Threat Assessment: Repellent Scorpius, Distributors of Cicada3301 Ransomware

By Navin Thomas, Jerome Tujague

Published: 2024-09-10 · Archived: 2026-04-05 12:36:42 UTC

Executive Summary

Repellent Scorpius is a new ransomware-as-a-service (RaaS) group that distributes Cicada3301 ransomware. The ransomware group appears to have first emerged in May 2024, with a multi-extortion operation.

This report based on Unit 42 Incident Response engagements provides a technical analysis of the ransomware employed by the Repellent Scorpius group. It also covers other tactics, techniques and procedures (TTPs) observed during this attack.

In addition, we discuss Repellent Scorpius' connection to a historical incident involving data exfiltration, predating the group's operation under the Cicada3301 brand, as well as the ransomware group’s plans going forward. Finally, we provide a walkthrough of an updated encryptor obtained through external sources, highlighting the differences from its previous variant. Unit 42 anticipates a rise in Cicada3301 ransomware activity, leading to an increase in the number of victims.

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- Cortex XDR
- Advanced WildFire
- Advanced URL Filtering and Advanced DNS Security
- Prisma Cloud through the Cloud Security Agent (CSA)

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Repellent Scorpius Threat Overview

Repellent Scorpius (distributors of Cicada3301 ransomware) is a new threat group that has recently emerged in the wild. Despite its recent inception, it is quickly picking up pace by setting up an affiliate program and recruiting partners. This has increased its number of victims according to the leak site.

There is an intriguing background associated with the name under which the ransomware group operates. According to Wikipedia, the name 3301 refers to three sets of highly complex and mysterious puzzles that first appeared on 4chan between 2012-2014, all signed with the pseudonym 3301. The third set of these puzzles remains unsolved to this day.

Based on the timeline from a Unit 42 Incident Response engagement, we estimate that the ransomware group began their operations in May 2024. Owing to the absence of other reports, we believe that this may be the beginning of their operations.

While the incidents may have begun around that time, we started to observe leak site activity in June. Despite a lack of activity on the leak site for around a month since June 19, the ransomware group has resumed operations.

Of note, we have observed signs that the group has data obtained in older compromise incidents. It is unclear whether this means that the threat actor previously operated using differently branded ransomware, or whether they have purchased or inherited data from other ransomware groups.

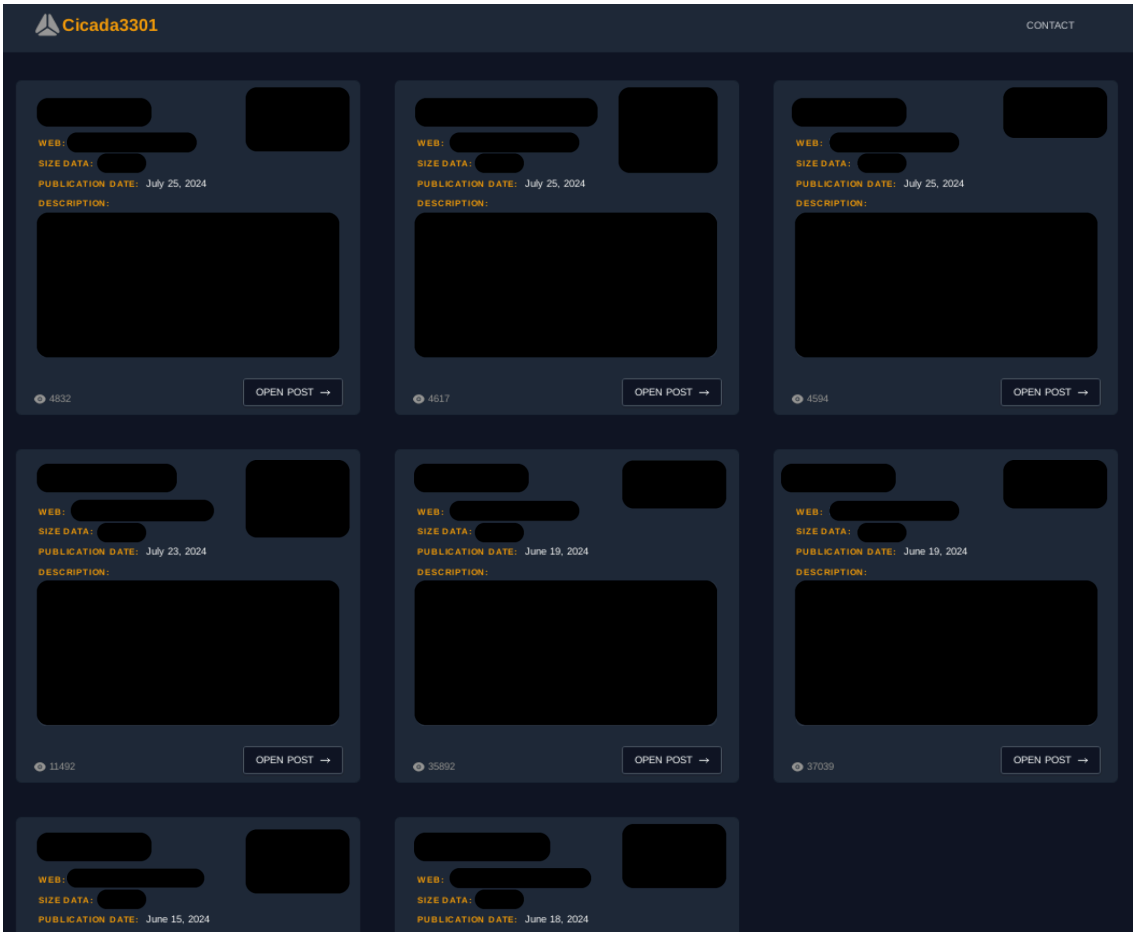

Figure 1. Cicada3301 leak site as of July 2024.

Repellent Scorpius employs a double extortion scheme of encrypting systems. This entails stealing data and threatening to publish it if the victim doesn't pay the ransom.

Unit 42 has evidence to suggest that the Repellent Scorpius operators have developed a RaaS affiliate program. It operates a control panel for affiliates and ransom payment pages for victims, and actively recruits initial access brokers (IAB) and network intruders on Russian-language cybercrime forums.

Given the limited number of victims, it might be too early to suggest whether this ransomware group targets a particular sector or region. Having said that, one of the points in the FAQ section on the affiliate panel website says, "It is strictly prohibited to target the CIS countries." (Translated from Russian.)

KrakenLabs posted a screenshot on X (formerly Twitter), displaying a Russian translated post by the Repellent Scorpius ransomware group on an underground forum to recruit partners for their affiliate program.

Incident Attack Lifecycle

We have mapped the attack stages captured from our incident response engagement to the MITRE ATT&CK® framework tactics, which we summarize below.

Initial Access

Multiple Remote Desktop Protocol (RDP) logon events were captured on a given host. Based on investigation findings and the group's modus operandi, we assess that attackers achieved initial access through stolen credentials, possibly purchased from an IAB.

The public IP address predominantly associated was 103.42.240[.]37, as an RDP server with the hostname: WIN-RMM48SHAUPR. This IP address is associated with a Pakistan-based hosting provider 0DAYHOST (SMC-PRIVATE) LIMITED, while the autonomous system name indicates that Serverius Holding B.V. controls the IP address allocation.

Execution

Unit 42 investigators observed attackers employing a batch script named 1.bat to execute the ransomware payload against multiple hosts within the client network. Details regarding the ransomware payload, along with its arguments, are below.

Figure 2. Batch script with multiple ransomware command executions.

Lateral Movement

PsExec is a legitimate tool that attackers leveraged to execute the ransomware payload against different hosts within the network. The tool is embedded within the ransomware payload and later extracted, which we describe in further detail below. It was executed through the following PowerShell command:

```
powershell -Command C:\Users\Public\psexec0.exe -accepteula -s -d "C:\Users\Public\locker.exe" --no_impl --key <redacted> -p \\<hostname>\C$
```

Collection

Unit 42 investigators found the creation of the following file C:\ProgramData\found_shares.txt. There have been previous occurrences of PowerView, a PowerSploit PowerShell module, storing file share enumeration results in the same file path and multiple ransomware intrusions have leveraged this technique.

Exfiltration

Unit 42 investigators identified Rclone (a legitimate open-source utility) as the tool used for exfiltration. Attackers installed the tool in the *ProgramData* file path (C:\ProgramData\rclone.exe), along with the configuration file (C:\ProgramData\rclone.conf).

We observed 91.238.181[.]238 was the public IP address attackers used for exfiltration activity. This IP address comes from a hosting provider called VDS&VPN services.

The IP address in question has previously been flagged for Cobalt Strike activity (watermark: 674054486) and was potentially linked to other ransomware groups such as Bashful Scorpius (aka Nokoyawa) and Ambitious Scorpius (aka ALPHV/BlackCat) in 2023. This IP address was also observed trying to exploit ScreenConnect vulnerabilities, (CVE-2024-1708 and CVE-2024-1709) in February 2024.

Impact (Encryptor)

The ransomware is a 64-bit binary written in the programing language Rust, which accepts the following command-line arguments:

```
1  USAGE:
2  locker.exe [FLAGS] [OPTIONS]
3  Additional Information:
4  --key Sets the keys for activation (Required parameter)
5  -p, --path Sets the path to the file or directory to be encrypted
6  -s, --sleep Sleep is indicated in seconds
7  --no_local Skip encrypting data stored locally on this device
8  --no_net Skip encryption of network data
9  --no_impl Don't use impersonation
10
11
12
```

```
13
14
15
16
17
```

Figure 2 shows the threat actors used a batch script to execute the ransomware multiple times against a list of hard-coded directory paths in the victim network. The encryptor requires a key parameter to begin execution, which has been redacted from the image.

The binary performs a key validation routine, in which it attempts to decrypt an embedded ransom note using the ChaCha20 stream cipher [PDF].

The ransomware note is Base64-decoded. It is then decrypted using the first 32 bytes of the submitted key as the ChaCha20 secret key and the last 12 bytes of the submitted key as the nonce. Then it is Base64-decoded a final time.

The encryptor will validate the decryption process by checking whether the string ***is_ok*** exists in the decrypted data. If the validation is successful, execution proceeds.

The encryptor contains a legitimate copy of PsExec embedded within itself, which it will extract and save to the location C:\Users\Public\psexec0.exe. The malware will then create a copy of itself in the C:\Users\Public\ directory.

Once copied, it will use the PsExec binary to execute itself several more times, using hard-coded credentials stolen from the victim network during the preceding incursion. This may be an attempt to get the encryptor to run with higher privileges.

```
C:\Users\Public\psexec0.exe -accepteula -s -d "C:\Users\Public\<encryptor>" --no_impl --key <key>

C:\Users\Public\psexec0.exe -accepteula -u <username> -p <password> -s -d "C:\Users\Public\
<encryptor>" --no_impl --key <key>
```

Next, the encryptor will run a series of commands to terminate services and processes, delete shadow copies and disable recovery features among other tasks. A list of the executed commands is below, and a full list of targeted processes and services is in the appendix.

Command	**Purpose**
cmd /C fsutil behavior set SymlinkEvaluation R2L:1	Enables remote to local

	symbolic links
cmd /C fsutil behavior set SymlinkEvaluation R2R:1	Enables remote to remote symbolic links
cmd /C iisreset.exe /stop	Stops Internet Information Services (IIS)
cmd /C vssadmin.exe Delete Shadows /all /quiet	Deletes volume shadow copies using VSSAdmin.exe
cmd /C wmic.exe Shadowcopy Delete	Deletes volume shadow copies using the Windows Management Instrumentation Command-Line (WMIC) utility
cmd /C bcdedit /set {default}	Possibly a misused command, as it requires additional parameters to execute properly
cmd /C bcdedit /set {default} recoveryenabled No	Disables the automatic recover feature for the default boot entry
cmd /C “for /F 'tokens=*' %1 in ('wevtutil.exe el') DO wevtutil.exe cl %1”	Clears Windows Event Logs
cmd /C reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f	Sets the number of concurrent

	network requests to the maximum allowed
cmd /C sc stop <service>	Stops the specified service
cmd /C taskkill /IM <process>* /F	Forcefully terminates the specified process

Once the sample completes the above processes, it begins the encryption routine. By default, the ransomware will check for the existence of drives from A:\ to Z:\. The sample encrypts all files within detected drives, excluding files with specific extensions or files located in directories matching keywords. This information is listed in the appendix.

The encryptor renames files with a new extension before starting the encryption process. In the sample analyzed by Unit 42 the extension was kcr5umw.

The encryption process is composed of two sequences. First, the encryptor will read the contents of the target file, encrypt the contents using ChaCha20 with a randomly generated key secret and nonce bytes, and write the result back to the file. Second, the ChaCha20 key and nonce are encrypted using a hard-coded RSA public key, and the result is appended to the file. Finally, the extension is appended to the end of the encrypted data.

Once encryption of all files is complete, the sample will write the ransom note, named in the format RECOVER-<encrypted_file_extension>-DATA.txt. The contents of the note are as follows.

```
1  ****************************************
2  *** Welcome to Cicada3301 ***
3  ****************************************
4  ** What Happened? **
5  ------------------------------------------
6  Your computers and servers are encrypted, your backups are deleted.
7  We use strong encryption algorithms, so you won't be able to decrypt your data.
8  You can recover everything by purchasing a special data recovery program from us.
9  This program will restore your entire network.
```

```
** Data Leak **

---------------------------------------------

We have downloaded more than %SIZE% GB of your company data.

Contact us, or we will be forced to publish all your data on the Internet

and send it to all regulatory authorities in your country, as well as to your customers, partners, and competitors.

We are ready to:

- Provide you with proof that the data has been stolen;

- Delete all stolen data;

- Help you rebuild your infrastructure and prevent similar attacks in the future;

** What Guarantees? **

---------------------------------------------

Our reputation is of paramount importance to us.

Failure to fulfill our obligations means not working with you, which is against our interests.

Rest assured, our decryption tools have been thoroughly tested and are guaranteed to unlock your data.

Should any problems arise, we are here to support you. As a goodwill gesture,

we are willing to decrypt one file for free.

** How to Contact us? **

---------------------------------------------

Using TOR Browser:

1) You can download and install the TOR browser from this site: https://torproject.org/

2) Open our website: <redacted>

WARNING: DO NOT MODIFY or attempt to restore any files on your own. This can lead to their permanent loss.
```

```
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
```

Links to Historical Incident

Unit 42 is aware of at least one case where Repellent Scorpius had access to a victim's data, which attackers likely took in an incident several years prior. A forensic review of the victim's environment identified no recent signs of compromise. A quick walkthrough of some of the TTPs observed during that incident were as follows:

MITRE Tactic	Description
Execution	• WinRAR to extract certain tools from its archive. • Certutil leveraged for payload download.
Persistence	Multiple scheduled tasks were set up for hourly execution of different commands.
Credential access	We observed the presence of tools such as Mimikatz and Impacket-based executables, primarily used for extracting credentials.
Discovery	• Execution of ADRecon PowerShell script to gather information and extract artifacts from a given Active Directory, and a Rubeus based executable. • Some of the tools or built-in commands attackers used were *wmic, nslookup, ping, ipconfig, net, quser, qwinsta* and SoftPerfect Network Scanner.
Command and control	• Reverse tunnel with adversary server via SSH • PowerShell command to send the victim IP address and hostname to a given hard-coded domain, via POST request. • Multiple other tools were used in this scenario, including *Plink, GOST* and a *SOCKS* proxy tool.

As previously mentioned, it is unclear how the Repellent Scorpius group possessed this data. However, we observed certain overlaps with another attack carried out by an affiliate that deployed BlackCat ransomware, reported in March 2022.

Examples include attackers using ADRecon and SoftPerfect Network Scanner tools, setting up a reverse SSH tunnel and creating similar scheduled tasks. That said, there was no evidence that BlackCat was deployed in this incident, likely due to the fact that different stages of the attack were thwarted.

While we did come across a few filename-based overlaps, we observed no substantial TTP overlaps between the recent ransomware incident and the historical one.

New Version of Encryptor

Unit 42 researchers found an updated Cicada3301 encryptor in late July 2024, which had some differences from the previously analyzed version.

Threat authors added a new command-line argument, --no-note. When this argument is invoked, the encryptor will not write the ransom note to the system.

Instead of running the embedded PsExec binary directly via PowerShell, the encryptor will create a randomly named .bat file in the C:\Users\Public directory, which executes using “cmd.exe /C”. Included in the created .bat file is a line to delete the script after execution is complete.

The most recent samples do not have hard-coded usernames or passwords in the binary but still retain the capability to execute PsExec using these credentials if they exist.

An example of the script is below:

```
C:\Users\Public\psexec0.exe -accepteula -s -d "C:\Users\Public\<encryptor>.exe" --no_impl --key <key> -p <path>

del /Q "C:\Users\Public\<random_10_chars>.bat"
```

Finally, the ransomware developers modified the methods used to stop services and added a PowerShell command to forcibly stop all running virtual machines (VMs) on the target system.

Command	**Action**
powershell -Command "$excludedVMs = @(); Get-VM | Where-Object { $_.Name -notin $excludedVMs } | ForEach-Object { Stop-VM -Name $_.Name -Force -Confirm:$false }"	Forcibly stops all running VMs. VM files that are not shut down before encryption are permanently damaged.
for /F "tokens=2 delims=:" %i in ('sc query state^= all ^| findstr /I <service_name>) do sc stop %i	Stops all services containing the supplied service name.
cmd /C "net stop <serviceName> /y"	Uses the net command to stop a running service. We list new services that the threat stops using this method in the appendix.

Conclusion

Although it may not currently appear to be widespread, Repellent Scorpius is actively hiring IAB and network intruders. It has also recently set up a RaaS affiliate program. Therefore, we can expect to see attackers posting a growing list of active incidents and victims on their leak site in the near future.

The TTPs highlighted here are from specific incident response engagements. Considering that the Cicada3301 ransomware is relatively new, we expect that its TTPs will change and evolve over time.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- The Cicada3301 ransomware is detected and prevented by Cortex XDR.
- Advanced WildFire identifies all known samples mentioned in this article as malicious.
- Advanced URL Filtering and Advanced DNS Security identify known URLs and domains associated with this activity as malicious.
- Prisma Cloud can detect known Cicada3301 ransomware binaries executed within cloud environments through the Cloud Security Agent (CSA).

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Hashes

8ec114b29c7f2406809337b6c68ab30b0b7f0d1647829d56125e84662b84ea74	Cicada3301 encryptor
0260258f6f083aff71c7549a6364cb05d54dd27f40ca1145e064353dd2a9e983	Batch script 1.bat containing multiple Cicada3301 encryptor execution commands
2d73b3aefcfbb47c1a187ddee7a48a21af7c85eb49cbdcb665db07375e36dc33	Cicada3301 encryptor
3969e1a88a063155a6f61b0ca1ac33114c1a39151f3c7dd019084abd30553eab	Cicada3301 encryptor new variant
56e1d092c07322d9dad7d85d773953573cc3294b9e428b3bbbaf935ca4d2f7e7	Cicada3301 encryptor new variant

Infrastructure

- 103.42.240[.]37
- 91.238.181[.]238
- cicadabv7vicyvgz5khl7v2x5yygcgow7ryy6yppwmxii4eoobdaztqd[.]onion/

Additional Resources

- Cicada 3301 – Wikipedia
- The internet mystery that has the world baffled – The Telegraph
- C0015, Campaign C0015 – MITRE ATT&CK
- CONTInuing the Bazar Ransomware Story – The DFIR Report
- Threat Brief: ConnectWise ScreenConnect Vulnerabilities (CVE-2024-1708 and CVE-2024-1709) – Unit 42, Palo Alto Networks

---