Ind.Cyber.Sec
Letters

Volume 02, Issue 04. 2025, December 16

Profiling Warlock Ransomware Group

Prof. Dr. Luiz Fernando Freitas-Gutierres

linkedin.com/in/lffreitas-gutierres

github.com/substationworm

luiz.gutierres@ufsm.br

Introduction

Since the second quarter of 2025 (April–June), Dragos has identified the ransomware group known as Warlock as an emerging threat to both corporate and industrial organizations[1]. Notably, Dragos reported that during the third quarter of 2025 (July–September), the Warlock group was responsible for 18 confirmed incidents, affecting victims across sectors such as aerospace, maritime, equipment manufacturing, pharmaceuticals, and petrochemicals[2]. Rising prominently within the ransomware ecosystem in mid-2025, Warlock has demonstrated operational capability in both the impact severity and attack volume of its campaigns[3]. To date, a total of 78 victims have been publicly recorded on ransomware.live.

The Warlock group operates under a ransomware-as-a-service (RaaS) model, typically employing a double-extortion strategy against its targets. Warlock has demonstrated advanced exploitation capabilities, including the use of zero-day vulnerabilities[4], such as the "ToolShell" zero-day impacting on-premises Microsoft SharePoint servers prior to public disclosure (CVE-2025-53770, CVSS v3.1 score 9.8, in conjunction with CVE-2025-53771), as well as other vulnerabilities (e.g., CVE-2025-49704 and CVE-2025-49706). Beyond initial compromise, Warlock's operations frequently result in operational disruption, data exfiltration and exposure on Darknet, reputational damage, and financial losses. The group deploys a Warlock ransomware payload, in which victim files are encrypted and typically appended with extensions such as `.x2anylock`[5], while volume shadow copies and system backups are deleted to impede recovery efforts.

Given its elevated cyber risk to organizations, particularly critical infrastructures and entities associated with the industrial and energy sectors, the fourth issue of the 2025 volume of Ind.Cyber.Sec Letters investigates the Warlock ransomware group through the use of StealthMole's platform trackers, combined with open-source intelligence (OSINT) techniques. The study then presents its key findings, beginning with the analysis of information attributed to the online persona `cnkjasdfgd`[6], who announced the recruitment of cybercriminals for the Warlock group on a Russian-language forum on June 10, 2025. Subsequently, the mapped threat group infrastructure is detailed, followed by the documentation of victims using StealthMole's ransomware monitoring tracker. The fourth issue concludes with observations regarding indicators linked to the group, followed by final remarks.

The Online Persona 'cnkjasdfgd'

As observed through StealthMole's Dark Web tracker, the online persona `cnkjasdfgd` was active on the Russian-language forum `RAMP4u[.]io` from at least April through August 2025. In an recruitment post dated June 10, 2025, titled "*If you want a Lamborghini,please contact me*," `cnkjasdfgd` presents themself as a member of what is described as "(...) *a mature hacking organization, we have many attack cases* (...)," subsequently providing a Tor uniform resource locator (URL) which is no longer active, `elqfbcx5no<redacted>2meim6cbqd[.]onion`, advertised

[1] Alamri, A. H., & Mooney, A. (2025, August 15). *Dragos Industrial Ransomware Analysis: Q2 2025*. Dragos. Link

[2] Alamri, A. H., & Mooney, A. (2025, December 9). *Dragos Industrial Ransomware Analysis: Q3 2025*. Dragos. Link

[3] Quorum Cyber. (2025, August 21). *Threat Intelligence – Threat Actor Profile: Warlock Group*. Link

[4] Halcyon Ransomware Research Center. (2025). *Warlock: Professional Development, China Ties, and the Multiple Variants it Planned from the Start*. Link

[5] Check Point Research. (2025, July 31). *Before ToolShell: Exploring Storm-2603's Previous Ransomware Operations*. Link

[6] Li, R., Moutos, J. (2025, August 25). *Warlock Ransomware Group Targets Global Industries via RaaS Affiliates*. Link

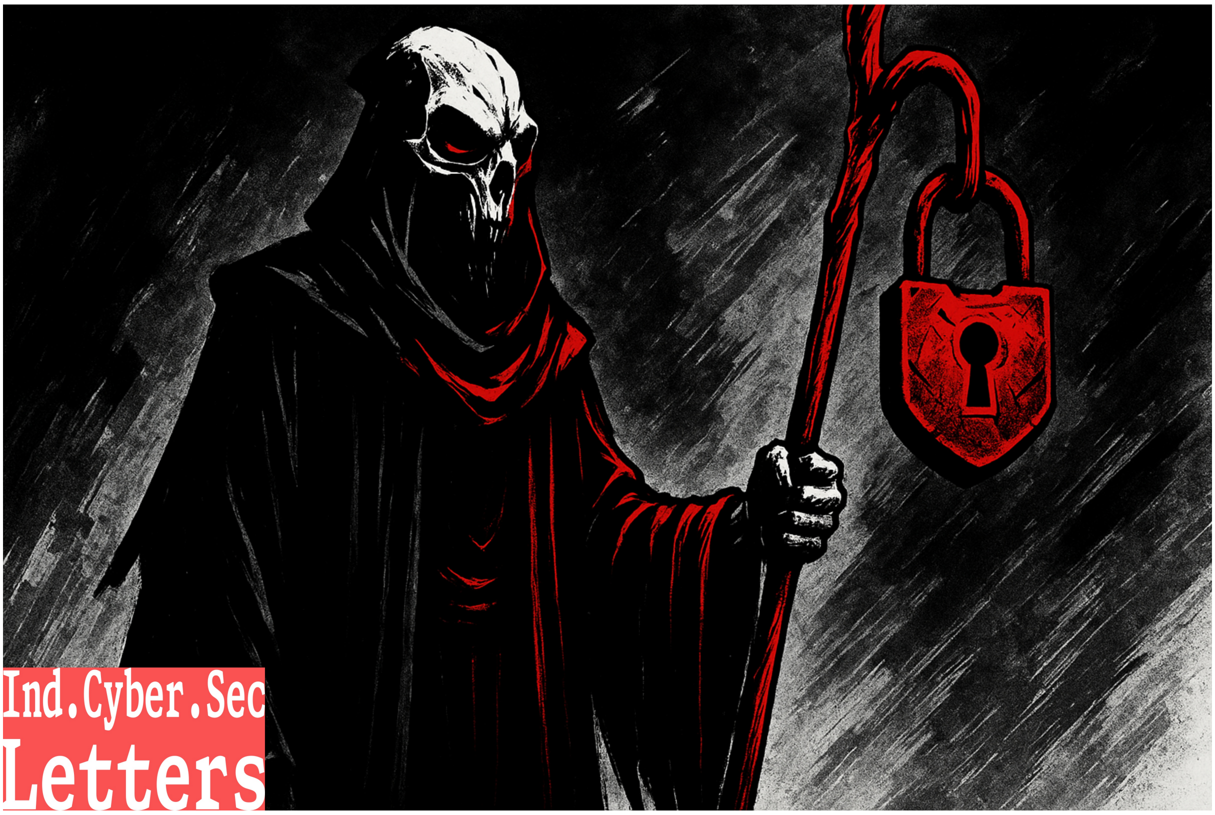


Figure 1. First artwork for Issue 04, Volume 02 of the Ind.Cyber.Sec Letters.

as the WarLock Client Data Leak Show. The post concludes by inviting interested parties to cooperate.

On June 1, 2025, *cnkjasdfgd* published two requests on *RAMP4u[.]io*. The first sought to purchase information on vulnerabilities affecting enterprise technologies, including VMware ESXi, VMware vCenter Server, Veeam Backup & Replication, Microsoft Exchange Server, Microsoft SharePoint, Internet information services (IIS), and Microsoft Active Directory. The second request focused on the acquisition of tools or techniques capable of disabling or bypassing antivirus (AV) and endpoint detection and response (EDR) solutions, indicating an interest in defense evasion capabilities. On July 6, 2025, *cnkjasdfgd* responded to a post written in Russian by *bless<redacted>*, which offered Outlook web app (OWA) access for multiple organizations, with prices starting at USD 100 per instance, requesting further contact via Tox.

On August 15, 2025, *cnkjasdfgd* offered for sale more than one million documents allegedly exfiltrated from Colt Technology Services, a multinational telecommunications company headquartered in London, United Kingdom. According to the post, *cnkjasdfgd*, acting on behalf of the Warlock group, claimed that the dataset includes employee data, financial records, customer contract information, internal executive personal data, employee personally identifiable information (PII), network architecture documentation, software development materials, and executive email data. The actor further stated that a file inventory, *colt-filelist.txt*—comprising 400,987 lines of file names—was made available via the Tor URL *ocwjy4ynmp<redacted>zoep2rbyid.onion/files.html?clientId=<redacted>*. In addition, a Tox ID (*3DCE1C4349<redacted>51FA3B694A*) was provided as a contact point for parties interested in purchasing the data or seeking additional information.

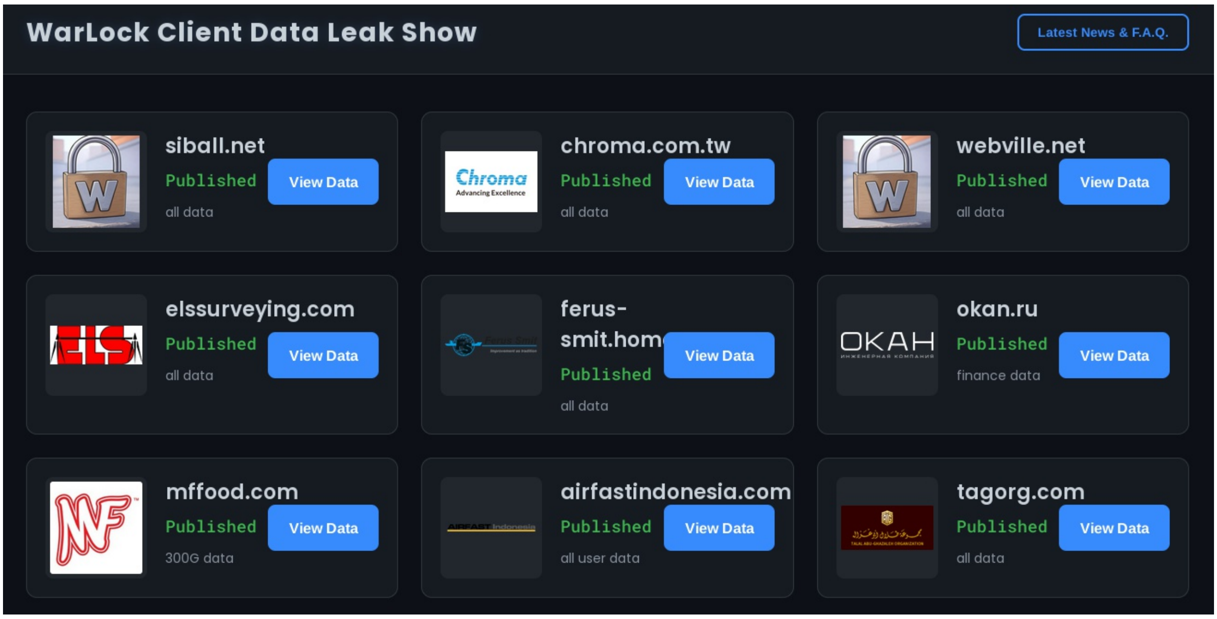
On August 16, 2025, the *cnkjasdfgd* announced the alleged compromise of Orange S.A., one of the largest telecommunications companies in France. In a post published on *RAMP4u[.]io*, cnkjasdfgd issued a ransom demand, threatening to leak sensitive data and to selectively disclose information should payment not be made. The actor additionally provided a Tor URL, ocwjy4ynmp<redacted>zoep2rbyid.onion/files.html?clientId=<redacted>, which directed to a Client File System purportedly containing files belonging to the victim. Within this repository, files named 4e162b1e06<redacted>61fc145395.txt, SCD-<redacted>.txt, and DFS-<redacted>.txt were observed, each comprising extensive listings of directories and files. Analysis of this material is consistent with a file/application server integrated into an Active Directory environment, encompassing backup functions (including structured query language [SQL] database backups, full system images, Microsoft Azure DevOps configuration data, and potentially Microsfot Active Directory domain services/domain controller artifacts), Microsoft Power BI assets, DevOps-related resources, personal data storage, corporate application logs, administrative tools, and legacy on-premises Microsoft SharePoint content (versions 2013 and 2016). Among the compromised materials, the repository also appears to contain documentation consistent with a governance project or audit, linked to a contractual relationship with Airbus. According to a statement published on the threat actors' site, the exposed repository represents only a sample of the compromised data, while access to the complete dataset is offered for sale to interested parties.

On August 18, 2025, in another post on RAMP4u[.]io, the online persona cnkjasdfgd, acting on behalf of the Warlock group, offered 150 GB of data—comprising 626,202 files—allegedly associated with Infoniqa for USD 100,000. On August 20, 2025, the threat actor similarly advertised data purportedly belonging to Cleary Building Corp. Since that time, no additional activity attributed to cnkjasdfgd on RAMP4u[.]io has been recorded by StealthMole's platform, and no corroborating footprints of this online persona have been identified on other Darknet forums.

Threat Group Infrastructure

The Warlock ransomware group operates a Darknet leak site titled WarLock Client Data Leak Show. This site—illustrated by a screenshot of zfytizegsz<redacted>ewviqqh7yd[.]onion presented in Figure 2—displays a list of alleged victims, some of whom are provided with access to sample data, while others are associated with full data access. The site also includes a Latest News & F.A.Q section, as shown in Figure 3. Within this section, the threat actors present guidance purportedly aimed at minimizing damage and losses following a cyberattack, while explicitly advocating for the prompt payment of the ransom. This section also reproduces the same text originally posted by the online persona cnkjasdfgd on the RAMP4u[.]io forum on June 1, 2025, in which interest was expressed in acquiring vulnerability information and malicious software. This reuse of content further reinforces the association between cnkjasdfgd and the Warlock group. Similarly, the site features text corresponding to the August 15, 2025 post in which data allegedly belonging to Colt Technology Services was offered for sale

Although this statement should be treated with caution and cannot be considered reliable, the Latest News & F.A.Q. section of the Warlock group's leak site asserts that, should any of its affiliates have targeted a "(...) *non-profit public welfare organization serving people with disabilities or other special needs* (...)," a decryption tool would be provided free of charge, and the group would allegedly offer assistance in system restoration and in remediating the exploited vulnerabilities. From an analytical perspective, the language employed suggests a lack of centralized operational control over individual attackers, implying that targeting decisions may



WarLock Client Data Leak Show

Latest News & F.A.Q.

siball.net
Published
View Data
all data

chroma.com.tw
Published
View Data
all data

webville.net
Published
View Data
all data

elssurveying.com
Published
View Data
all data

ferus-smit.hom
Published
View Data
all data

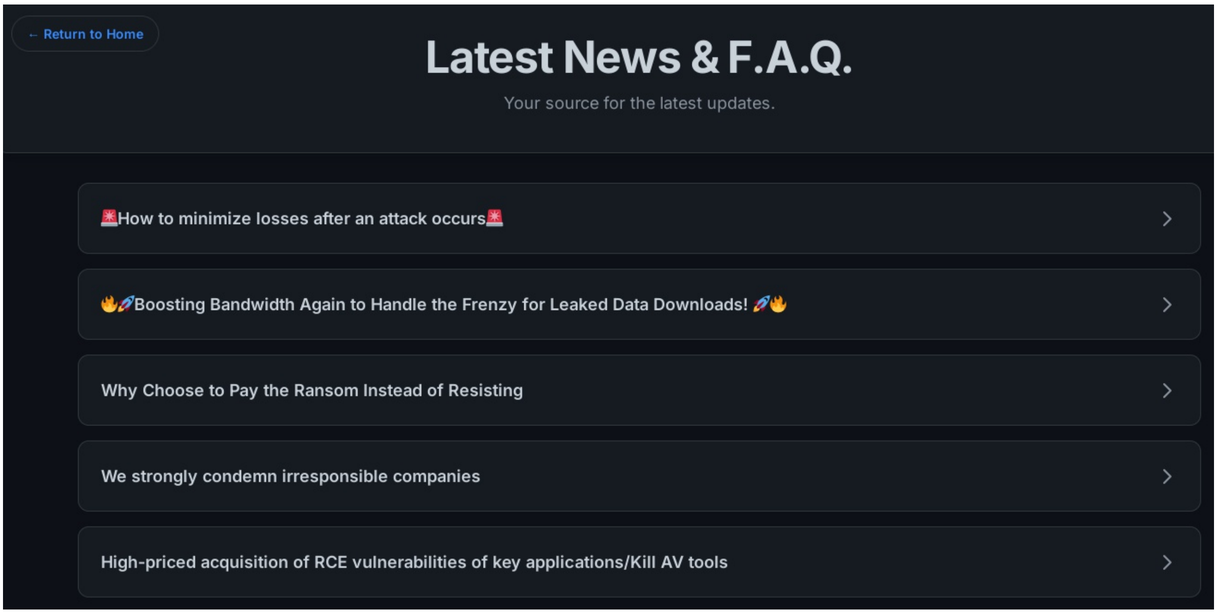
okan.ru
Published
View Data
finance data

mffood.com
Published
View Data
300G data

airfastindonesia.com
Published
View Data
all user data

tagorg.com
Published
View Data
all data

Figure 2. Screenshot of the WarLock Client Data Leak Show.



← Return to Home

Latest News & F.A.Q.

Your source for the latest updates.

🚨How to minimize losses after an attack occurs🚨 ›

🔥🚀Boosting Bandwidth Again to Handle the Frenzy for Leaked Data Downloads! 🚀🔥 ›

Why Choose to Pay the Ransom Instead of Resisting ›

We strongly condemn irresponsible companies ›

High-priced acquisition of RCE vulnerabilities of key applications/Kill AV tools ›

Figure 3. Latest News & F.A.Q. section of the WarLock Client Data Leak Show.

be made autonomously by affiliates. This dynamic is strongly indicative of a RaaS operating model, in which the core group provides tooling and infrastructure while affiliates independently conduct intrusions, select victims, and execute attacks.

The WarLock Client Data Leak Show has previously been hosted on, or remains accessible through, the following Tor (`[.]onion`) domains:

- `elqfbcx5no<redacted>2meim6cbqd[.]onion` (inactive at the time of analysis).
- `ocwjy4ynmp<redacted>zoep2rbyid[.]onion`.
- `zfytizegsz<redacted>ewviqqh7yd[.]onion`.
- `warlockhga<redacted>h64s4vsuyd[.]onion`.
- `warlock4fa<redacted>aerm5zhaqd[.]onion`.
- `warlock6d4<redacted>xlcwmbuuyd[.]onion`.

- warlockhga<redacted>h64s4vsuyd[.]onion.
- warlockmdu<redacted>uy2fiqblad[.]onion.
- warlockoac<redacted>iujfea4yyd[.]onion.
- warlock5zl<redacted>idgxzjc6id[.]onion.

Across both the posts published on the RAMP4u[.]io forum and the information disclosed through associated Tor domains, at least three Tox IDs are notable:

- 3DCE1C4349<redacted>51FA3B694A.
- F79A71AD8B<redacted>1A1C97F197.
- 84490152E9<redacted>2847F71685.

In addition, queries conducted using StealthMole's platform identified six ransomware-related indicators, represented by the following SHA-256 hashes:

- 2aeeee44a8<redacted>cd8d381135.
- 657929381f<redacted>5c37630a6e.
- d3254ec47d<redacted>4ba3303247.
- d1f9ace720<redacted>5752307474.
- da8de7257c<redacted>761c266fdb.
- 349a4a5642<redacted>04a3a6a592.

Ransomware Monitoring Tracker

The StealthMole's ransomware monitoring tracker enabled the identification of 71 victims attributed to the Warlock group. Tables 1 through 4 organize the incidents identified during the investigation, cataloging them by victim organization, sector (in reference to the United States critical infrastructure sectors as defined by Presidential Policy Directive 21 [PPD-21], issued on February 12, 2013), country of the victim, and the Tor URL on which the attack and/or data leak was announced.

It is important to note that the victim list follows the sequence identified on StealthMole's platform, and that critical infrastructure sector classification was applied with flexibility, not always adhering strictly to the formal definitions of each sector—particularly in cases involving the information technology (IT) and critical manufacturing sectors in the subsequent tables. Additionally, when a victim organization could not be classified as part of a critical infrastructure sector, a forward slash ("/") was used in the sector field, and when sufficient information was unavailable to determine any specific attribute, a question mark ("?") was applied.

The distribution of victims by United States critical infrastructure sector classification is as follows:

1. Critical manufacturing (11).
2. Information technology (10).
3. Chemical (4).
4. Energy (3).
5. Communications (2).

Victim	Sector	Country	Tor URL
primrose.com	Energy	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
tagorg.com	/	JOR	zfytizegsz<redacted>ewviqqh7yd[.]onion
wfd2027uae.ae	/	UAE	zfytizegsz<redacted>ewviqqh7yd[.]onion
magcpa.com	/	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
rougine-mfg.com	Chemical	IRN	zfytizegsz<redacted>ewviqqh7yd[.]onion
webcids.com	?	?	zfytizegsz<redacted>ewviqqh7yd[.]onion
wytechnology.local	Information Technology	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
sipecom.com	Information Technology	ECU	zfytizegsz<redacted>ewviqqh7yd[.]onion
starsalliance.com	Energy	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
brightwork.com	Information Technology	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
syspro.com	Information Technology	GBR	zfytizegsz<redacted>ewviqqh7yd[.]onion
anthembio.com	Chemical	IND	zfytizegsz<redacted>ewviqqh7yd[.]onion
orange.fr	Communications	FRA	zfytizegsz<redacted>ewviqqh7yd[.]onion
atcmanufacturing.com	Critical Manufacturing	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
mysecop.com	?	?	zfytizegsz<redacted>ewviqqh7yd[.]onion
advion.com	Chemical	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
accsnet.com	Information Technology	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
nszi	?	?	zfytizegsz<redacted>ewviqqh7yd[.]onion
kipl	?	?	zfytizegsz<redacted>ewviqqh7yd[.]onion
infoniqa.com	Information Technology	AUT	zfytizegsz<redacted>ewviqqh7yd[.]onion

Table 1. Victims identified via StealthMole's ransomware monitoring tracker.

Victim	Sector	Country	Tor URL
airfastindonesia.com	Transportation	IDN	zfytizegsz<redacted>ewviqqh7yd[.]onion
gmpc.com	/	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
mffood.com	Food and Agriculture	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
okan.ru	Critical Manufacturing	RUS	zfytizegsz<redacted>ewviqqh7yd[.]onion
hitachi-hta.com	Critical Manufacturing	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
medkar.com	?	TUR	zfytizegsz<redacted>ewviqqh7yd[.]onion
elssurveying.com	/	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
webville.net	Information Technology	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
kmssa.net	/	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion
jubileelife.com	Financial Services	PAK	zfytizegsz<redacted>ewviqqh7yd[.]onion
ferus-smit.com	Critical Manufacturing	DEU	zfytizegsz<redacted>ewviqqh7yd[.]onion
chroma.com.tw	Critical Manufacturing	TWN	zfytizegsz<redacted>ewviqqh7yd[.]onion
siball.net	?	RUS	zfytizegsz<redacted>ewviqqh7yd[.]onion
silanosn.local	?	?	warlockhga<redacted>h64s4vsuyd[.]onion
alphasys.bo	Information Technology	BOL	warlockhga<redacted>h64s4vsuyd[.]onion
nartis.ru	Critical Manufacturing	RUS	warlockhga<redacted>h64s4vsuyd[.]onion
sf.walltopia.com	/	USA	warlockhga<redacted>h64s4vsuyd[.]onion
ippm.org	?	GBR	warlockhga<redacted>h64s4vsuyd[.]onion
bel.quadra.ru	Energy	RUS	warlockhga<redacted>h64s4vsuyd[.]onion
tein.co.jp	Critical Manufacturing	JPN	warlockhga<redacted>h64s4vsuyd[.]onion

Table 2. Victims identified via StealthMole's ransomware monitoring tracker.

Victim	Sector	Country	Tor URL
atg.cz	Critical Manufacturing	CZE	warlockhga<redacted>h64s4vsuyd[.]onion
mytune.me	/	MYS	warlockhga<redacted>h64s4vsuyd[.]onion
miltech.local	?	?	warlockhga<redacted>h64s4vsuyd[.]onion
fabrity.com	Information Technology	USA	warlockhga<redacted>h64s4vsuyd[.]onion
cybervector.co.uk	Information Technology	GBR	warlockhga<redacted>h64s4vsuyd[.]onion
metro.local	?	?	warlockhga<redacted>h64s4vsuyd[.]onion
mnpease.ca	/	CAN	warlockhga<redacted>h64s4vsuyd[.]onion
bengineered.com.au	Critical Manufacturing	AUS	warlockhga<redacted>h64s4vsuyd[.]onion
goldenline.com	/	POL	warlockhga<redacted>h64s4vsuyd[.]onion
energogroup.net	?	?	warlockhga<redacted>h64s4vsuyd[.]onion
arch-con.com	/	USA	warlockhga<redacted>h64s4vsuyd[.]onion
carducci	?	?	warlockhga<redacted>h64s4vsuyd[.]onion
taos	?	?	elqfbcx5no<redacted>2meim6cbqd[.]onion
icidesi	?	?	elqfbcx5no<redacted>2meim6cbqd[.]onion
sras.org	/	USA	elqfbcx5no<redacted>2meim6cbqd[.]onion
astronika.pl	Critical Manufacturing	POL	elqfbcx5no<redacted>2meim6cbqd[.]onion
dad	?	?	elqfbcx5no<redacted>2meim6cbqd[.]onion
ssi-mi.com	/	USA	elqfbcx5no<redacted>2meim6cbqd[.]onion
lactanet.ca	Food and Agriculture	CAN	elqfbcx5no<redacted>2meim6cbqd[.]onion
bthk.org	Government Facilities	TUR	elqfbcx5no<redacted>2meim6cbqd[.]onion

Table 3. Victims identified via StealthMole's ransomware monitoring tracker.

Victim	Sector	Country	Tor URL
NCVOO	?	?	elqfbcx5no<redacted>2meim6cbqd[.]onion
ersar.pt	Government Facilities	PRT	elqfbcx5no<redacted>2meim6cbqd[.]onion
unilever.com	Commercial Facilities	GBR	elqfbcx5no<redacted>2meim6cbqd[.]onion
nipponindiaim.com	Financial Services	IND	elqfbcx5no<redacted>2meim6cbqd[.]onion
komatsu.pe	/	PER	elqfbcx5no<redacted>2meim6cbqd[.]onion
eiragroup.co	/	COL	elqfbcx5no<redacted>2meim6cbqd[.]onion
iberol.pt	Chemical	PRT	elqfbcx5no<redacted>2meim6cbqd[.]onion
via-optronics.com	Critical Manufacturing	DEU	elqfbcx5no<redacted>2meim6cbqd[.]onion
currimjee.com	/	MUS	elqfbcx5no<redacted>2meim6cbqd[.]onion
colt.net	Communications	GBR	zfytizegsz<redacted>ewviqqh7yd[.]onion
clearybuilding.us	/	USA	zfytizegsz<redacted>ewviqqh7yd[.]onion

Table 4. Victims identified via StealthMole's ransomware monitoring tracker.

6. Food and agriculture (2).
7. Financial services (2).
8. Government facilities (2).
9. Commercial facilities (1).
10. Transportation (1).
11. Non–critical infrastructure, "/" (17).
12. Unclassified occurrences, "?" (16).

Among the incidents classified as critical infrastructure, the critical manufacturing sector accounts for the largest number of attacks attributed to the Warlock group. This distribution is particularly concerning, as discrete manufacturing industries continue to be among the primary targets of cyberattacks affecting operational technology (OT) environments with potential physical consequences[7], including production delays and outages, equipment damage, environmental incidents, and personnel injuries or casualties. Although the Warlock group has not demonstrated explicit capabilities—or apparent intent—to directly disrupt OT–ICS environments, the indirect impacts of ransomware incidents on industrial networks can nevertheless be significant. Industrial operations may depend, in whole or in part, on corporate

[7] Machtemes, R., Hale, G., Walhof, M., & Ginter, A. (2025). *2025 OT Cyber Threat Report. Waterfall Security*. Link

IT services or shared network resources, and ransomware activity affecting the enterprise environment can therefore trigger cascading effects, including operational disruptions or precautionary shutdowns of OT and industrial control systems (ICS) implemented to reduce risk and ensure operational safety.

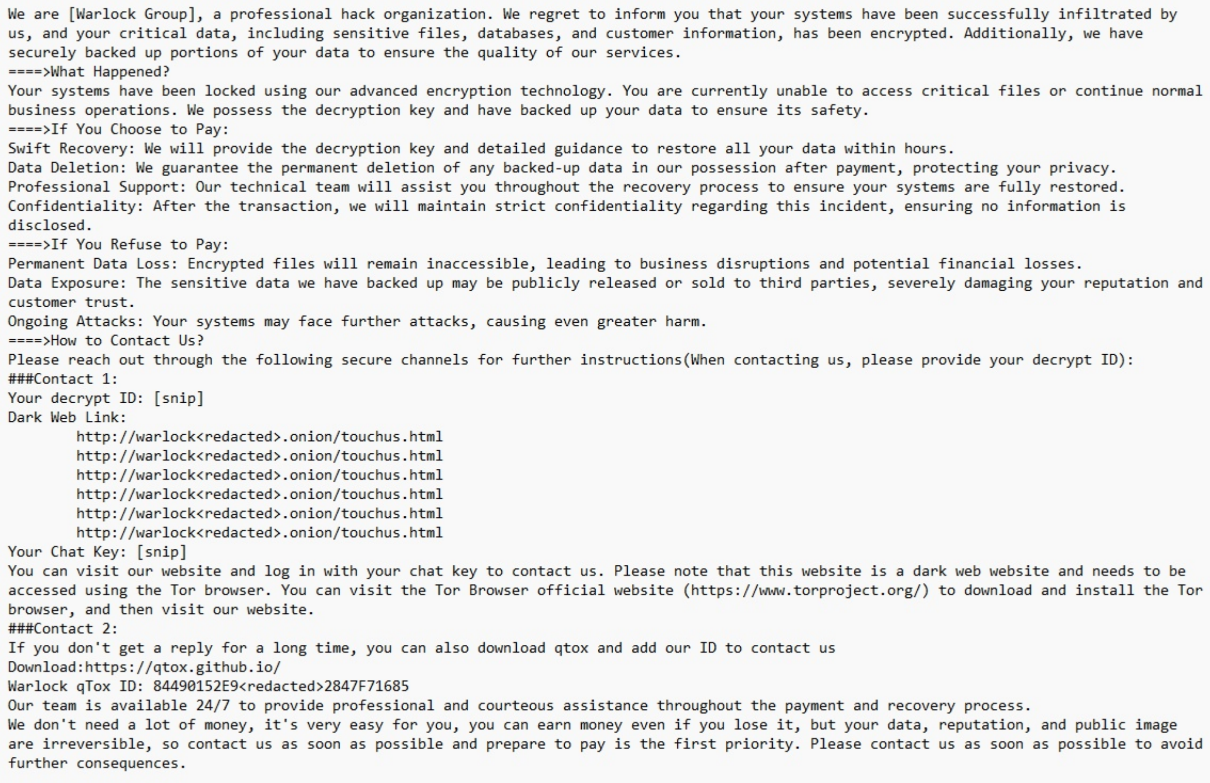
Regarding the geographic distribution of attacks, the three countries most affected by cyber incidents attributed to the Warlock group were the United States (20 incidents), the United Kingdom (5 incidents), and Russia (4 incidents). All remaining countries recorded one or two incidents each, as documented in Tables 1 through 4.

Finally, an additional seven alleged victims were identified across the domains zfytizegsz<redacted>ewviqqh7yd[.]onion and warlockhga<redacted>h64s4vsuyd[.]onion. These entities were listed on the WarLock Client Data Leak Show as getdomain, STRGOME, woodboure, gmtaconline, lactanet, houxt, and houra; however, no sample data or complete datasets were publicly disclosed for these entries.

Additional Information on the Threat Group

After a successful encryption process during an attack, ransom notes are typically left on the victim's system, often titled: How to decrypt my data.txt, How_to_decrypt_my_data.txt, and How to decrypt my data.log. Figure 4 illustrates the content of one such TXT file, with portions omitted. The ransom notes contain Tor URLs and Tox IDs for victims to use in order to continue the negotiation process. The Tor URLs provided are of the form warlockhga<redacted>h64s4vsuyd[.]onion/touchus.html, for example, which direct victims to a Client Chat platform. Access to this chat requires logging in with an access key, which is made available in the ransom notes.

Recent technical reports, including analyses published by the Halcyon Ransomware Research



```
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: [snip]
Dark Web Link:
        http://warlock<redacted>.onion/touchus.html
        http://warlock<redacted>.onion/touchus.html
        http://warlock<redacted>.onion/touchus.html
        http://warlock<redacted>.onion/touchus.html
        http://warlock<redacted>.onion/touchus.html
        http://warlock<redacted>.onion/touchus.html
Your Chat Key: [snip]
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: 84490152E9<redacted>2847F71685
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 possible to avoid
further consequences.
```

Figure 4. Excerpt from a Warlock ransomware note.

Center, indicate potential ties to Chinese nation-state–aligned actors. In a threat intelligence report, Quorum Cyber assesses a linkage between Warlock group and Storm-2603, a China-based threat cluster that has previously deployed Warlock ransomware—an assessment also supported by a Microsoft Threat Intelligence blog post published on July 22, 2025. Notably, the group's demonstrated access to zero-day vulnerability exploits substantially elevates the cyber risk posed by Warlock and distinguishes it from lower-tier criminal operations, positioning the group at a more advanced level within the contemporary threat landscape.

Conclusions

The fourth issue of the 2025 volume of Ind.Cyber.Sec Letters conducted a profiling of the Warlock ransomware group, based on findings derived from StealthMole's platform in combination with OSINT techniques. Figure 5 illustrates the node-graph representation of the investigation conducted using StealthMole's platform. As highlighted by Dragos in its analyses covering the second and third quarters of 2025, the Warlock group has exhibited growing threat activity against organizations broadly, with emphasis on critical infrastructure sectors, including manufacturing, IT, chemical, and energy.

Nevertheless, the investigation did not reveal clear evidence of direct compromise of OT-ICS environments, despite indications that some victim organizations experienced multi-day service outages. The findings likewise do not demonstrate advanced or purpose-built capabilities explicitly targeting OT-ICS devices. However, given the group's financially motivated objectives, the risk of indirect impacts on OT-ICS infrastructures cannot be discounted, particularly through infection of IT systems or the compromise of industrial databases or historians, as well as engineering workstations, which may in turn affect the continuity and reliability of operations.

Acknowledgments

The author thanks the entire StealthMole team for their support and for granting access to the platform's trackers.

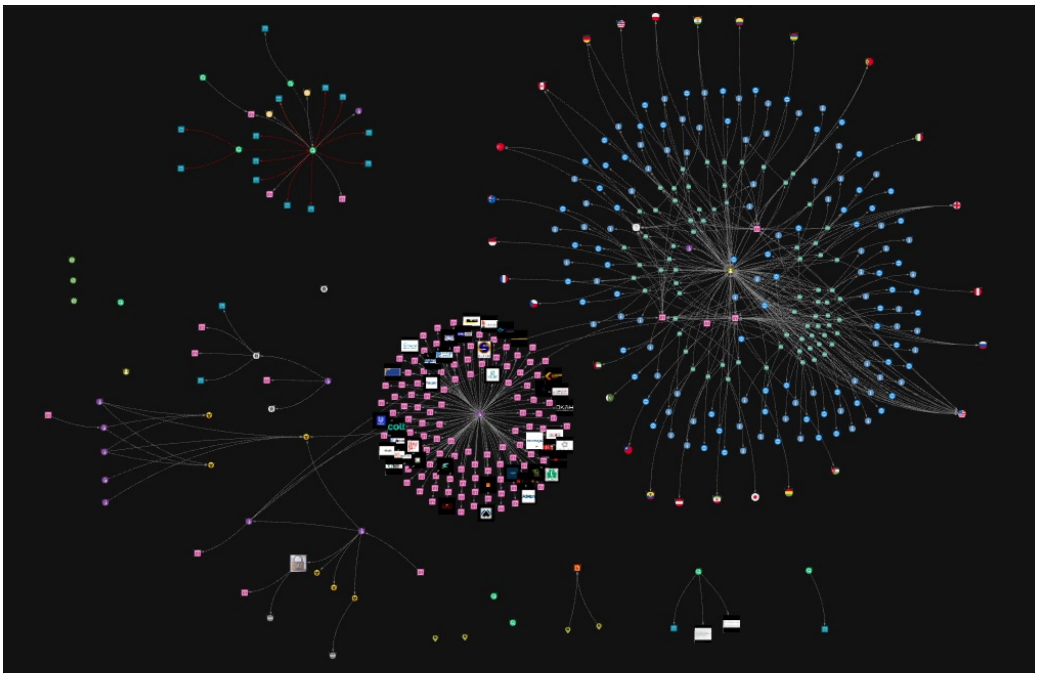


Figure 5. Warlock ransomware group investigation conducted using StealthMole's platform.

Ind.Cyber.Sec Letters

Volume 02, Issue 04. 2025, December 16
Profiling Warlock Ransomware Group

Luiz F. Freitas-Gutierres (a.k.a. substationworm) is a professor in the Department of Electromechanics and Power Systems at the Federal University of Santa Maria. His primary research interests include: industrial cybersecurity, cyber threat intelligence, and the automation of electric power systems.

Ind.Cyber.Sec Letters is a collection of studies and analyses of incidents in the field of industrial cybersecurity.

Prof. Dr. Luiz Fernando Freitas-Gutierres

in linkedin.com/in/lffreitas-gutierres

github.com/substationworm

✉ luiz.gutierres@ufsm.br