

Before ToolShell: Exploring Storm-2603's Previous Ransomware Operations

Key Findings Check Point Research (CPR) conducted a focused analysis of Storm-2603 , a threat actor associated with recent ToolShell exploitations, together with other Chinese APT groups. Storm-2603 utilizes a custom malware Command and Control (C2) framework dubbed internally by the attacker as ak47c2 . This framework includes

at

least two different types of clients: HTTP-based (dubbed by us ak47http) and DNS-based (dubbed by us ak47dns). Based on VirusTotal data, Storm-2603 likely

targeted some organizations in Latin America throughout the first half of 2025, in parallel to attacking organizations in APAC. Some of the actor's TTPs align with many other ransomware groups, and involve open-source tools such as PsExec and masscan. In addition, the threat actors use a custom tool that leverages the BYOVD (Bring Your Own Vulnerable Driver) technique to tamper with endpoint protections. Storm-2603 attacks involved multiple

ransomware families, sometimes bundled together. Those are commonly deployed by abusing DLL hijacking.

Introduction Check Point Research (CPR) has been closely monitoring the ongoing exploitation of a group of Microsoft SharePoint Server vulnerabilities collectively referred to as ToolShell. These active attacks leverage four vulnerabilities CVE-2025-49704 , CVE-2025-49706 , CVE-2025-53770 , and CVE-2025-53771 and are attributed to multiple China affiliated threat actors. Among the threat groups identified by Microsoft , two are known APTs: Linen Typhoon (aka APT27) and Violet Typhoon (aka APT31). Another group is a newly observed, previously undocumented cluster called Storm-2603 . While Microsoft linked this cluster's activity to potential ransomware deployment, it was unable to assess the group's objectives. As part of our ongoing investigation into ToolShell and its associated risks,

we launched a targeted effort to better understand and characterize the threat posed by Storm-2603. Throughout our analysis, we uncovered several files likely tied to Storm-2603 intrusions, offering new insights that correspond to Microsoft's description of the group. In this publication, we provide an in-depth examination of Storm-2603's tactics, techniques, and procedures (TTPs), along with a technical breakdown of the ak47c2, a custom malware framework used in their attacks and their different ransomware payloads. Background Storm-2603 was first mentioned by Microsoft during investigations into a set of attacks on Microsoft SharePoint servers, known as the ToolShell campaign. While some activity was tied to known Chinese affiliated groups like Linen Typhoon (APT27) and Violet Typhoon (APT31), Storm-2603 appeared as a new, previously unreported actor. Microsoft linked the group to Lockbit and Warlock ransomware use. Figure 1 Events associated with Storm-2603. Microsoft's report provided only limited information about Storm-2603, including some of the TTPs associated with it, most of them quite generic. In addition, some of the reported indicators of compromise (IOCs) helped us uncover additional artifacts associated with previous Storm-2603 intrusions. One domain in particular,

update

.updatemicfosoft[.]com, linked to Storm-2603's SharePoint exploitation, turned out to have been used in earlier campaigns dating back to March 2025. In those operations, it served as a C2 server for both DNS tunneling malware and an HTTP backdoor and was part of infrastructure used to deliver LockBit Black and Warlock/x2anylock ransomware. Incidents Our search for cases where the IOCs reported by Microsoft, revealed two incidents in which LockBit Black and WarLock ransomware variants were deployed together, in addition to multiple other tools, mostly open-source. Case #1 Open-source tools, custom backdoor, ransomware In April 2025, a RAR archive named Evidencia.rar was uploaded to VirusTotal. The archive contains several artifacts likely extracted from compromised machines in a Storm-2603 case in a LATAM country. The artifacts in the archive provide a look

at

some of the open-source tools used by the actors in the intrusions which correlates with previous knowledge of the group: masscan Scans large IP

ranges for open ports. WinPcap Captures and filters network traffic on Windows.

PsExec Executes commands on
remote

Windows systems. SharpHostInfo Collects host and domain info on Windows environments. nxc Exploits common vulnerabilities in network

services

. In addition to the open-source tools, the archive also contains the custom backdoor used by the group, as well as its unique ransomware payloads. dnsclient .exe A custom backdoor utilized by Storm-2603 that communicates over DNS tunneling with

update

.updatemicfoso[.]com, a domain associated with the group. See the next section for our analysis of the backdoor.

7z

.exe &

7z

.dll Legitimate

7z

executable side-loading malicious

7z

.dll delivering X2anylock (aka Warlock), a ransomware used by Storm-2603. bbb.msi An installer which uses clink_x86 .exe to side-load clink_dll_x86.dll , leading to the execution of LockBit Black

ransomware . Case #2 Custom AV killer,

ransomware Another MSI file uploaded to VirusTotal in April used a similar deployment method, starting with the MSI installer to launch multiple ransomware strains simultaneously: Figure 2 MSI Multi-Ransomware Deployment. The MSI relies on the following files:

MpCmdRun.exe

& Mpclient.dll Warlock

Ransomware, deployed via DLL-hijacking. clink_x86

.exe & clink_dll_x86.dll LockBit Black

ransomware, deployed via DLL-hijacking. z

.exe & z.dll x2anylock

ransomware, deployed via DLL-hijacking. VMToolsEng

```
.exe Custom Antivirus Terminator. ServiceMouse.sys Vulnerable driver used  
by VMToolsEng  
.exe for killing Antivirus processes. log  
.exe A list of Antivirus processes to kill. msi.bat Executes VMToolsEng  
.exe. 1  
.bat Executes all the needed  
executables and the MSI. AK47  
C2 Framework We attributed two custom backdoors to Storm-2306, both of which  
appear to be part of the framework named AK47  
C2 based on the shared PDB path:
```

```
C:\
```

```
Users\Administrator\Desktop\work\tools\ak47
```

```
c2\ . AK47DNS backdoor The sample appears to be a 64 bit console backdoor  
called dnsclinet (typo in the source) whose debugging symbols point to:
```

```
C:\
```

```
Users\Administrator\Desktop\work\tools\ak47
```

```
c2\dnsclinet-c\dnsclient\x64\Release\dnsclient.pdb When executed, the  
program immediately hides its console window, determines the host computer  
name (defaulting to unknown.local if that fails), and builds a DNS based  
command and control
```

```
payload. It chooses a random five-character session ID, such as H4T14, and  
prefixes it with 1 for task requests or 2 for result uploads (e.g., 1H4T14  
or 2H4T14 ). Each element, such as the task/result tag, a size flag ( a for  
all when the entire message fits into one request), and the computer name,  
is
```

```
XOR
```

```
encoded with the ASCII key VHBD@H , converted to hexadecimal, and  
concatenated with dots before being prepended to the  
C2 domain
```

```
update
```

```
.micfosoft[.]com. This what the overall
```

```
query
```

```
looks like: .a . .
```

```
update
```

```
.micfosoft[.]com DNS TXT and MG (a mail group member record type) record  
lookups (DnsQuery_A) are used to transmit and retrieve data. If the  
C2 server is unreachable, the client simply receives error 9003 (   
DNS_ERROR_RCODE_NAME_ERROR ). Otherwise, the response text is decoded from  
hex,
```

XOR

decrypted, and parsed for the delimiter
:::, which separates metadata from the actual command string. Commands run under

cmd.exe

/c

2>&1

; a built in directive sleep n pauses execution for n seconds. For outputs larger than 0xFF bytes, the backdoor fragments data into 63 byte sub segments. Each DNS

query

then follows: .**s** **t** **p** . . .

update

.micfosoft[.]com Where: s marks segmentation t gives the total segment count, and p indicates the position of the current pair of segments AK47HTTP backdoor HttpClient backdoor has the pdb path

C:\

Users\Administrator\Desktop\work\tools\ak47

c2\httpClient-cpp\x64\Release\httpClient-cpp.pdb and uses plain HTTP instead of DNS for the

C2. It is built as a 64 bit console program that also immediately hides its window on launch. On start up, the malware gathers the host computer name (similar to the DNS version, it defaults to unknown.local), then builds a JSON object with the fields

cmd

,

cmd

_id , fqdn , result , and type . For a task request, the object looks like this: { "

cmd

": " ",

cmd

_id": "", "fqdn": " ", "result": "", "type": "task" } After the host executes a command, the result is sent back with type: result . Before transmission, the entire JSON blob is

XOR

encrypted with the ASCII key VHBD@H , converted to hexadecimal, and placed in the body of an HTTP POST to / with generic headers (Content Type: text/plain, Accept: */*) . The

C2 replies with a similarly encoded JSON where the

cmd

field contains the next command. The implant executes it via

cmd.exe

/c

2>&1

and returns the output.

Ransomware We identified that during these attacks, several types of ransomware were deployed simultaneously. One is regular LockBit Black , and the second uses the.x2anylock extension. This extension was later used by the Warlock

ransomware operator, mentioned in Microsoft s report on the SharePoint exploitation. The Warlock ransom note is usually saved as

How to decrypt my data.txt and looks like this: Figure 3 Warlock Group ransom note. The ransom notes for all

ransomware strains deployed by Storm-2603 are named

How to decrypt my data.log (x2anylock) or .README.txt (LockBit Black) and have the same short content: Your decrypt ID: [redacted] Tox ID Support: 3DCE[redacted] Email Support:

[redacted]@proton.me,[redacted]@proton.me,[redacted]@proton.me You can contact us in email or qtox. This ransom note s name

How to decrypt my data.log appeared in a recent LinkedIn post by Huntress, describing the case where multiple

ransomware families were deployed together against the same target. While not a new tactic , this approach is rarely observed among established

ransomware groups. Antivirus Terminator An important part of the infection package described earlier is called Antivirus Terminator. It is a custom command line tool abusing a third-party signed legitimate driver to kill processes. From what we can see, it s been in the wild since

at

least late 2024. The tool requires administrative privileges on the infected machine. The screenshot below shows how the listing is displayed in the console when the tool is run without parameters: Figure 4 Antivirus Terminator supported arguments when run without parameters. The tool first creates a service called ServiceMouse , where the path to the service binary file is ServiceMouse.sys from the package. Figure 5 Antivirus Terminator installs third-party service. Next, the tool communicates with the

installed service via IO

control

code 0x99000050 , which is responsible for killing processes. The tool also has more capabilities, like deleting files and uninstalling drivers, and these use different IO

control

codes (0x990000D0 and 0x990001D0). Figure 6 Antivirus Terminator kills process using third-party driver. The supplied third-party driver is a legitimate and signed component of Antiy System In-Depth Analysis Toolkit, originally named AToolsKrn164.sys . The toolkit was developed by Antiy Labs, a Chinese security vendor, and features a graphical user interface that allows users, among others, to interact with and manipulate processes. The ability to kill processes is the most important feature which is abused by threat actors in this particular case. Figure 7 Antiy System In-Depth Analysis Tookit GUI. The following piece of code in the driver handles the IO

control

code 0x99000050 mentioned above: Figure 8 IO

control

code processing in the Antiy driver. The second function is the piece of code responsible for killing a process with a given PID. Figure 9 Killing processes in the Antiy driver. Summary In this report we analyze Storm-2603 , a relatively new

threat actor first mentioned by Microsoft during investigations into the ToolShell

campaign targeting SharePoint servers. While some of the exploitation activity was tied to known Chinese

APT groups, Storm-2603 stood out as a previously undocumented group linked to

ransomware deployment. By examining infrastructure indicators shared in public reporting, we were able to connect this actor to earlier campaigns involving LockBit Black and Warlock/X2anylock

ransomware, dating back to

at

least March 2025. These earlier attacks used similar infrastructure and tools, including DNS tunneling and HTTP-based backdoors. Interestingly, multiple

ransomware variants were deployed in the same attack. This behavior, along with the overlap in techniques, helps us better understand how Storm-2603

operates IOCs updatemicfoso[.]com microsfot[.]org
f711b14efb7792033b7ac954ebcfaec8141eb0abafe9c17e769ff96e8fecdf3
035998b724044d20d583ffa393907c7fef11ad8b93b4d423ad8cb8e53f248b7
abb0fa128d3a75e69b59fe0391c1158eb84a799ddb0abc55d2d6be3511ef0ea1
3b013d5aec75bf8aab2423d0f56605c3860a8fb4f343089a9a8813b15ecc550
dbf5ee8d232ebce4cd25c0574d3a1ab3aa7c9caf9709047a6790e94d810377de
1eb914c09c873f0a7bcf81475ab0f6bdfacc6b63bf7e5f2dbf19295106af192
d6da885c90a5d1fb88d0a3f0b5d9817a82d5772d5510a0773c80ca581ce2486d
0f4b0d65468fe3e5c8fb4bb07ed75d4762e722a60136e377bdad7ef06d9d7
c22 f01675f9ca00da067bdb1812bf829f09ccf5658b87d3326d6fddd773df352574
1eb914c09c873f0a7bcf81475ab0f6bdfacc6b63bf7e5f2dbf19295106af192
8f58da414ec4cdad2f6ac86c19e0a806886c63cfdf1fbbb5a0713dce8a0164c5
24480dbe306597dalba393b6e30d542673066f98826cc07ac4b9033137f37dbf
aa25646ea17ae33285203
c225386304de1fe4155be44bb86deb154b87b47e3fb
b5a78616f709859a0d9f830d28ff2f9dbbb2387df1753739407917e96dadf6b0
c27b725ff66fdfb11dd6487a3815d1d1eba89d61b0e919e4d06ed3ac6a74fe94
eaec6b1b23c4450d1d0a7d409d3f21e8a4a171a9e9b82bb8ef2c05a2f7435e9c
257fed1516ae5fe1b63eae55389e8464f47172154297496e6f4ef13c19a26505
ceec1a2df81905f68c7ebe986e378fec0805aebdc13de09a4033be48ba66da8b
55a246576af6f6212
c26ef78be5dd8f83e78dd45aea97bb505d8ceelaeef6f17
aca888bbb300f75d69dd56bc22f87d0ed4e0f6b8ed5421ef26fc3523980b64ad
f06fe1c3e882092a23002bed3e170da7b64e6b4475acdedea1433a874b10afdf
7c31d43b30bda3a891f0332ee5b1cf610cdc9ecf772cea9b073ac905d886990d The post
Before ToolShell: Exploring Storm-2603 s Previous
Ransomware Operations appeared first on Check Point Research .