communicate with its command-and-control servers. In cases where Oyster has been deployed as part of a larger attack chain, it has facilitated lateral movement via RDP and staged data for potential exfiltration through domains like temp[.]sh and disroot[.]org.

Tools and Attack Flow

Oyster typically arrives through a trojanized installer, such as MSTeamsSetup_c_l_.exe or TMSSetup.exe. These installers drop the backdoor component, CleanUp30.dll or similar DLLs, into temporary directories. Persistence is established through scheduled tasks that invoke rundll32.exe to load these DLLs at regular intervals. The malware fingerprints the host and sends the collected data to hard-coded domains using non-standard encoding. In several incidents, follow-on activity includes the execution of PowerShell scripts, additional payload delivery, and reconnaissance commands aimed at mapping out the target environment.

Image 2: Oyster Attack Flow



Recent Attacks

In August 2024, Oyster was used in an attack against the Port of Seattle as part of a broader campaign by Rhysida ransomware. This attack caused disruptions at Seattle-Tacoma International Airport, leading to delays and operational issues.

More broadly, 2024 saw Oyster deployed in malvertising campaigns that tricked users worldwide into downloading trojanized software, with a significant focus on U.S. based users.

KEPAVLL/KEPAVLL!RFN

Kepavll (also labeled as Kepavll!rfn) is not tied to a documented malware family or threat actor group. The name appears in Microsoft Defender detections, which identify behavior patterns typical of TrojanDownloaders or Remote Access Trojans. The term often reflects heuristic detections rather than a signature matched malware family.

Research on Kepavll is scattered. Most of what's out there comes from forum posts, removal guides, and community reports. What we do know is that the activity linked to Kepavll often involves downloading other malware, setting up persistence, escalating privileges, and helping attackers move through a network

Tactics and Techniques

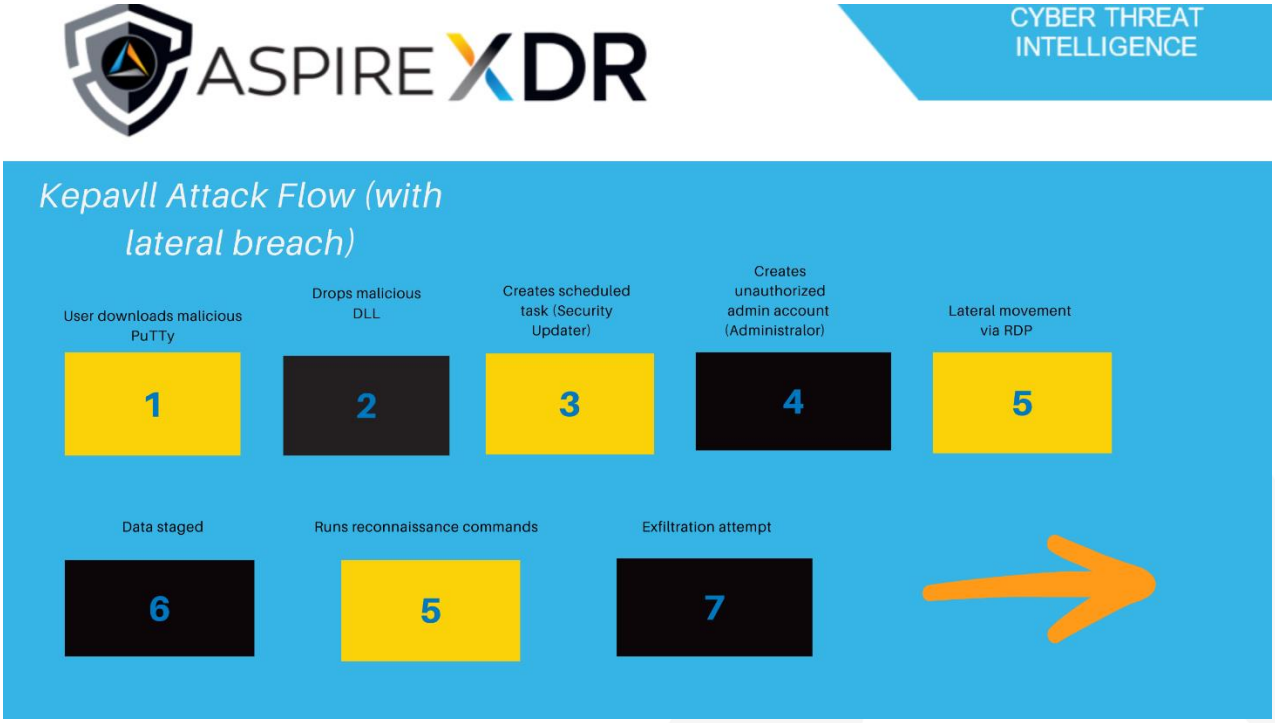
Kepavll-related activity often begins with the download and execution of trojanized software, such as malicious PuTTY installers. These downloads drop DLLs that are executed via rundll32.exe. Persistence is maintained through scheduled tasks like Security Updater that frequently re-execute the malicious DLL. The malware has been seen creating unauthorized administrator accounts, such as the "**Administralor**" account noted in one incident.

The attacker uses RDP for lateral movement. They run commands to list domain groups, find domain controllers, and gather user session details. Data staging for exfiltration has included the creation of .csv and .zip files, with uploads to services like temp[.]sh and disroot[.]org.

Tools and Attack Flow

Incidents involving Kepavll include the use of fake PuTTY executables with revoked digital signatures. These files drop DLLs into temporary directories and set up scheduled tasks to repeatedly invoke malicious code. The attacker creates privileged accounts and moves laterally within the environment. Staged data files are prepared for exfiltration, with suspicious connections made to external file-sharing or command-and-control domains. The use of legitimate tools such as net.exe, nltest.exe, and quser.exe for reconnaissance is a common element of these attacks.

Image 3: KEPAVLL Attack Flow



Recent Attacks

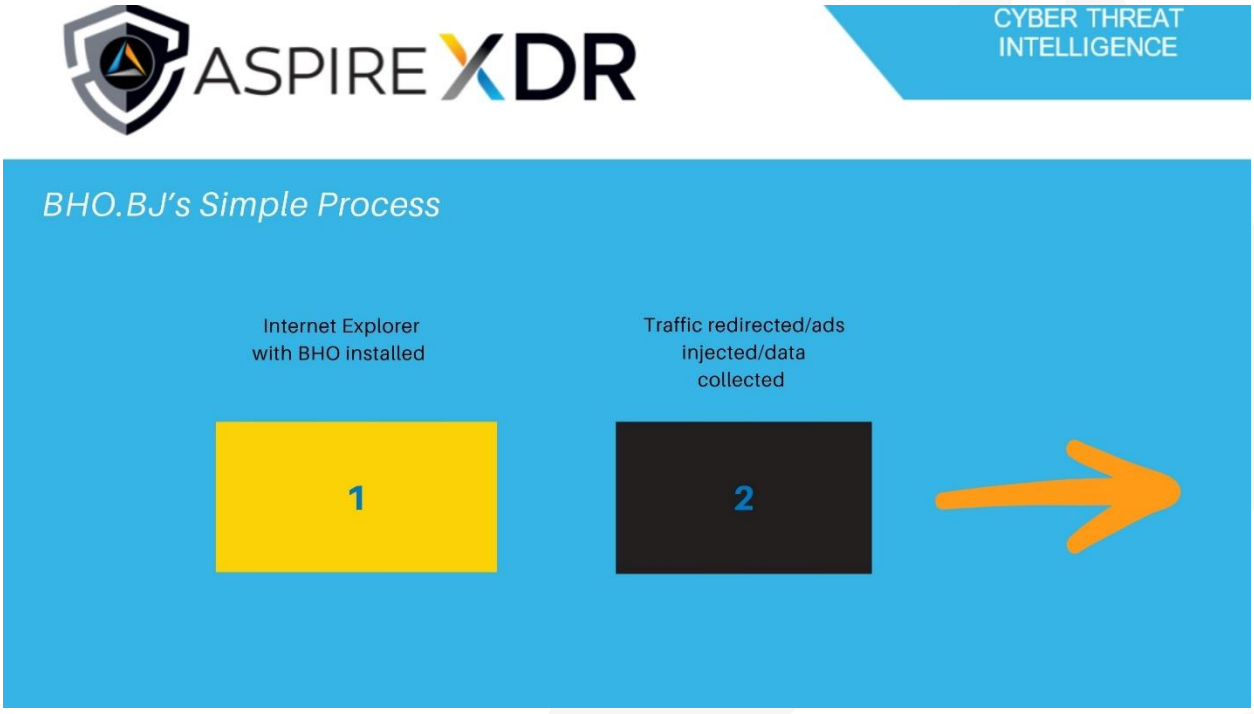
An enterprise case in 2025 involved the download of a malicious PuTTY installer that triggered behaviors consistent with Kepavll. This included unauthorized account creation, lateral movement, data staging, and suspected exfiltration attempts via file-sharing sites.

BHO.BJ

BHO.BJ is a Trojan that abuses the **Browser Helper Object framework** within Internet Explorer to perform malicious actions. BHO.BJ is a detection name used by antivirus tools for a Trojan that abuses Browser Helper Objects (BHOs) in Internet Explorer to hijack browser activity. The “BJ” part of the name is just a label assigned by Microsoft Defender (or similar antivirus vendors) as part of their internal naming convention for detection signatures.

Its exact origin and initial discovery date are not well documented. There is no evidence linking BHO.BJ to any specific threat actor or group. Instead, it appears to be a general-purpose Trojan that can be adapted by various threat actors as needed.

Image 4: BHO.BJ’s Simple Process



***Note*: BHO.BJ hijacks the browser and works inside it, without the kind of multi-step attack chain seen in Oyster and other malware.**

Tactics and Techniques

BHO.BJ functions by embedding itself as a browser extension or helper object. It can redirect traffic, inject advertisements, or capture sensitive data entered through the browser. The malware may alter browser settings or system configurations to maintain persistence and continue its malicious activities without detection.

Tools and Attack Flow

BHO.BJ exploits the BHO architecture to integrate into Internet Explorer. Once installed, it manipulates browser behavior, rerouting traffic or inserting unwanted content. It may also monitor user input to capture sensitive information, depending on the attacker's objectives.

Recent Attacks

There are no recent publicly documented cases or named victims tied to BHO.BJ. Most information comes from antivirus detection records and generic removal guides.

Conclusion and What to Expect Next

Oyster, Kepavll, and BHO.BJ are not the kinds of threats that dominate headlines, and that's exactly what makes them malware to watch. Each of these malware families (or in Kepavll's case, behavioral patterns) succeeds not because of technical sophistication, but because they exploit blind spots.

Oyster's use of malvertising and trojanized software installers exposes how many organizations focus too narrowly on endpoint defense, while neglecting the early stages of an attack chain, which is where users are tricked into downloading malicious files in the first place. The threat isn't just the malware; it's the failure to control how users find and install software.

Kepavll magnifies another weakness that few security programs address well. The overreliance on clear signatures and defined malware families. Kepavll thrives in that gray zone where routine system actions (DLL loading, scheduled task creation, account manipulation) are twisted just enough to support compromise without setting off alarms

in environments that don't fully baseline their own normal activity. These kinds of threats force defenders to think beyond named malware and start looking at the behaviors that allow access and lateral movement, regardless of the tool being used.

BHO.BJ proves how legacy components can quietly keep the door open long after organizations believe those risks are gone. The fact that a malicious Browser Helper Object can still be a threat speaks more to the persistence of forgotten technology than to the code itself. Many companies assume older software isn't dangerous simply because it's outdated, but BHO.BJ proves that old attack surfaces don't disappear.

ASPIRE'S RECOMMENDATIONS

To defend against Oyster

- Block access to typo-squatted and suspicious domains using DNS and network security tools.
- Restrict software downloads to official vendor sites and enforce code signing validation.
- Monitor for unauthorized scheduled tasks and suspicious rundll32.exe activity.
- Analyze outbound network traffic for encoded HTTP POST connections to known C2 infrastructure.
- Implement MFA across all administrative accounts and reduce unnecessary domain admin privileges.
- Conduct regular malvertising awareness training for employees.

To defend against Kepavll

- Block unauthorized scheduled tasks and monitor for unusual rundll32.exe activity.
- Enforce strict controls on software installation, including code-signing validation.

- Limit RDP access to essential systems and require MFA for all remote connections.
- Continuously monitor for domain admin changes and suspicious account creations.
- Block access to known file-sharing and temporary upload domains at the network level.
- Use EDR and SIEM tools to detect lateral movement and reconnaissance activity.

To defend against BHO.BJ

- Remove or disable unnecessary BHOs, especially in legacy systems still running Internet Explorer.
- Transition from Internet Explorer to modern browsers with stronger security controls.
- Deploy endpoint protection with capabilities to detect browser hijacking attempts.
- Educate users on the risks of installing unverified browser add-ons.
- Audit browser configurations in enterprise environments for unauthorized extensions.
- Use application controls to block the installation of legacy browser components.

MITRE MAP

Oyster

Resource Development	T1583.001 – Acquire infrastructure: Domains
Execution	T1059.001 – Command and Scripting Interpreter: PowerShell T1204.002 – Malicious file execution
Persistence	T1053.005 - Scheduled Task/Job: Scheduled Task

Defense Evasion	T1036.005 - Masquerading: Match Legitimate Resource Name or Location
Collection	T1005 - Data from local system
Command and Control	T1132.002 - Data Encoding: Non-Standard Encoding

KepavII

Execution	T1204.002 - User Execution: Malicious File
Persistence	T1053.005 - Scheduled Task/Job: Scheduled Task
Privilege Escalation	T1078 - Valid Accounts
Lateral Movement	T1021.001 - Remote Services: Remote Desktop Protocol
Collection	T1005 - Data from Local System

BHO.BJ

Initial Access	T1176 - Software Extensions
Collection	T1114 – Email Collection
Defense Evasion	T1036 – Masquerading

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all

threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.
  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

Oyster *(via Rapid7)*

SHA-256

- MSTeamsSetup_c_l_.exe
  - 574C70E84ECDAD901385A1EBF38F2EE74C446034E97C33949B52F3A2FDDCD822
- CleanUp30.dll
  - CFC2FE7236DA1609B0DB1B2981CA318BFD5FBBB65C945B5F26DF26D9F948CBB4

Domains

- whereverhomebe[.]com
- supfoundrysettlers[.]us
- retdirectyourman[.]eu

IP Addresses

- 149.248.79[.]62
- 64.95.10[.]243
- 206.166.251[.]114

KepavII *(via internal forensic data from Aspire)*

SHA-256

- PuTTY.exe
  - 80C8A6ECD5619D137AA57DDF252AB5DC9044266FCA87F3E90C5B7F3664C5142F
- twain_96.dll
  - 36726E100520ABC7CD6F2ABD449B3E44E1FB85DD9798E242D57B1ED8B0E843CC
- green.dll
  - 4B45C6AA53E5976D2752F262C15CF74915B26754533E5E6EE4AE5F01F7C9F681

Domains

- puttysystems[.]com
- temp[.]sh
- disroot[.]org

BHO.BJ

No specific IoCs documented publicly yet. Detections rely solely on antivirus signatures (e.g., Microsoft Defender's Trojan:Win32/BHO.BJ).

SUPPORTING DOCUMENTATION

Malvertising Campaign Leads to Execution of Oyster Backdoor | Rapid7 Blog

Oyster Backdoor Spreading via Trojanized Popular Software Downloads

Rhysida Using Oyster Backdoor in Attacks - Arete

Oyster Backdoor Distributes via Trojanized Downloads of Frequently Used Software – Active IOCs Oyster Backdoor Distributes via Trojanized Downloads of Frequently Used Software – Active IOCs - Rewterz

Oyster Backdoor Delivered Through Malvertising Campaign Offering Popular Software Solutions - SpamTitan Email Security

[Solved] 'Kepavll' malware was prevented on a Microsoft SQL server Malware was detected on a Windows Server with Microsoft... | CliffsNotes

Found Trojan:Win32/Kepavll!rfn in a Program - Possible False Positive? - File Detections - Malwarebytes Forums

Heya does anyone have information on the trojan called - Microsoft Community

What is Kepavll!rfn : r/computerviruses

Trojan:Win32/Kepavll!rfn Virus or Windows Defender Being Sensitive? - Microsoft Community

Digital security for your entire family #sandwichgeneration #cybersecurity

Trojan:Win32/BHO.BJ threat description - Microsoft Security Intelligence

BHO: Understanding BHOs and How to Remove or Disable | Lenovo US

Oyster Backdoor Executed Following Malvertising Campaign - Cybersecurity News Everyday

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.