HC3: Analyst Note

August 24, 2022 TLP: White Report: 202208241200

Karakurt Threat Profile

Executive Summary

Karakurt ransomware group, also known as the Karakurt Team and Karakurt Lair, is a relatively new cybercrime group, with researchers reporting its first emergence in late 2021. Karakurt actors claim to steal data and then threaten to auction it off or release it to the public unless they receive payment of the demanded ransom, which have been known to range from $25,000 to $13,000,000 in Bitcoin, with payment deadlines typically set to expire within a week of first contact with the victim. The group likely has ties to the Conti ransomware group, either as a business relationship or as a side business with Conti. Karakurt is also known for extensive harassment campaigns against victims to shame them. HC3 recommends the Healthcare and Public Health Sector (HPH) be aware of their operations and apply appropriate cybersecurity principles and practices found in this document in defending their infrastructure and data against compromise.

Impact to HPH Sector

HC3 has noted at least four attacks affecting the US Healthcare and Public Health Sector since June 2022. The observed attacks have affected an assisted living facility, a dental firm, a healthcare provider, and a hospital.

According to open source reporting, Karakurt typically conducts scanning, reconniasance, and collection on its targets for an estimated two month time span. The threat actor gains access to files containing patient names, addresses, Social Security numbers, dates of birth, medical history information, medical diagnosis information, treatment information, medical record numbers and health insurance information. The threat actor then threatens to release the information unless a ransom is paid.

Report

Once access to a compromised system has been obtained, Karakurt actors deploy Cobalt Strike beacons to enumerate a network [T1083], install Mimikatz to pull plain-text credentials [T1078], use AnyDesk to obtain persistent remote control [T1219], and utilize additional situation-dependent tools to elevate privileges and move laterally within a network.

Karakurt actors then compress (typically with 7zip) and exfiltrate large sums of data—and, in many cases, entire network-connected shared drives in volumes exceeding 1 terabyte (TB)—using open source applications and File Transfer Protocol (FTP) services [T1048], such as Filezilla, and cloud storage services including rclone and Mega.nz [T1567.002]. Following the exfiltration of data, Karakurt actors present the victim with ransom notes by way of “readme.txt” files, via emails sent to victim employees over the compromised email networks, and emails sent to victim employees from external email accounts. The ransom notes reveal the victim has been hacked by the “Karakurt Team” and threaten public release or auction of the stolen data. The instructions include a link to a TOR URL with an access code. Visiting the URL and inputting the access code open a chat application over which victims can negotiate with Karakurt actors to have their data deleted.

Karakurt victims have reported extensive harassment campaigns by Karakurt actors in which employees, business partners, and clients receive numerous emails and phone calls warning the recipients to encourage the victims to negotiate with the actors to prevent the dissemination of victim data. These communications often included samples of stolen data—primarily personally identifiable information (PII),

such as employment records, health records, and financial business records. Victims who negotiate with Karakurt actors receive a "proof of life"—such as screenshots—showing file trees of allegedly stolen data or, in some cases, actual copies of stolen files. Upon reaching an agreement on the price of the stolen data with the victims, Karakurt actors provided a Bitcoin address—usually a new, previously unused address—to which ransom payments could be made. Upon receiving the ransom, Karakurt actors provide some form of alleged proof of deletion of the stolen files, such as a screen recording of the files being deleted, a deletion log, or credentials for a victim to log into a storage server and delete the files themselves.

Karakurt actors appear to obtain access to victim devices primarily:

- By purchasing stolen login credentials [T1589.001] [T1589.002] via cooperating partners in the cybercrime community, who provide Karakurt access to already compromised victims.
- Through buying access to already compromised victims via third-party intrusion broker networks [T1589.001].

Common intrusion vulnerabilities exploited for initial access in Karakurt events include the following:

- Outdated SonicWall SSL VPN appliances [T1133] are vulnerable to multiple recent CVEs
- Log4j "Log4Shell" Apache Logging Services vulnerability (CVE-2021-44228) [T1190]
- Phishing and spearphishing [T1566]
- Malicious macros within email attachments [T1566.001]
- Stolen virtual private network (VPN) or Remote Desktop Protocol (RDP) credentials [T1078]
- Outdated Fortinet FortiGate SSL VPN appliances [T1133]/firewall appliances [T1190] are vulnerable to multiple recent CVEs
- Outdated and/or unserviceable Microsoft Windows Server instances

Indicators of Compromise and Mitigations

As of publication, the below IOCs are being used.

EMAILS

mark.hubert1986[at]gmail[.]com
karakurtlair[at]gmail[.]com
personal.information.reveal[at]gmail[.]com
ripidelfun1986[at]protonmail[.]com
gapreappballye1979[at]protonmail[.]com
confedicial.datas.download[at]protonmail[.]com
armada.mitchell94[at]protonmail[.]com

Protonmail email accounts in the following formats:
victimname_treasure[at]protonmail[.]com
victimname_jewels[at]protonmail[.]com
victimname_files[at]protonmail[.]com

TOR URL: hxxps://omx5iqrdbsoitf3q4xexrqw5r5tfw7vp3vl3li3lfo7saabxazshnead[.]onion

Tools: Rclone.exe;; AnyDesk.exe; Mimikatz

Ngrok: SSH tunnel application SHA256 - 3e625e20d7f00b6d5121bb0a71cfa61f92d658bcd61af2cf5397e0ae28f4ba56

DLLs Masquerading as Legitimate Microsoft Binaries to System32:

Mscxxx.dll: SHA1 - c33129a680e907e5f49bcbab4227c0b02e191770
Msuxxx.dll: SHA1 - 030394b7a2642fe962a7705dcc832d2c08d006f5

Msxsl.exe: Legitimate Microsoft Command Line XSL Transformation Utility SHA1 - 8B516E7BE14172E49085C4234C9A53C6EB490A45

dllhosts.exe: Rclone SHA1 - fdb92fac37232790839163a3cae5f37372db7235

rclone.conf: Rclone configuration file

filter.txt: Rclone file extension filter file

c.bat: UNKNOWN

3.bat: UNKNOWN

Potential Malicious Document:
SHA1 - 0E50B289C99A35F4AD884B6A3FFB76DE4B6EBC14
SHA1 - 7E654C02E75EC78E8307DBDF95E15529AAAB5DFF

Malicious Text File:
SHA1 - 4D7F4BB3A23EAB33A3A28473292D44C5965DDC95
SHA1 - 10326C2B20D278080AA0CA563FC3E454A85BB32F

Cobalt Strike Hashes
SHA256 - 563BC09180FD4BB601380659E922C3F7198306E0CAEBE99CD1D88CD2C3FD5C1B
SHA256 - 5E2B2EBF3D57EE58CADA875B8FBCE536EDCBBF59ACC439081635C88789C67ACA
SHA256 - 712733C12EA3B6B7A1BCC032CC02FD7EC9160F5129D9034BF9248B27EC057BD2
SHA256 - 563BC09180FD4BB601380659E922C3F7198306E0CAEBE99CD1D88CD2C3FD5C1B
SHA256 - 5E2B2EBF3D57EE58CADA875B8FBCE536EDCBBF59ACC439081635C88789C67ACA
SHA256 - 712733C12EA3B6B7A1BCC032CC02FD7EC9160F5129D9034BF9248B27EC057BD2
SHA1 - 86366bb7646dcd1a02700ed4be4272cbff5887af

Ransom Note Text Sample:

1. Here's the deal. We breached your internal network and took control over all of your systems.
2. We analyzed and located each piece of more-or-less important files while spending weeks inside.
3. We exfiltrated anything we wanted (xxx GB (including Private & Confidential information, Intellectual Property, Customer Information and most important Your TRADE SECRETS)
4. FAQ: Who the hell are you?

Payment Wallets:
bc1qfp3ym02dx7m94td4rdaxy08cwyhdamefwqk9hp
bc1qw77uss7stz7y7kkzz7qz9gt7xk7tfet8k30xax
bc1q8ff3lrudpdkuvm3ehq6e27nczm393q9f4ydlgt
bc1qenjstexazw07gugftfz76gh9r4zkhhvc9eeh47
bc1qxfqe0l04cy4qgjx55j4qkkm937yh8sutwhlp4c

bc1qw77uss7stz7y7kkzz7qz9gt7xk7tfet8k30xax
bc1qrtq27tn34pvxaxje4j33g3qzgte0hkwshtq7sq
bc1q25km8usscsra6w2falmtt7wxyga8tnwd5s870g
bc1qta70dm5clfcxp4deqycxjf8l3h4uymzg7g6hn5
bc1qrkcjtdjccpy8t4hcna0v9asyktwyg2fgdmc9al
bc1q3xgr4z53cdaeyn03luhen24xu556y5spvyspt8
bc1q6s0k4l8q9wf3p9wrywf92czrxaf9uvscyqp0fu
bc1qj7aksdmgrnvf4hwjcm5336wg8pcmpegvhzfmhw
bc1qq427hlxpl7agmvfftefIrnasxpu7wznjsu02nc
bc1qz9a0nyrqstqdlr64qu8jat03jx5smxfultwpm0
bc1qq9ryhutrprmehapvksmefcr97z2sk3kdycpqtr
bc1qa5v6amyey48dely2zq0g5c6se2keffvnjqm8ms
bc1qx9eu6k3yhtve9n6jtnagza8l2509y7uudwe9f6
bc1qtm6gs5p4nr0y5vugc93wr0vqf2a0q3sjyxw03w
bc1qta70dm5clfcxp4deqycxjf8l3h4uymzg7g6hn5
bc1qx9eu6k3yhtve9n6jtnagza8l2509y7uudwe9f6
bc1qqp73up3xff6jz267n7vm22kd4p952y0mhcd9c8
bc1q3xgr4z53cdaeyn03luhen24xu556y5spvyspt8

Among the mitigations CISA recommends are to:

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location.
- Implement network segmentation and maintain offline backups of data to ensure limited interruption to the organization.
- Regularly back up data and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Install and regularly update antivirus software on all hosts and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Disable unused ports.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Enforce multi-factor authentication.
- Use National Institute for Standards and Technology (NIST) standards for developing and managing password policies. Require administrator credentials to install software.

References

Karakurt Data Extorition Group
https://www.cisa.gov/uscert/ncas/alerts/aa22-152a

Karakurt Extortion Group Connected to Conti Ransomware?
https://www.secureworld.io/industry-news/karakurt-ransomware-conti

Ransomware Attack Hits More Than 59,000 Patients At Vermont Health Center
https://www.beckershospitalreview.com/cybersecurity/ransomware-attack-hits-more-than-59-000-

patients-at-vermont-health-center.html?utm_campaign=bhr&utm_source=website&utm_content=latestarticles

Texas Hospital Computer Systems Hacked, Patient Social Security Numbers Exposed
https://www.beckershospitalreview.com/cybersecurity/computer-systems-at-texas-hospital-2-surgery-centers-hacked-exposing-social-security-numbers-health-data.html

Links to additional references and resources can be found in the above referenced report.

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback