Karakurt Data Extortion Group

cisa.gov/uscert/ncas/alerts/aa22-152a

Summary

Actions to take today to mitigate cyber threats from ransomware:
• Prioritize patching known exploited vulnerabilities.
• Train users to recognize and report phishing attempts.
• Enforce multifactor authentication.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury (Treasury), and the Financial Crimes Enforcement Network (FinCEN) are releasing this joint Cybersecurity Advisory (CSA) to provide information on the Karakurt data extortion group, also known as the Karakurt Team and Karakurt Lair. Karakurt actors have employed a variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation. Karakurt victims have not reported encryption of compromised machines or files; rather, Karakurt actors have claimed to steal data and threatened to auction it off or release it to the public unless they receive payment of the demanded ransom. Known ransom demands have ranged 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.

Karakurt actors have typically provided screenshots or copies of stolen file directories as proof of stolen data. Karakurt actors have contacted victims' employees, business partners, and clients [T1591.002] with harassing emails and phone calls to pressure the victims to cooperate. The emails have contained examples of stolen data, such as social security numbers, payment accounts, private company emails, and sensitive business data belonging to employees or clients. Upon payment of ransoms, Karakurt actors have provided some form of proof of deletion of files and, occasionally, a brief statement explaining how the initial intrusion occurred.

Prior to January 5, 2022, Karakurt operated a leaks and auction website found at https://karakurt[.]group. The domain and IP address originally hosting the website went offline in the spring 2022. The website is no longer accessible on the open internet, but has been reported to be located elsewhere in the deep web and on the dark web. As of May 2022, the website contained several terabytes of data purported to belong to victims across North America and Europe, along with several "press releases" naming victims who had not paid or cooperated, and instructions for participating in victim data "auctions."

Download the PDF version of this report (pdf, 442kb).

Click here for STIX.

Technical Details

Initial Intrusion

Karakurt does not appear to target any specific sectors, industries, or types of victims. During reconnaissance [TA0043], 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; or
- Through buying access to already compromised victims via third-party intrusion broker networks [T1589.001].

    Note: Intrusion brokers, or intrusion broker networks, are malicious individual cyber actors or groups of actors who use a variety of tools and skills to obtain initial access to—and often create marketable persistence within—protected computer systems. Intrusion brokers then sell access to these compromised computer systems to other cybercriminal actors, such as those engaged in ransomware, business email compromise, corporate and government espionage, etc.

Common intrusion vulnerabilities exploited for initial access [TA001] 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

Network Reconnaissance, Enumeration, Persistence, and Exfiltration

Upon developing or obtaining access to a compromised system, 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].

Extortion

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.

Although Karakurt’s primary extortion leverage is a promise to delete stolen data and keep the incident confidential, some victims reported Karakurt actors did not maintain the confidentiality of victim information after a ransom was paid. **Note:** the U.S. government strongly discourages the payment of any ransom to Karakurt threat actors, or any cyber criminals promising to delete stolen files in exchange for payments.

In some cases, Karakurt actors have conducted extortion against victims previously attacked by other ransomware variants. In such cases, Karakurt actors likely purchased or otherwise obtained previously stolen data. Karakurt actors have also targeted victims at the same time these victims were under attack by other ransomware actors. In such cases, victims received ransom notes from multiple ransomware variants simultaneously, suggesting Karakurt actors purchased access to a compromised system that was also sold to another ransomware actor.

Karakurt actors have also exaggerated the degree to which a victim had been compromised and the value of data stolen. For example, in some instances, Karakurt actors claimed to steal volumes of data far beyond the storage capacity of compromised systems or claimed to steal data that did not belong to the victim.

Indicators of Compromise

Email

mark.hubert1986@gmail.com; karakurtlair@gmail.com; personal.information.reveal@gmail.com; ripidelfun1986@protonmail.com; gapreappballye1979@protonmail.com; confedicial.datas.download@protonmail.com; armada.mitchell94@protonmail.com

Protonmail email accounts in the following formats:
victimname_treasure@protonmail.com
victimname_jewels@protonmail.com
victimname_files@protonmail.com

Tools

Onion site	https://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

Tools	
Potential malicious document	SHA1 - 0E50B289C99A35F4AD884B6A3FFB76DE4B6EBC14

.

Tools	
Potential malicious document	SHA1 - 7E654C02E75EC78E8307DBDF95E15529AAAB5DFF
Malicious text file	SHA1 - 4D7F4BB3A23EAB33A3A28473292D44C5965DDC95
Malicious text file	SHA1 - 10326C2B20D278080AA0CA563FC3E454A85BB32F

Cobalt Strike hashes

SHA256 - 563BC09180FD4BB601380659E922C3F7198306E0CAEBE99CD1D88CD2C3FD5C1B
SHA256 - 5E2B2EBF3D57EE58CADA875B8FBCE536EDCBBF59ACC439081635C88789C67ACA
SHA256 - 712733C12EA3B6B7A1BCC032CC02FD7EC9160F5129D9034BF9248B27EC057BD2
SHA256 - 563BC09180FD4BB601380659E922C3F7198306E0CAEBE99CD1D88CD2C3FD5C1B
SHA256 - 5E2B2EBF3D57EE58CADA875B8FBCE536EDCBBF59ACC439081635C88789C67ACA
SHA256 - 712733C12EA3B6B7A1BCC032CC02FD7EC9160F5129D9034BF9248B27EC057BD2
SHA1 - 86366bb7646dcd1a02700ed4be4272cbff5887af

Ransom note text sample:

> Here's the deal
>
> We breached your internal network and took control over all of your systems.

Ransom note text sample:

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)

Ransom note text sample:

FAQ: Who the hell are you?

Who the hell are you?

Payment Wallets:

bc1qfp3ym02dx7m94td4rdaxy08cwyhdamefwqk9hp
bc1qw77uss7stz7y7kkzz7qz9gt7xk7tfet8k30xax
bc1q8ff3lrudpdkuvm3ehq6e27nczm393q9f4ydlgt
bc1qenjstexazw07gugftfz76gh9r4zkhhvc9eeh47
bc1qxfqe0l04cy4qgjx55j4qkkm937yh8sutwhlp4c
bc1qw77uss7stz7y7kkzz7qz9gt7xk7tfet8k30xax
bc1qrtq27tn34pvxaxje4j33g3qzgte0hkwshtq7sq
bc1q25km8usscsra6w2falmtt7wxyga8tnwd5s870g
bc1qta70dm5clfcxp4deqycxjf8l3h4uymzg7g6hn5
bc1qrkcjtdjccpy8t4hcna0v9asyktwyg2fgdmc9al
bc1q3xgr4z53cdaeyn03luhen24xu556y5spvyspt8
bc1q6s0k4l8q9wf3p9wrywf92czrxaf9uvscyqp0fu
bc1qj7aksdmgrnvf4hwjcm5336wg8pcmpegvhzfmhw
bc1qq427hlxpl7agmvffteflrnasxpu7wznjsu02nc
bc1qz9a0nyrqstqdlr64qu8jat03jx5smxfultwpm0
bc1qq9ryhutrprmehapvksmefcr97z2sk3kdycpqtr

Payment Wallets:
bc1qa5v6amyey48dely2zq0g5c6se2keffvnjqm8ms
bc1qx9eu6k3yhtve9n6jtnagza8l2509y7uudwe9f6
bc1qtm6gs5p4nr0y5vugc93wr0vqf2a0q3sjyxw03w
bc1qta70dm5clfcxp4deqycxjf8l3h4uymzg7g6hn5
bc1qx9eu6k3yhtve9n6jtnagza8l2509y7uudwe9f6
bc1qqp73up3xff6jz267n7vm22kd4p952y0mhcd9c8
bc1q3xgr4z53cdaeyn03luhen24xu556y5spvyspt8

Mitre Att&ck Techniques

Karakurt actors use the ATT&CK techniques listed in table 1.

Table 1: Karakurt actors ATT&CK techniques for enterprise

Reconnaissance		
Technique Title	ID	Use
Gather Victim Identify Information: Credentials	T1589.001	Karakurt actors have purchased stolen login credentials.
Gather Victim Identity Information: Email Addresses	T1589.002	Karakurt actors have purchased stolen login credentials including email addresses.
Gather Victim Org Information: Business Relationships	T1591.002	Karakurt actors have leveraged victims' relationships with business partners.
Initial Access		
Technique Title	ID	Use
Exploit Public-Facing Applications	T1190	Karakurt actors have exploited the Log4j "Log4Shell" Apache Logging Service vulnerability and vulnerabilities in outdated firewall appliances for gaining access to victims' networks.

Reconnaissance		
External Remote Services	T1133	Karakurt actors have exploited vulnerabilities in outdated VPN appliances for gaining access to victims' networks.
Phishing	T1566	Karakurt actors have used phishing and spearphishing to obtain access to victims' networks.
Phishing – Spearphishing Attachment	T1566.001	Karakurt actors have sent malicious macros as email attachments to gain initial access.
Valid Accounts	T1078	Karakurt actors have purchased stolen credentials, including VPN and RDP credentials, to gain access to victims' networks.

Privilege Escalation		
Technique Title	ID	Use
Valid Accounts	T1078	Karakurt actors have installed Mimikatz to pull plain-text credentials.

Technique Title	ID	Use
File and Directory Discovery	T1083	Karakurt actors have deployed Cobalt Strike beacons to enumerate a network.

Technique Title	ID	Use
Remote Access Software	T1219	Karakurt actors have used AnyDesk to obtain persistent remote control of victims' systems.

Exfiltration		
Technique Title	ID	Use
Exfiltration Over Alternative Protocol	T1048	Karakurt actors have used FTP services, including Filezilla, to exfiltrate data from victims' networks.
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Karakurt actors have used rclone and Mega.nz to exfiltrate data stolen from victims' networks.

Mitigations

- 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 (i.e., hard drive, storage device, the cloud).
- 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.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized accounts.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind. Do not give all users administrative privileges.
- 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.
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length;
    - Store passwords in hashed format using industry-recognized password managers;
    - Add password user “salts” to shared login credentials;
    - Avoid reusing passwords;
    - Implement multiple failed login attempt account lockouts;
    - Disable password “hints”;
    - Refrain from requiring password changes more frequently than once per year. **Note:** NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password “patterns” cyber criminals can easily decipher.
    - Require administrator credentials to install software.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

Resources

- For additional resources related to the prevention and mitigation of ransomware, visit Stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide and NIST's Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. Stopransomware.gov is the U.S. government's one-stop location for resources to tackle ransomware more effectively.
- CISA's Ransomware Readiness Assessment is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware.
- Financial Institutions must also ensure compliance with any applicable Bank Secrecy Act requirements, including suspicious activity reporting obligations. Indicators of Compromise, such as suspicious email addresses, file names, hashes, domains, and IP addresses, can be provided under Item 44 of the Suspicious Activity Report (SAR) form. For more information on mandatory and voluntary reporting of cyber events via suspicious activity reports (SARs), see FinCEN Advisory FIN-2016-A005, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, October 25, 2016, and FinCEN Advisory FIN-2021-A004, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, November 8, 2021, which updates FinCEN Advisory FIN-2020-A006.
- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.

Revisions

Initial Version: June 01, 2022

June 2, 2022: Added STIX File

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.