Tracking Adversaries: The Qilin RaaS

By BushidoToken

Published: 2024-06-12 · Archived: 2026-04-05 17:18:20 UTC

This blog is part of my Tracking Adversaries blog series, whereby I perform a summary analysis of a particular adversary that has caught my attention and made me feel like they deserve special attention and investigation.

Qilin has been covered already by experts from Trend Micro, Secureworks, Group-IB, SentinelOne, SOCRadar, BleepingComputer, and MalwareHunterTeam. Kudos to them, because without these researchers sharing their findings with the community, we would be a lot less informed about this prominent ransomware gang.

Background

Active since at least May 2022, Qilin ransomware is named after the mythical Chinese creature which you may pronounce as "Chee-lin". The origin of this cybercriminal threat group, however, is believed to be from Russia.

Like many other ransomware campaigns run by organised cybercriminal gangs, Qilin ransomware is used for domain-wide encryption of servers and workstations and its operators steal vast quantities of data. A ransom is then demanded for the decryption keys and/or to prevent the publication of the stolen data. This is also known as double extortion.

Qilin is a Ransomware-as-a-Service (RaaS), which means that cybercriminals external to the core Qilin team (also known as ransomware affiliates) are invited to perform ransomware attacks using the Qilin RaaS platform. The Qilin RaaS will handle payload generation, the publication of stolen data, and ransom negotiations.

Adversary

The Qilin RaaS operators are also tracked as Water Galura (Trend Micro) and GOLD FEATHER (Secureworks). Qilin is advertised on the exclusive Russian-speaking forum RAMP (short for Ransom Anon Market Place [sic]), where acquiring an account can cost up to $500 in BTC. The forum profile “Haise” joined RAMP on 29 May 2022 and advertised Qilin on 13 February 2023 (see Figure 1).

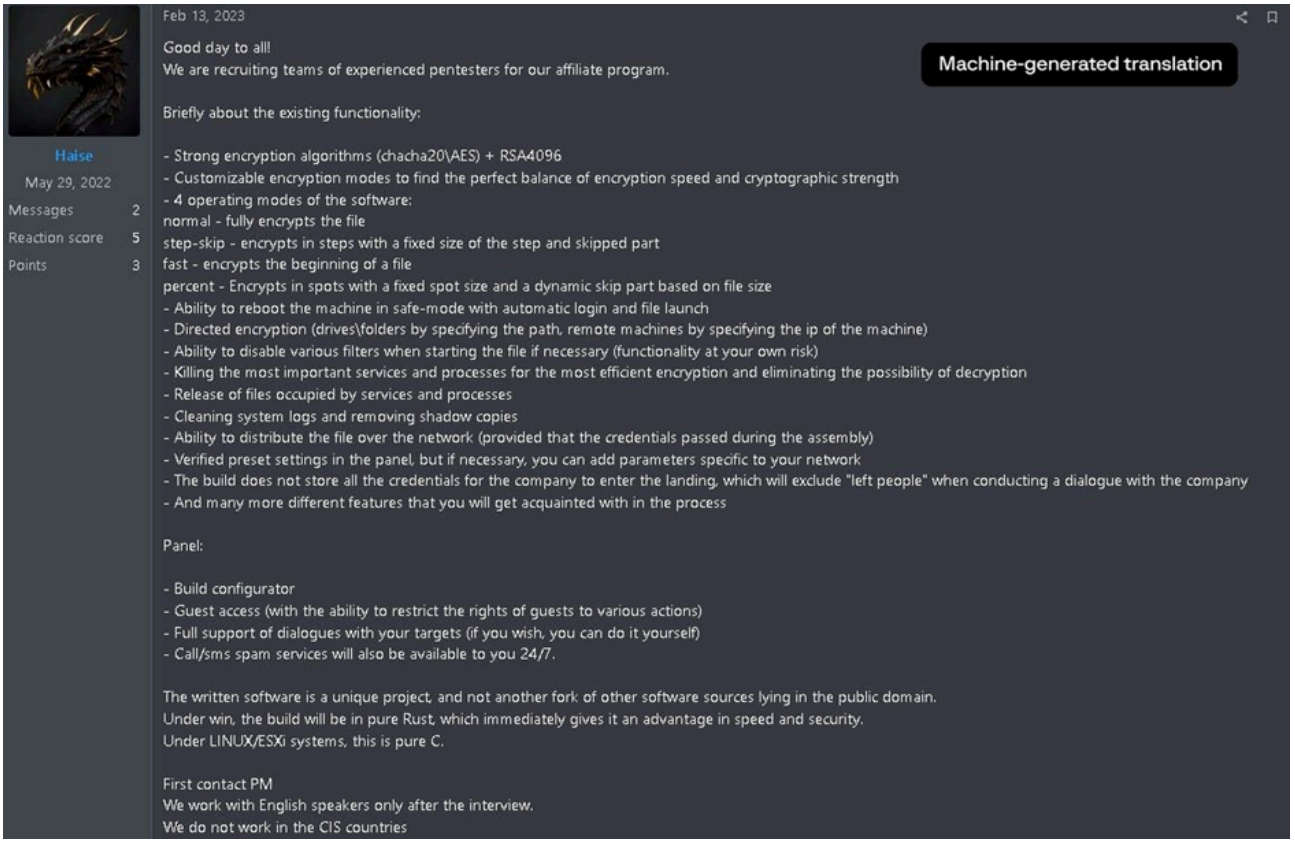

Figure 1: Qilin RaaS operator Haise advert on RAMP. (Source: Group-IB)

Further, according to Group-IB, Qilin affiliates that use the RaaS can receive up to 80% if the ransom is paid by the victim (if the ransom paid is 3 million USD or less). And for ransoms over 3 million USD an affiliate's cut can rise to 85%.

In July 2023, KELA spotted that Qilin announced significant changes to their affiliate payment system. The Qilin RaaS operator Haise stated on RAMP that ransom payments are paid to their affiliates’ wallets first and only then a share of profits is transferred to the Qilin RaaS owners.

Victims

In October 2022, the first victim of Qilin was posted to their Tor data leak site. However, there are reports of Qilin (formerly known as Agenda) being deployed as early as June 2022. From Q2 2023, the number of Qilin victims began to steadily be listed at a rate of around five victims per month. Since the start of 2024, the number of Qilin victims has noticeably increased (see Figure 2). Do note, however, these are the Qilin victims that are not paying the ransoms who are being leaked. Trying to research the actual true amount of ransomware attacks is a difficult challenge.

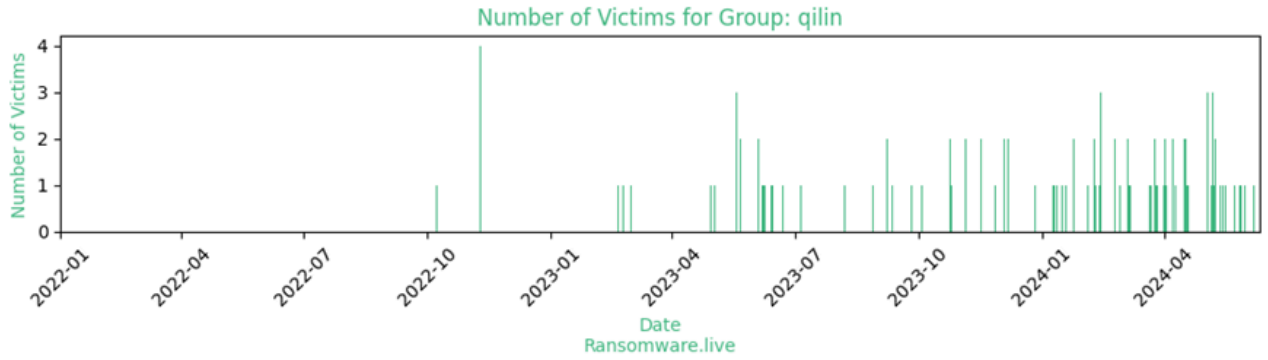

Figure 2: Frequency of Qilin victim posts. (Source: Ransomware.live)

Victims of Qilin have been globally dispersed. The affiliates of Qilin appear to indiscriminately target large companies from around the world, which includes organisations from Argentina, Australia, Brazil, Canada, Colombia, France, Germany, Japan, New Zealand, Serbia, Thailand, The Netherlands, the UAE, the UK and the US. Some of Qilin's most notable victims include the automotive giant Yanfeng, UK newspaper The Big Issue, and most importantly Synnovis, a healthcare provider for multiple hospitals in London and a major part of the UK National Health Service (NHS).

Further, as is typical of the Russian-speaking cybercriminal underground, the operators of Qilin stated "We do not work in the CIS countries" in their RAMP forum post. This means they do not allow their affiliates to deploy Qilin ransomware or extort victims from the Commonwealth of Independent States (CIS), which are all the countries that used to make up the Soviet Union (USSR).

In mid-2023, KELA observed Qilin affiliates demanding ransoms in the range of 25,000 to 600,000 USD and identified a real estate development company in Thailand paying 600,000 USD after 20 days of negotiations.

Capabilities

At the time of writing, only a handful of public resources are available on the tactics, techniques, and procedures (TTPs) of Qilin affiliates with Trend Micro being the primary contributor (big thanks to them for sharing with the community).

Not too much has been shared publicly about the initial access methods leveraged by Qilin affiliates. Trend Micro, however, has reportedly observed one Qilin affiliate use stolen credentials to access a public-facing Citrix servers for the point of entry, but how the credentials were stolen in the first place is unknown – potentially via an earlier intrusion by an initial access broker (IAB) or from infostealer malware logs. KELA also tweeted that they saw a Qilin affiliate claiming they gained access via a phishing email during a ransom negotiation with a victim.

Qilin affiliate post-compromise TTPs also appear to vary somewhat and only limited information is available in open sources. Trend Micro observed one affiliate using Nmap and Nping for internal enumeration and RDP with valid credentials for lateral movement. Another affiliate was found to be using a combination of Cobalt Strike and remote monitoring and management (RMM) tools, though Trend Micro did not say which one(s). To disable endpoint protection and response (EDR) systems, Qilin affiliates are known to use the bring-your-own-vulnerable-driver (BYOVD) trick using Terminator.exe by SpyBoy or the publicly available rootkit tool called YDArk. Secureworks stated they saw a Qilin affiliate using PCHunter and PowerTool. Data exfiltration TTPs by Qilin affiliates have not been shared publicly either.

For ransomware distribution, the final stage of the intrusion, Qilin operators have reportedly used an Active Directory Group Policy Object (GPO) to create a scheduled task called enc64.exe. The first version of Qilin (formerly called Agenda) would also change the default user's password and enable automatic login with the new credentials. Plus it would reboot the victim's machine in safe mode and then proceed with the encryption routine upon reboot to bypass protection systems. The Rust version of Qilin ransomware has also been deployed using a custom PowerShell script embedded in the binary to propagate across VMware vCenter and ESXi servers as well as via PsExec, the Windows Sysinternals tool. Another notable TTP about Qilin ransomware that SentinelOne highlighted is that it uses intermittent encryption, reportedly to bypass protections.

As for the ransom notes, in August 2022, Trend Micro uncovered the first version of the ransomware, which was called Agenda and was later renamed to Qilin (see Figure 3 and 4).

Figure 3: Agenda ransom note example. (Source: Trend Micro)

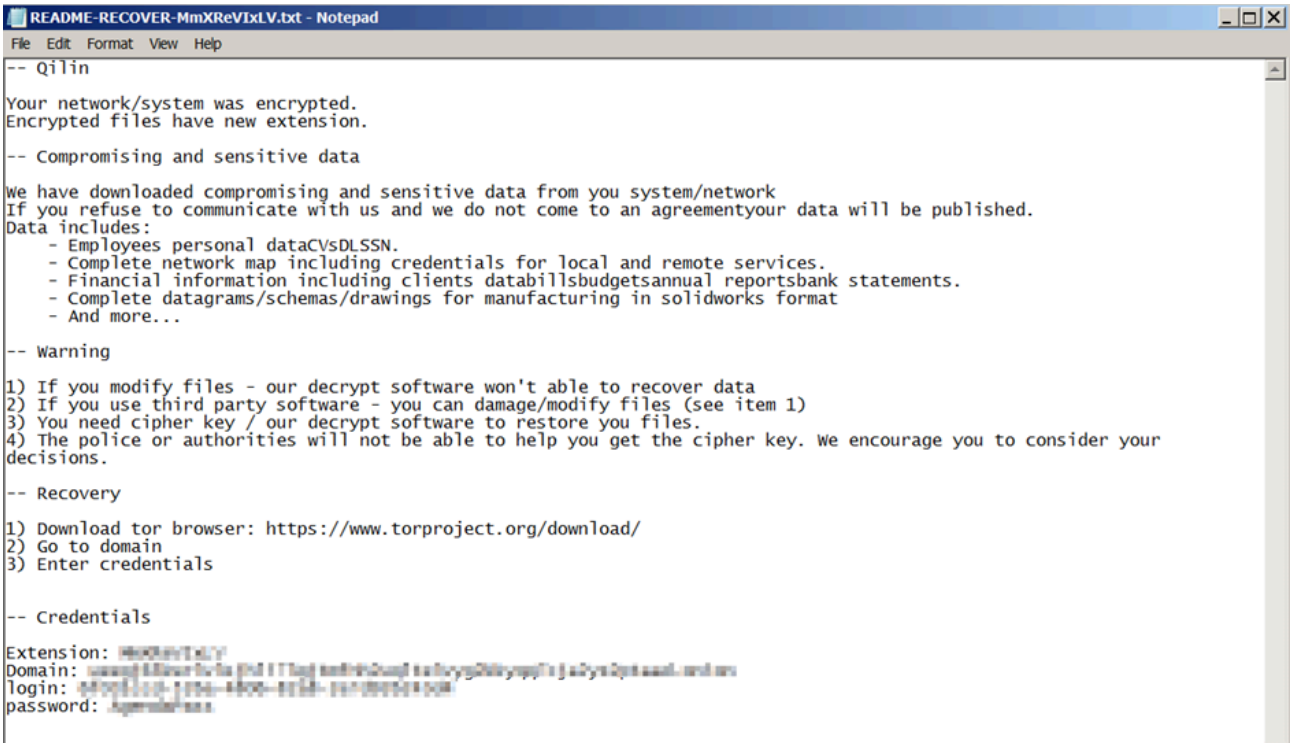

Figure 4: Qilin ransom note example. (Source: Trend Micro)

There are multiple versions of Qilin ransomware. This includes a Golang variant and Rust variant to target Windows. Plus, since December 2023, a custom-coded version of Qilin to target Linux virtual machines on VMware ESXi hypervisors. This is notable as many other ransomware gangs that target ESXi often just use the leaked Babuk source code.

Infrastructure

The Qilin ransom notes shown above are dropped on the encrypted devices at victim organisations. If a victim follows the instructions in the ransom notes they are greeted with a “recovery portal” hosted on Tor as part of the Qilin RaaS for ransom negotiations and decryption (see Figure 5).

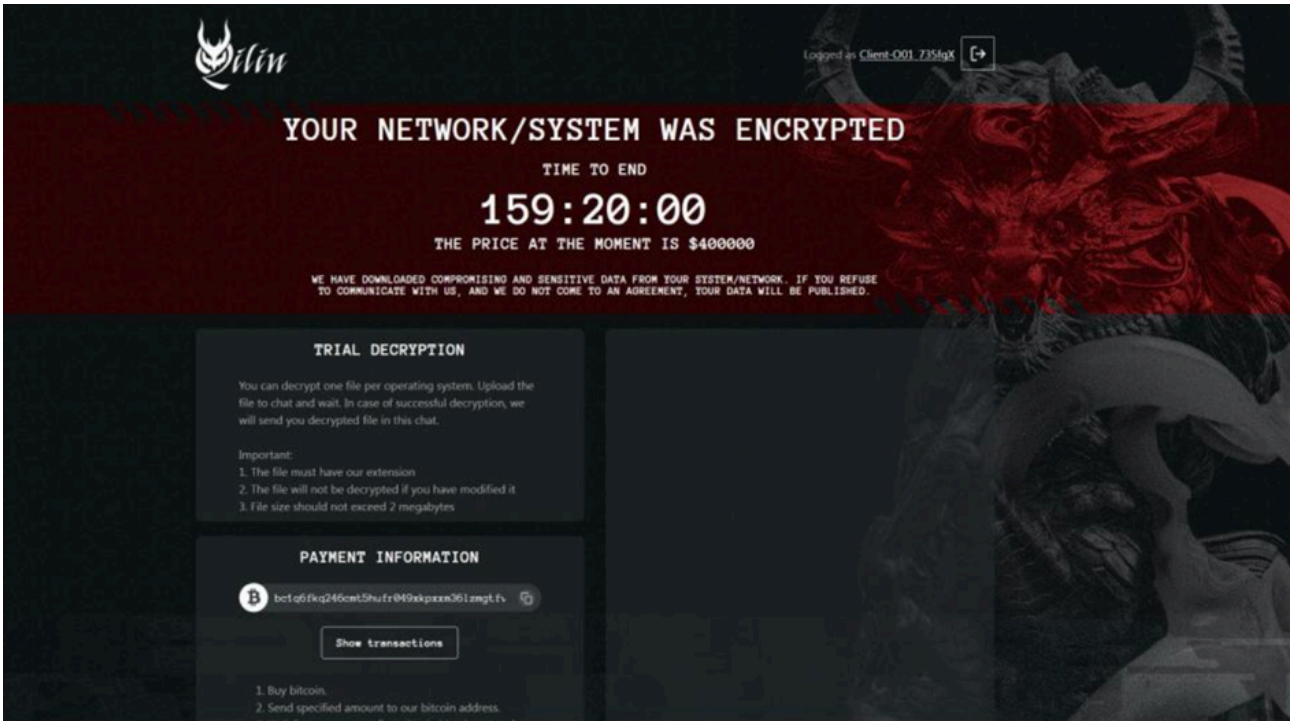

Figure 5: Qilin victim recovery portal. (Source : BleepingComputer Forums)

If a victim does not pay the ransom to Qilin, then their data is posted to the Qilin Tor Data Leak Site, which has also gone through an upgrade and the operators have since added some more Qilin branding graphics (see Figure 6).

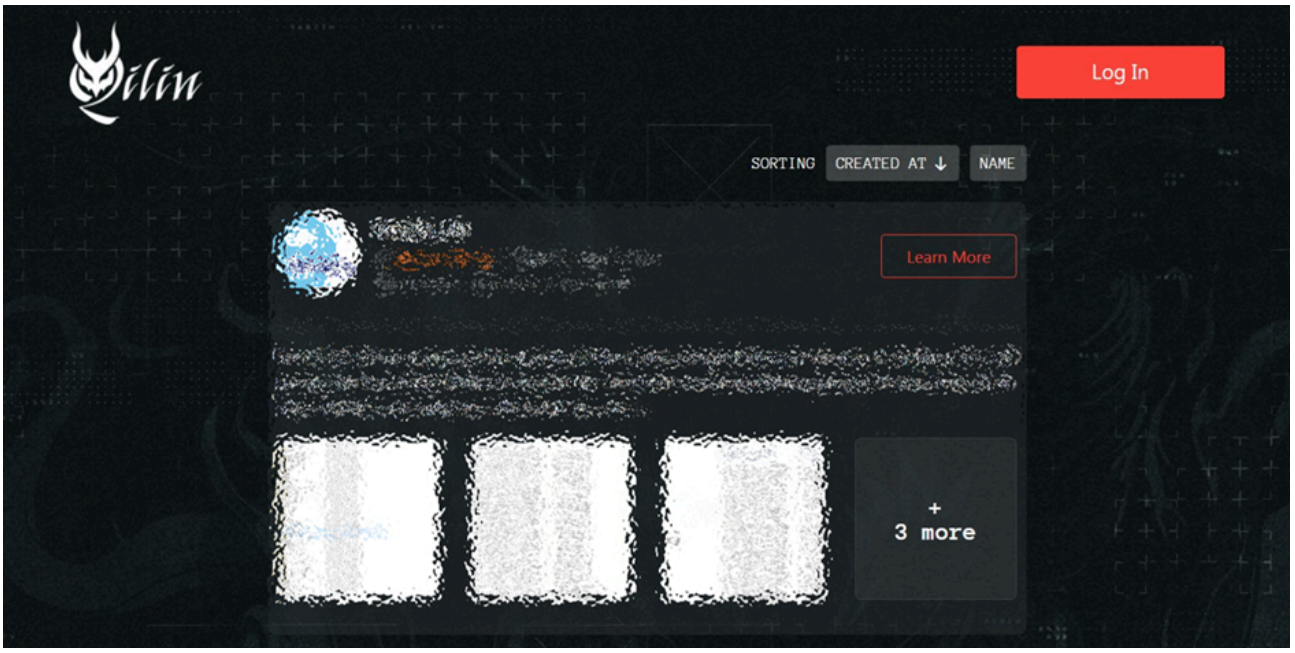

Figure 6: Qilin data leak site.

In May 2023, Group-IB disclosed that they managed to infiltrate the Qilin group in March 2023 and managed to gain visibility to the Qilin RaaS (see Figure 7, 8, and 9), highlighting the power of human intelligence (HUMINT) and undercover operations. The RaaS platform operates similarly to others we have seen in the past. Affiliates get

access to a panel to build customisable payloads for Windows and ESXi, publish stolen victim files to the data leak site, negotiate with victims for the ransom payments, and read some guidance shared by the RaaS operators on how to use Qilin ransomware.

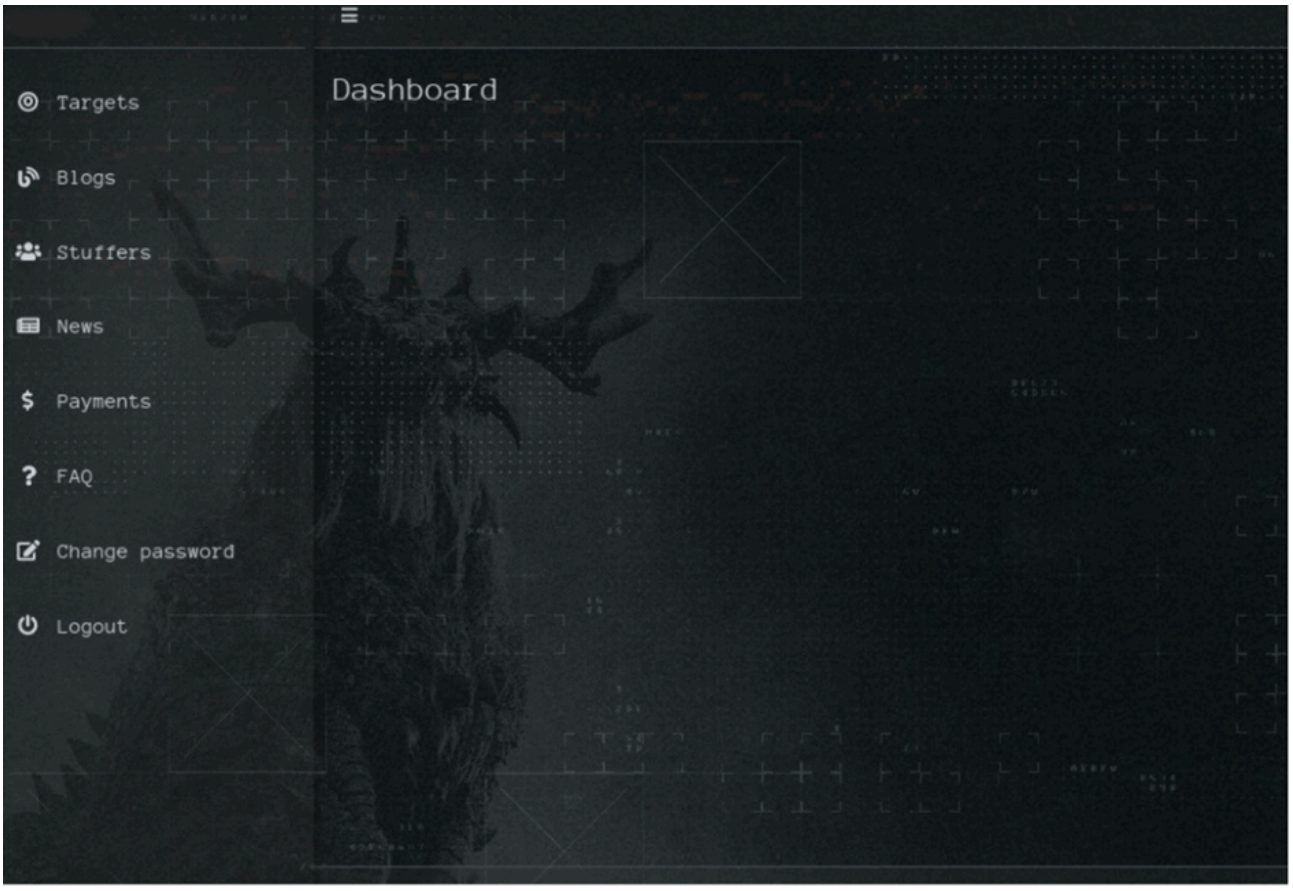

Figure 7: Qilin RaaS dashboard. (Source: Group-IB)

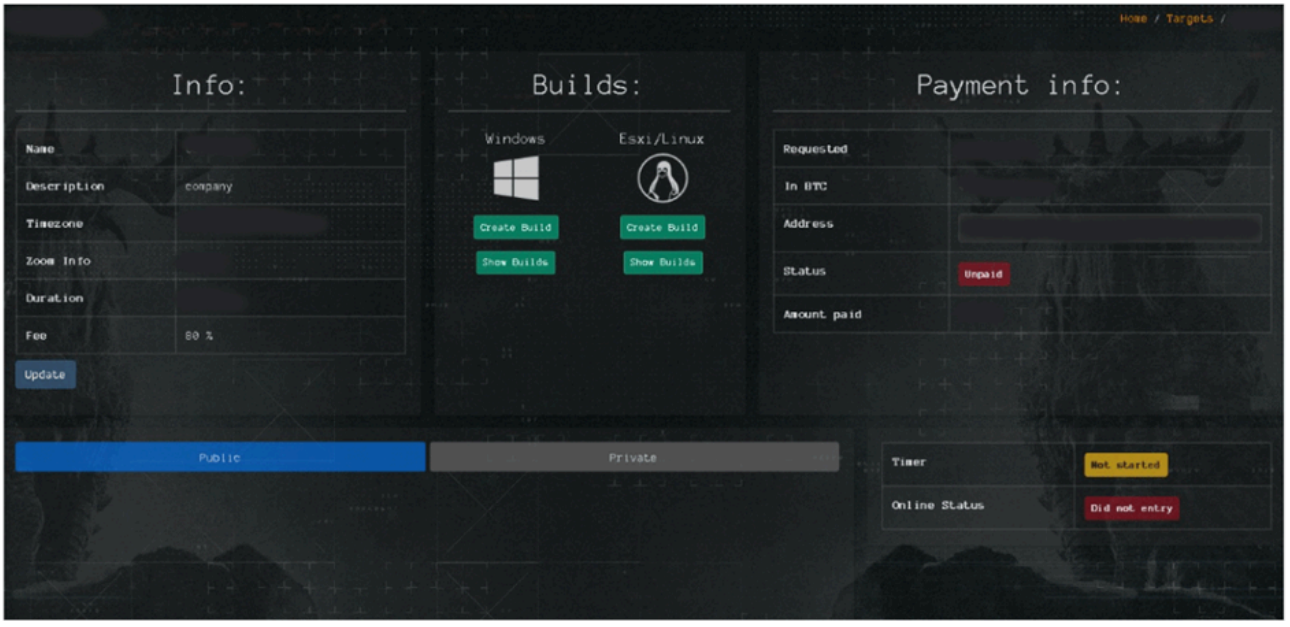

Figure 8: Qilin RaaS customisable options. (Source: Group-IB)

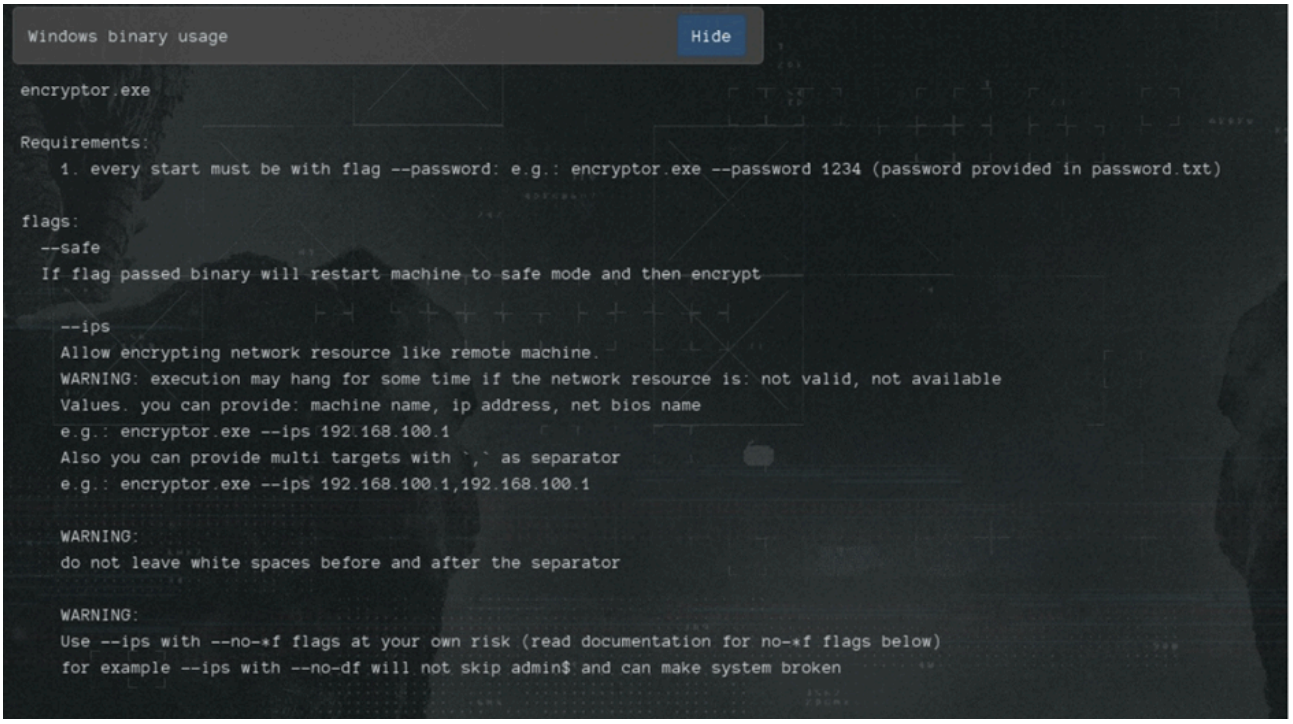

Figure 9: Qilin ransomware usage guide. (Source: Group-IB)

Alongside their Tor data leak site, Qilin also runs another Telegram news channel to make announcements (see Figure 10).

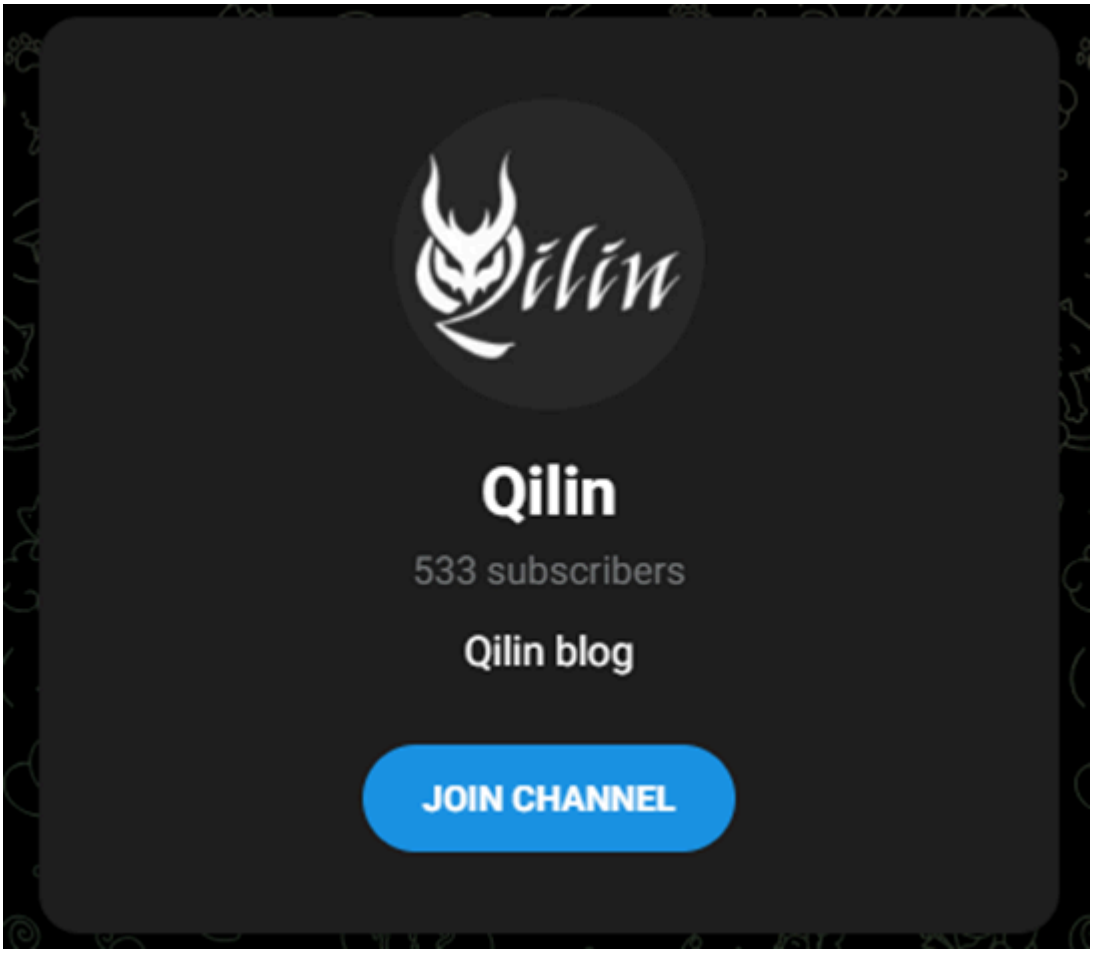

Figure 10: Telegram channel of Qilin ransomware.

On 1 May 2024, Qilin pulled an unusual move and added a new QR code to its Tor data leak site which pointed to a site called WikiLeaksV2, which is hosted on the Clearnet site (see on URLscan here) where they listed a selection of their victims in addition to soliciting cryptocurrency donations (see Figure 11).

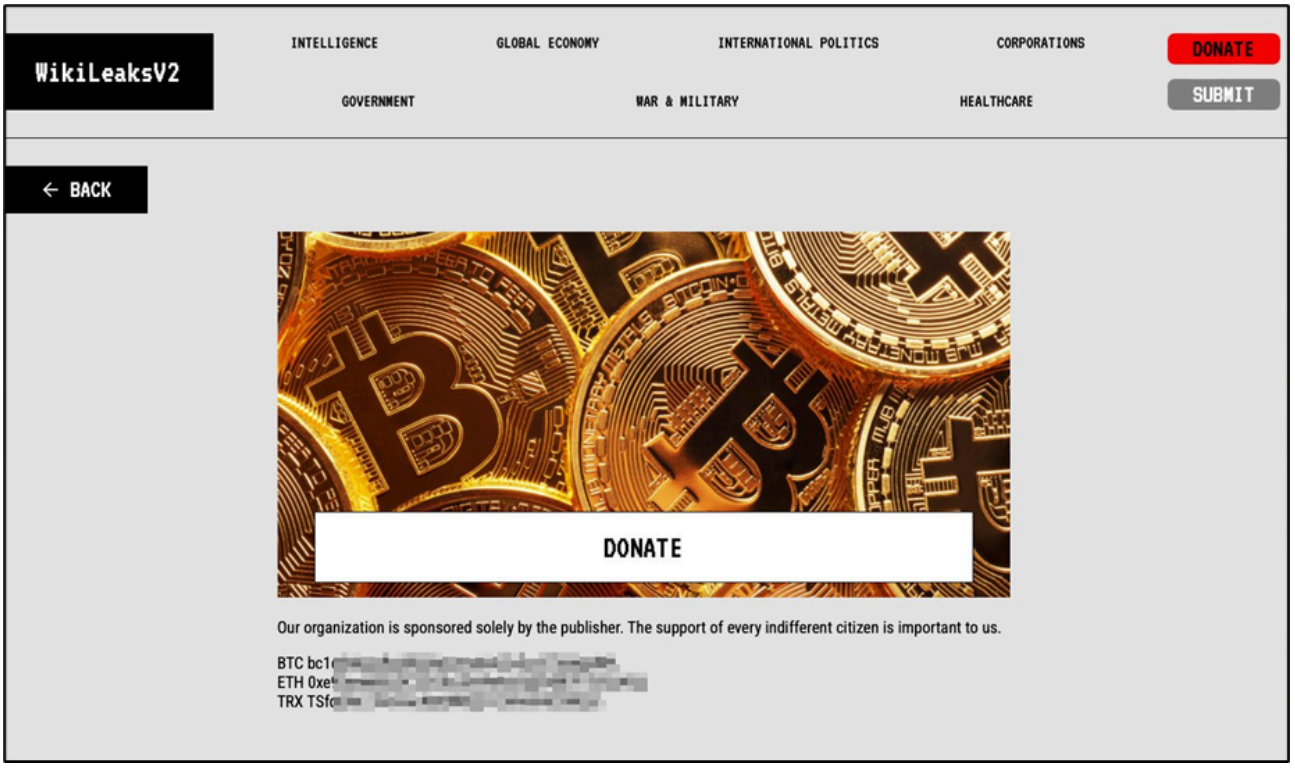

Figure 11: WikiLeaksV2 created by Qilin. (Source: @BrettCallow)

Overlaps between Qilin and other ransomware groups

At the time of writing, Qilin has listed over 100 organisations as victims on their Tor data leak site. Among those victims, there have been overlaps with over ransomware 'name-and-shame' sites. On the 30 April 2023, Qilin published the Siix Corporation to its Tor data leak site. On the 17 October 2023, ALPHV/BlackCat also published Siix Corporation to its Tor data leak site. On 26 October 2023, SG World appeared on the Qilin Tor data leak site. It was previously listed on the Conti Tor data leak site on 17 April 2021.

Interestingly, following the overlaps in victims between Qilin, ALPHV/BlackCat, and Conti, Microsoft shared that Pistachio Tempest (formerly DEV-0237 and also known as FIN12) was experimenting with Qilin ransomware back in June 2022, back when it was called Agenda ransomware still (see Figure 12). Pistachio Tempest is known for deploying Ryuk, Conti, Hive, and became a prolific ALPHV/BlackCat affiliate. The link to FIN12 also closely aligns with the usage of Qilin against healthcare targets (particularly the UK NHS), which is a well-documented TTP of the group.

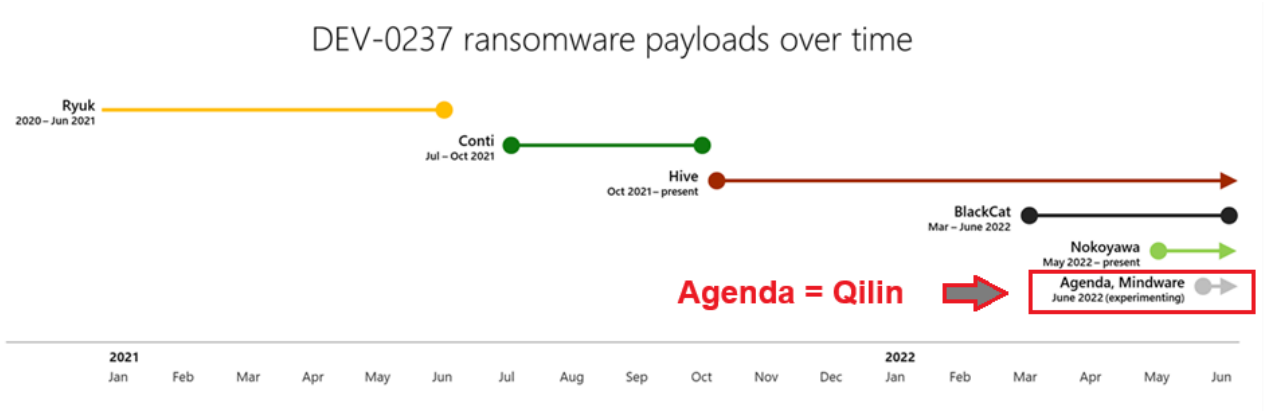

Figure 12: DEV-0237 usage of Qilin. (Source: Microsoft)

Additional similarities between Qilin and other well-known ransomware families include features such as the user verification system on the Qilin victim recovery portal is very similar to that of BlackMatter (the predecessor of ALPHV/BlackCat). Other features of the Golang variant of Qilin such as the function of changing system passwords and rebooting into safe mode is reminiscent of REvil and BlackBasta. REvil has several ties to ALPHV/BlackCat and BlackBasta is a known descendent of the Conti gang.

Further, the Rust variant of Qilin prompts the user for a password to be passed as an argument which is a feature reminiscent of ALPHV/BlackCat, which was also written in Rust. Another finding was that SCATTERED SPIDER, an affiliate of the ALPHV/BlackCat RaaS is also regularly known to use the BYOVD technique to bypass EDR systems. Plus, Terminator.exe has also been deployed during ALPHV/BlackCat ransomware attacks in June 2023 as well as leveraged by Akira ransomware affiliates, who also have ties to Conti.

Conclusion

So far, Qilin appears to be nothing special but is evidently attracting the affiliates leftover from the Conti shutdown, the ALPHV/BlackCat exit scam, and is likely to also be a benefactor of the LockBit takedown. The numerous overlaps between affiliates, victims, features and design choices indicate just how closely the ransomware ecosystem is all interconnected. Due to Qilin being relatively new but virtually mirroring the functionality of ALPHV/BlackCat does make it highly likely that some of the same Russian-speaking cybercriminals associated with ALPHV/BlackCat are associated with Qilin.

Therefore, it seems Qilin may be the next big RaaS to fill the vacuum left by the other big RaaS shutting down or getting taken down. However, there is a big question mark around whether they can withstand the pressure from international law enforcement joint operations. Qilin shall almost certainly be receiving a lot of extra attention since the UK National Health Service was attacked. Therefore it is likely safe to assume that the operators behind Operation Cronos at the UK National Crime Agency (NCA) shall be looking closely into Qilin.

Additional Resources

https://id-ransomware.blogspot.com/2022/06/agenda-ransomware.html

https://github.com/rivitna/Malware/blob/main/Qilin/Qilin_samples.txt

Qilin Data Leak Site: ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd[.]onion

Qilin Victim Portal: kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad[.]onion

Qilin Clearnet Site: wikileaksv2[.]com (31.41.244[.]100)
