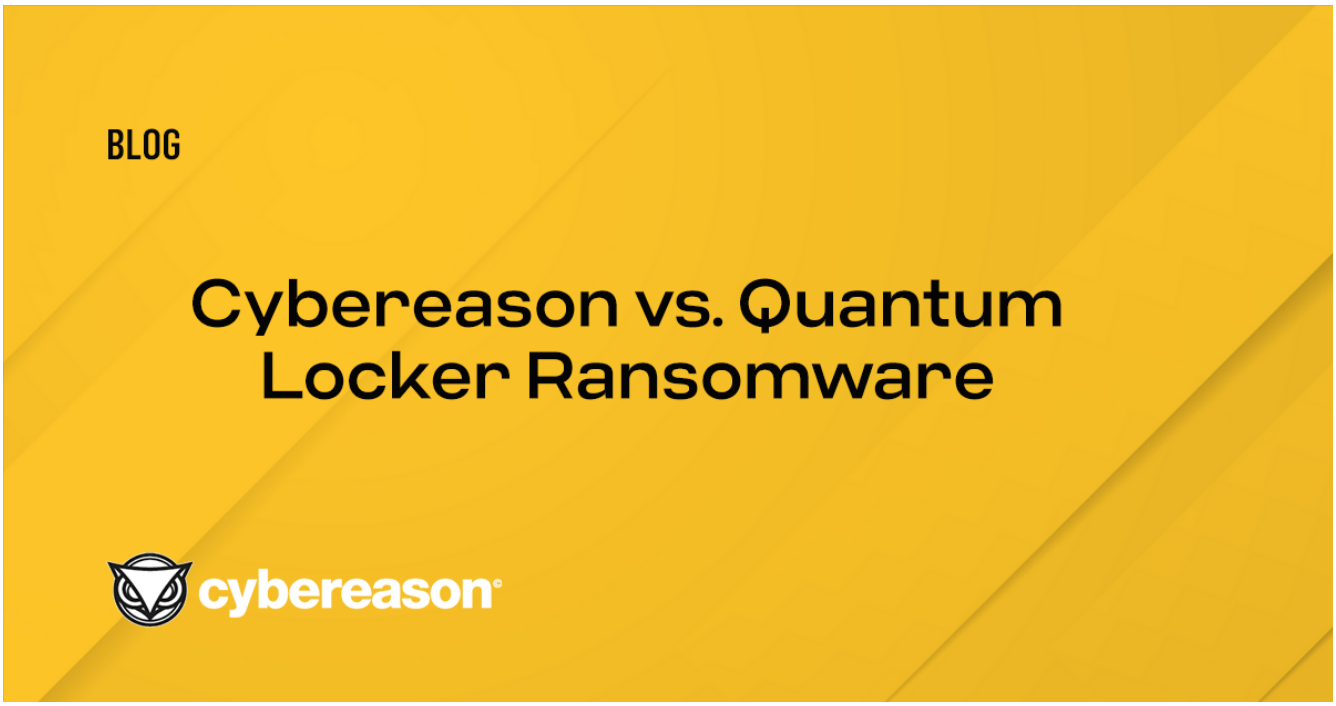
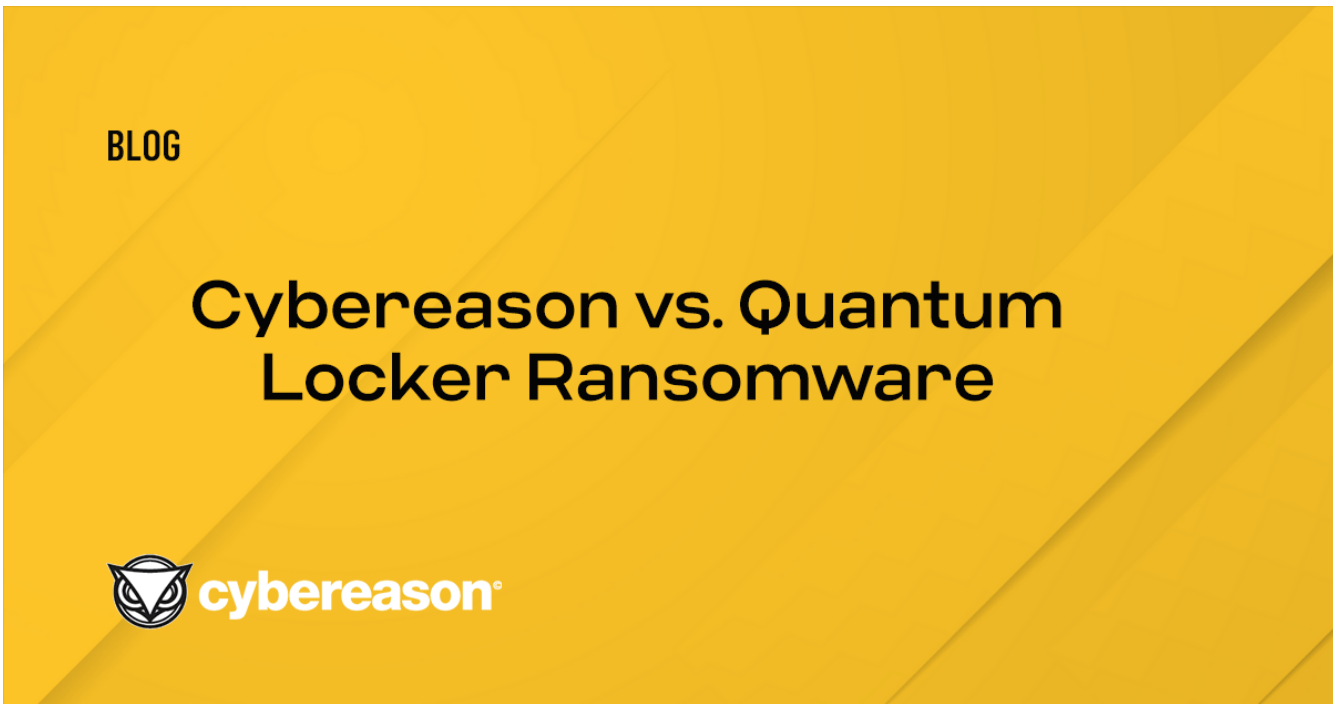
Cybereason vs. Quantum Locker Ransomware

cybereason.com/blog/cybereason-vs.-quantum-locker-ransomware





Written By
Cybereason Nocturnus

May 9, 2022 | 5 minute read

The Quantum Locker is a ransomware strain that was first discovered in July 2021. Since then, the ransomware was observed used in fast ransomware attacks, in some cases even Time-to-Ransom (TTR) of less than 4 hours, leaving defenders little time to react.

Key Details

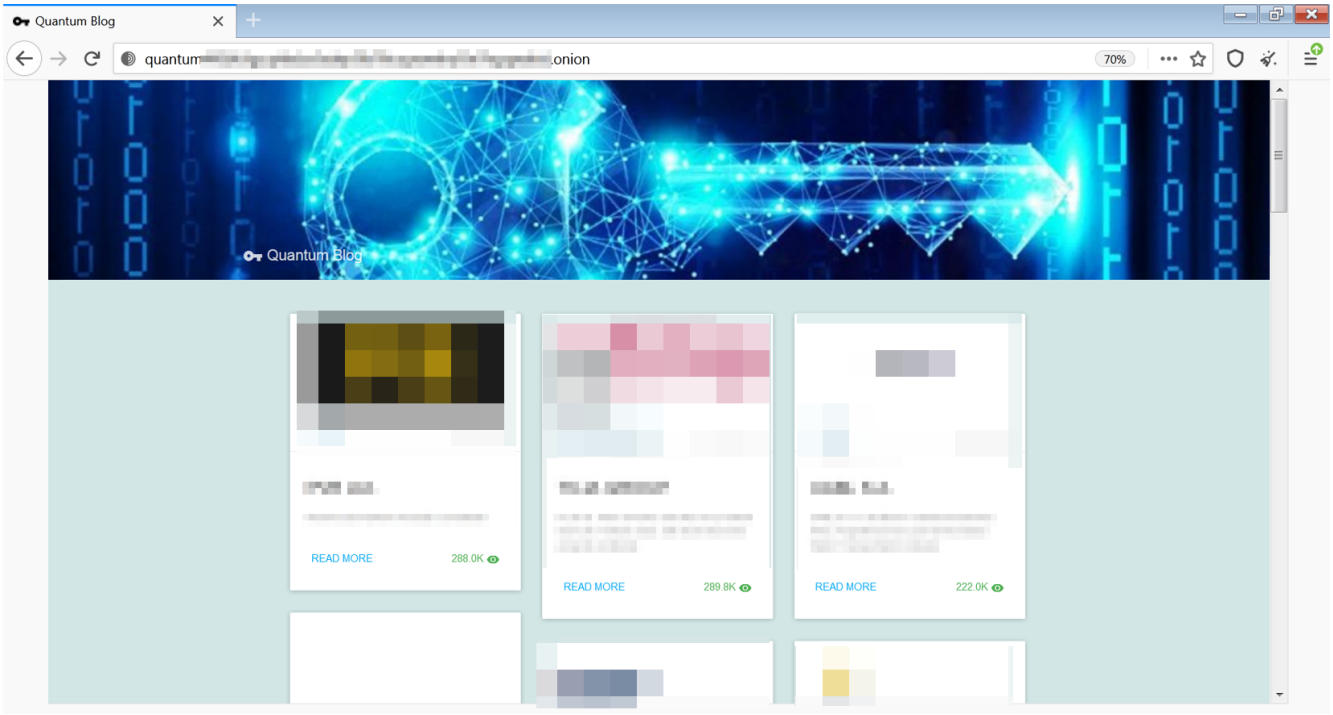
- **Time-to-Ransom (TTR) of less than 4 hours**: From initial infection to encryption takes even less than 4 hours, leaving a very short window for defenders to successfully defend against the threat.
- **High Severity**: The Cybereason Nocturnus Team assesses the threat level as HIGH given the destructive potential of the attacks.
- **Human Operated Attack:** Prior to the deployment of the ransomware, the attackers attempt to infiltrate and move laterally throughout the organization, carrying out a fully-developed *RansomOps* attack.
- **Detected and Prevented**: The AI-Driven Cybereason XDR Platform fully detects and prevents the Quantum Locker.

Cybereason Blocks Quantum Locker

The Quantum ransomware is another rebranding of the notorious MountLocker ransomware, which launched back in September 2020. Since then, the ransomware gang has rebranded its operation to various names, including AstroLocker, XingLocker, and now in its current phase, the Quantum Locker:

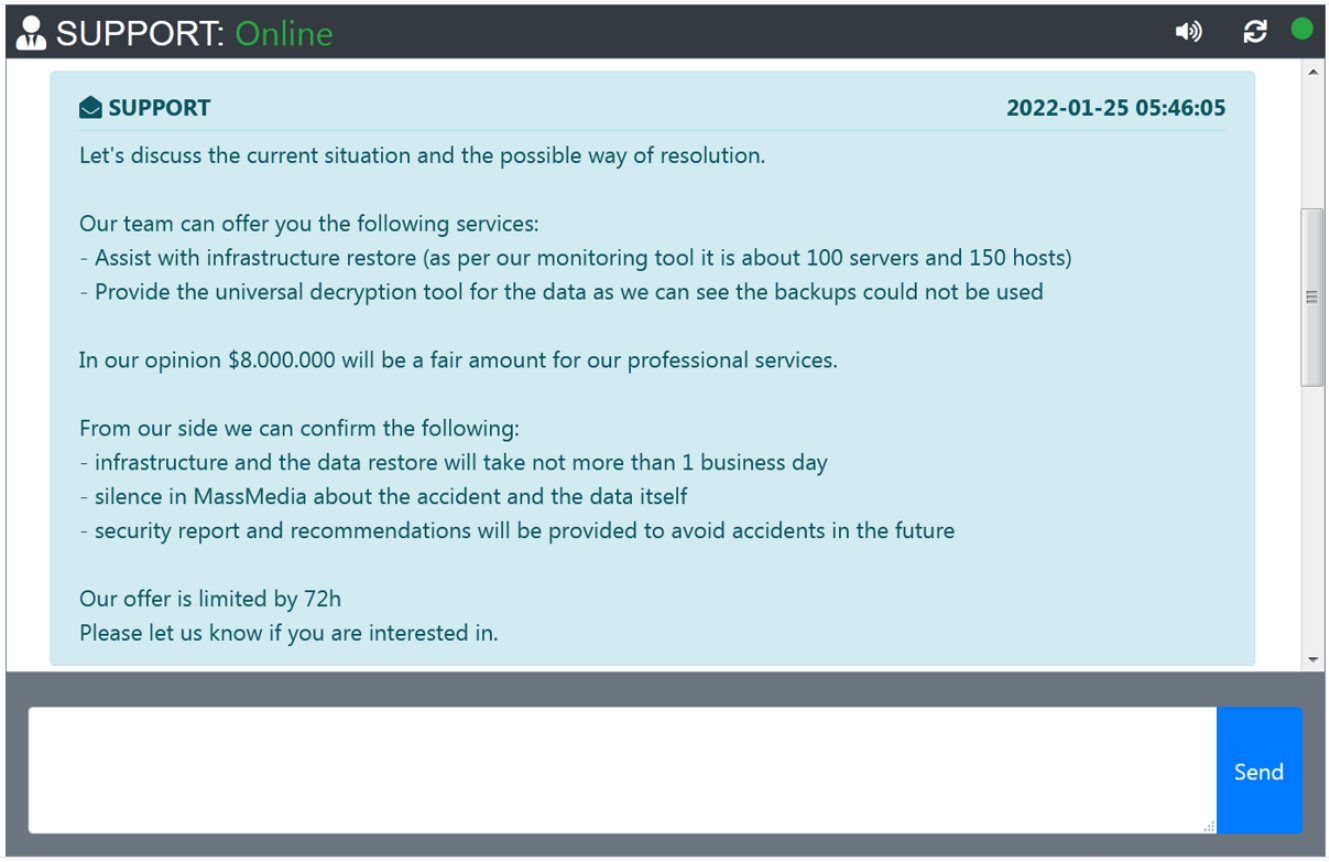
Rebranding of Mount Locker

Same with other ransomware that follow the double extortion trend, that became already a second nature to ransomware, the Quantum Locker has its own data leak TOR website - “Quantum Blog”, and according to it the gang has over 20 victims, with 7 of them being new as of April 2022:



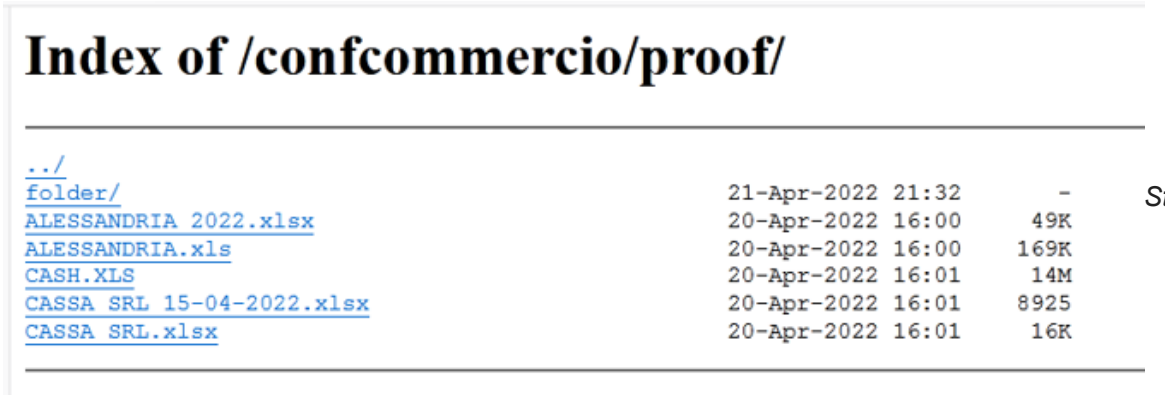
Quantum Leaks website

The ransom demands for the gang vary depending on the victim, with some attacks demanding $150,000 to receive a decryptor, while others are multi-million dollar demands, as shown below:



Quantum support chat

The victim only gets 72 hours to get back in touch with the gang, and if not - the stolen data is shared on the website for free downloads for the public:



Stolen data shared on the Quantum Blog website

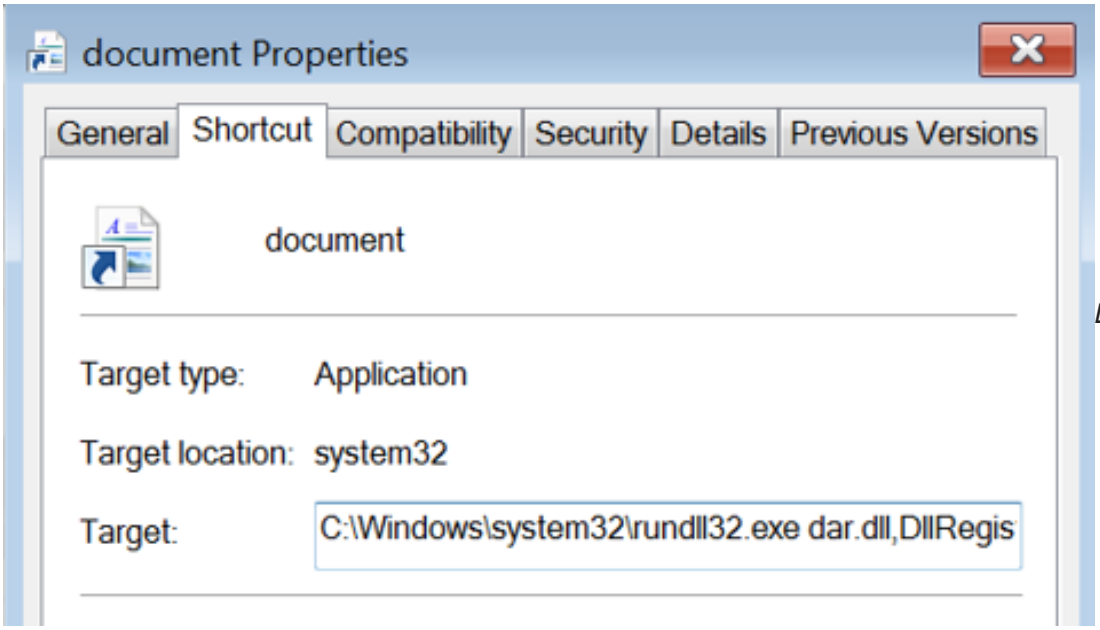
Breaking Down the Attack

Initial Infection Vector - IcedID

The infamous malware, IcedID, that started as a banking trojan back in 2017, is observed being utilized as the initial access by various ransomware gangs. Among those gangs are Conti, REvil, and the former brand of Quantum - the Xing Locker. As for now, the gang seems to continue with this method with the Quantum Locker as well; “If it ain't broke don’t fix it.”

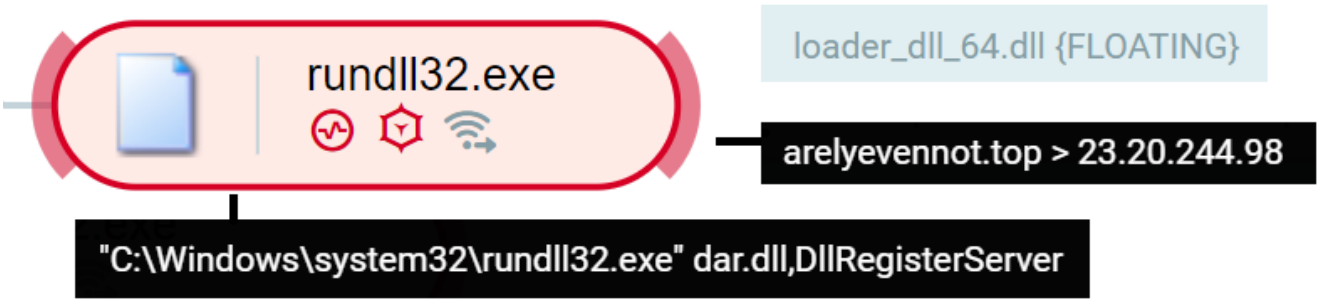
The campaign of IcedID observed ending in Quantum Locker execution starts with a phishing attack via email. The email contained an .iso image file that contains the IcedID loader payload in the form of a DLL (dar.dll) and shortcut file - an .LNK file - that targets the IcedID payload and masquerades as a document.

When mounting the .iso file, the end user only sees the shortcut file named “document”, and the DLL itself is hidden. After the user clicks on the shortcut, the IcedID DLL is executed:



Document.lnk properties

The unpacked DLL is loaded into memory (loader_dll_64.dll) and it begins its communication with the C2:



The execution of the IcedID payload as shown in the Cybereason XDR platform

As with most commodity malware, for example TrickBot, IcedID executes initial discovery commands and then exfiltrates the results via the C2 channel. If threat actors find the organization to be of interest, they will launch the next phase:

```
Cmd.exe /c chcp >&2
Ipconfig /all
Systeminfo
Net config workstation
Nltest /domain_trusts /all_trusts
Net view /all /domain
Net view /all
Net group Domain Admins /domain
```

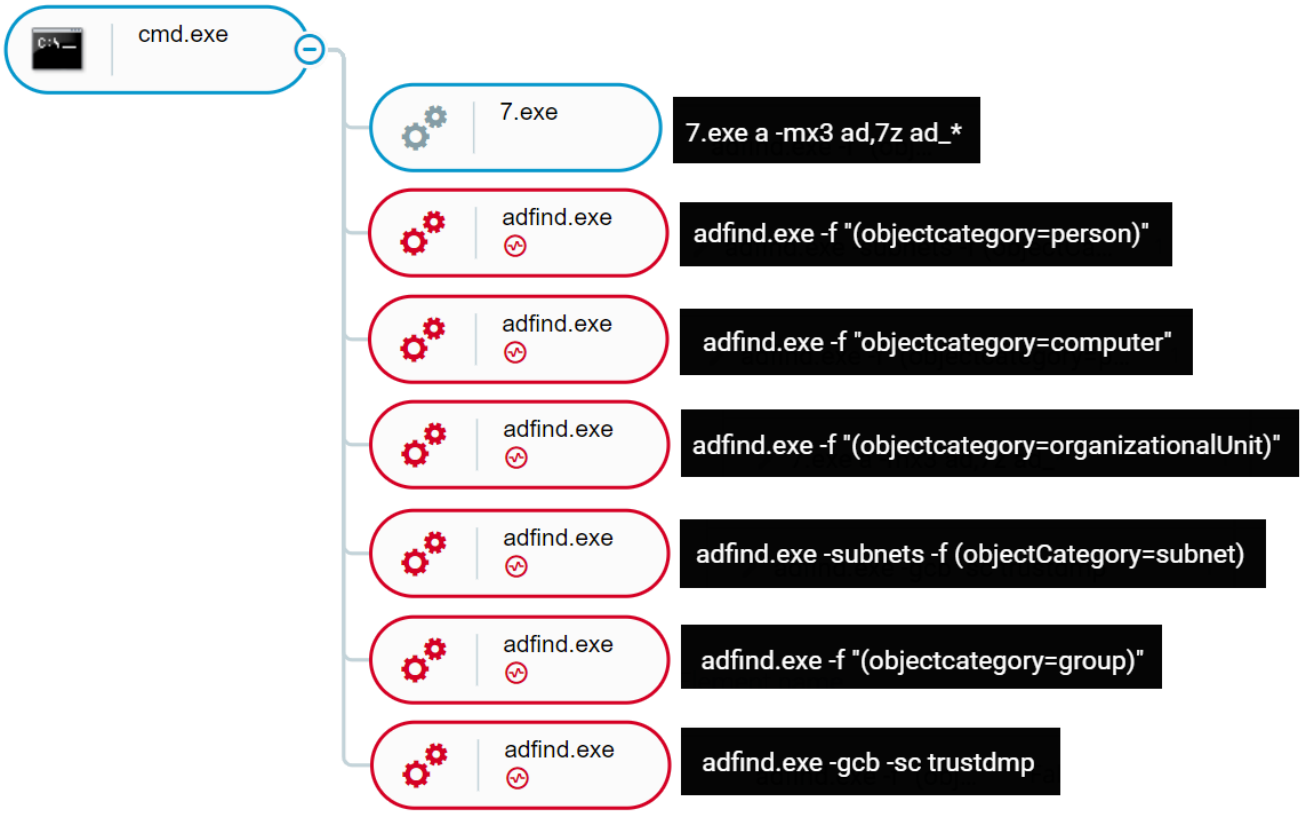
IcedID reconnaissance commands

Moving to an Interactive Attack

The next phase of the attack starts after IcedID sends the reconnaissance output back to the C2. In some cases, it started just two hours after the user clicks on the .lnk file. In this phase, the threat actor starts an interactive attack in the breached network. To do so, they use the initial IcedID implant to download and execute another implant. In most cases the gang used Cobalt Strike beacon to launch the interactive phase.

First, the threat actor wants to perform additional and more in-depth reconnaissance activity. They execute a script named *adfind.bat* that uses the tool AdFind to collect information about the Active Directory. In addition, they also run a batch script named *ns.bat* which runs nslookup for each host in the domain.

The *AdFind.bat* script is dropped in the %temp% directory, along with the AdFind.exe binary and 7Zip binary named 7.exe. The output is saved into .txt files and sent to the C2. After that, the batch file removes tracks by deleting the script, the AdFind binary, the .txt files and the 7Zip binary:

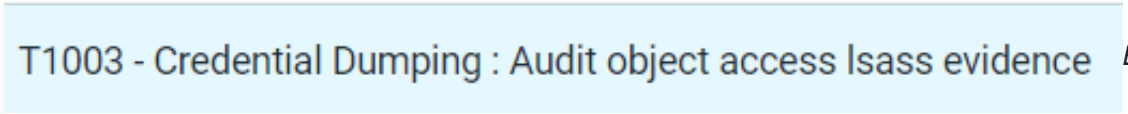


The execution of AdFind.bat, as shown in the Cybereason XDR Platform

Lateral Movement

To move laterally in the environment, the threat actor first dumps the lsass process and gains credentials.

Then, they start making RDP connections to other servers in the environment and remote WMI discovery tasks to test the gained credentials:



Evidence of credential dumping as shown in the Cybereason XDR Platform

After confirming that the credentials work, the threat actor continues to prepare for the deployment of the Quantum Locker. They start spreading in the network by copying the ransomware binary to the other machine's *c$\windows\temp* shared folder and then execute them remotely via WMI and PsExec.

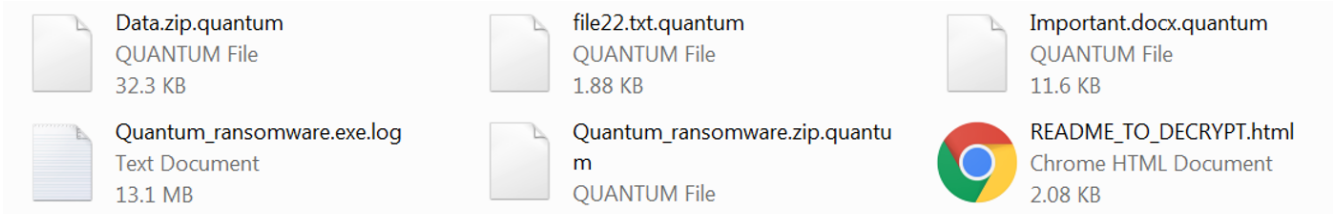
Ransomware Execution

Upon execution, the ransomware first checks for the presence of different services and processes related to security software such as AVs, malware analysis tools, Microsoft Office, browsers and databases. If found, the ransomware tries to kill the service / process:

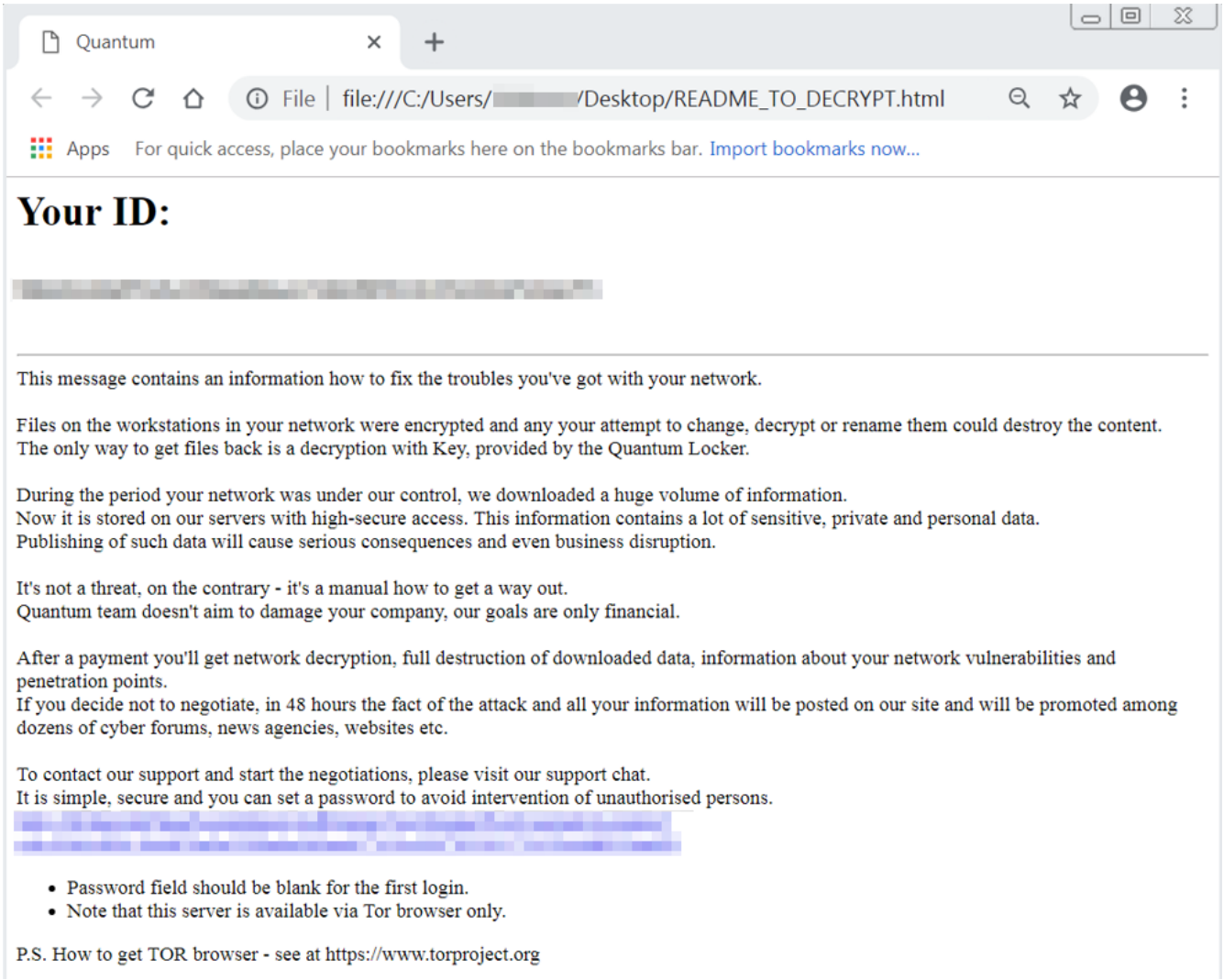
msftesql.exe	ocomm.exe	wordpad.exe
sqlbrowser.exe	mysqld.exe	QBW32.exe
sqlwriter.exe	sqlagent.exe	QBW64.exe
oracle.exe	mysqld-nt.exe	ipython.exe
ocssd.exe	mysqld-opt.exe	wpython.exe
dbsnmp.exe	dbeng50.exe	python.exe
synctime.exe	sqbcoreservice.exe	dumpcap.exe
agntsvc.exe	excel.exe	procmon.exe
isqlplussvc.exe	infopath.exe	procmon64.exe
xfssvccon.exe	msaccess.exe	procexp.exe
sqlservr.exe	mspub.exe	procexp64.exe
encsvc.exe	onenote.exe	thebat.exe
ocautoupds.exe	outlook.exe	steam.exe
mydesktopservice.exe	powerpnt.exe	thebat64.exe
firefoxconfig.exe	sqlservr.exe	thunderbird.exe
firefoxconfig.exe mydesktopqos.exe	visio.exe	
	winword.exe	

List of processes to terminate

Then, the ransomware starts its encryption routine. It encrypts the files on the disc and appends the .quantum extension to it. It also leaves a ransom note named *README_TO_DECRYPT.html:*



Files encrypted by the Quantum Locker



Quantum Locker ransom note

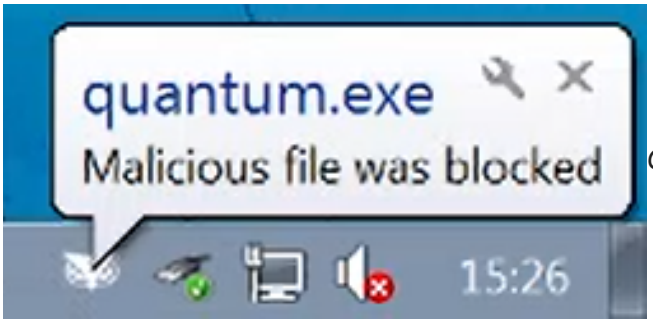
In addition, the ransomware creates a log file for its execution named <ransom_binary>.exe.log. This log file contains information about the machine, user, domain, killed processes and services, and each file's status - if it was encrypted or skipped.

Cybereason Detection and Prevention

The AI-driven Cybereason XDR Platform is able to prevent the execution of the Quantum Locker using multi-layer protection that detects and blocks malware with threat intelligence, machine learning, and next-gen antivirus (NGAV) capabilities. Additionally, when the Anti-Ransomware feature is enabled, behavioral detection techniques in the platform are able to detect and prevent any attempt to encrypt files and generates a MalOp™ for it:

MalOp for Quantum Locker as shown in the Cybereason XDR Platform

Using the Anti-Malware feature with the right configurations (listed in the recommendations below), the Cybereason XDR Platform will also detect and prevent the execution of the ransomware and ensure that it cannot encrypt targeted files. The prevention is based on machine learning, which blocks both known and unknown malware variants:



Cybereason user notification for preventing the execution of Quantum Locker

Security Recommendations

- **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - more information for Cybereason customers can be found here
- **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - more information for cybereason customers can be found here
- **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities
- **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data
- **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

Indicators of Compromise

IOC	Type	Description
b63e94928da25e18caa1506305b9ca3dedc267e747dfa4710860e757d2cc8192	SHA256	Quantum binaries
1d64879bf7b1c7aea1d3c2c0171b31a329d026dc4e2f1c876d7ec7cae17bbc58		
511c1021fad76670d6d407139e5fef62b34ca9656fb735bd7d406728568fa280		
faf49653a0f057ed09a75c4dfc01e4d8e6fef203d0102a5947a73db80be0db1d		
0f3bb820adf6d3bba54988ef40d8188ae48b34b757277e86728bdb8441d01ea2		
0789a9c0a0d4f3422cb4e9b8e64f1ba92f7b88e2edfd14b7b9a7f5eee5135a4f		

8d30ab8260760e12a8990866eced1567ced257e0cb2fc9f7d2ea927806435208 2c84b5162ef66c154c66fed1d14f348e5e0054dff486a63f0473165fdbee9b2e 116e8c1d09627c0330987c36201100da2b93bf27560478be4043c1a834ad8913 99a732c0512bc415668cc3a699128618f02bf154ff8641821c3207b999952533 f72c47948a2cb2cd445135bc65c6bf5c0aaacc262ee9c04d1483781355cda976 f8136eb39ee8638f9eb1acf49b1e10ce73e96583a885e4376d897ab255b39bd6 79e25568a8aeec71d18adc07cdb87602bc2c6048e04daff1eb67e45f94887efc d44c065f04fe13bd51ba5469baa9077efb541d849ad298043739e08b7a90008f 239d1c7cfd5b244b10c56abbf966f226e6a0cb91800e9c683ba427641e642f10 7522b6de340a68881d11aa05e2c6770152e2d49ca5b830821ffce533fad948fd 5bc00ad792d4ddac7d8568f98a717caff9d5ef389ed355a15b892cc10ab2887b	SHA256	IcedID .iso files
138[.]68.42.130 157[.]245.142.66 188[.]166.154.118:80	IP	IcedID C2
dilimoretast[.]com antnosience[.]com oceriesfornot[.]top arelyevennot[.]top	Domain	IcedID C2

MITRE ATT&CK TECHNIQUES

Initial Access	Lateral Movement	Execution	Defense Evasion	Credential Access	Discovery	Collection	Impact
Phishing	Taint Shared Content	Command and Scripting Interpreter: PowerShell	Masquerading	Credentials from Password Stores	Account Discovery	Data from Local System	Data Encrypted for Impact
Valid Accounts	Remote File Copy	Scheduled Task/Job	Process Injection		System Information Discovery		Inhibit System Recovery
		Windows Management Instrumentation			File and Directory Discovery		

User Execution	System Location Discovery

About the Researcher:

LIOR ROCHBERGER, SENIOR THREAT RESEARCHER AND THREAT HUNTER, CYBEREASON

As part of the Nocturnus team at Cybereason, Lior has created procedures to lead threat hunting, reverse engineering and malware analysis teams. Lior has also been a contributing researcher to multiple threat and malware blogs including Bitbucket, Valak, Ramnit, and Racoon stealer. Prior to Cybereason, Lior led SOC operations within the Israeli Air Force.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus