THREAT BULLETINS

Joint Cybersecurity Advisory – Karakurt Data Extortion Group

TLP:WHITE

Jun 01, 2022

Health-ISAC is distributing the following threat bulletin regarding recently observed malicious activity enacted by the Karakurt data extortion group also known as the Karakurt Team and Karakurt Lair. The threat actors tend to utilize ambiguity within their operations as they rely on a variety of tactics, techniques, and procedures (TTPs) creating significant challenges for defense and mitigation. Instead of encrypting compromised systems, Karakurt actors claim to steal data and threaten to auction it off or release the information to the public unless they receive payment by a certain deadline with ransom demands typically ranging from $25,000 to $13,000,000 in Bitcoin.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury, and the Financial Crimes Enforcement Network (FinCEN) released this Joint Cybersecurity Advisory (CSA) (AA22-152A) to provide information regarding Karakurt actors' extortionist activity. The extortionist group typically provides screenshots or copies of stolen data as proof of compromised systems and pressures victims to cooperate by contacting victims' employees, business partners, and clients.

All members are encouraged to review AA22-152A: Karakurt Data Extortion Group for additional details including indicators of compromise (IOCs) and observed MITRE ATT&CK techniques.

Initial Intrusion

Karakurt does not appear to target any specific sectors, industries, or types of victims. During reconnaissance, Karakurt actors appear to obtain access to victim devices primarily:

- By purchasing stolen login credentials;
- 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.

    - **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 in Karakurt events include the following:

- Outdated SonicWall SSL VPN appliances are vulnerable to multiple recent CVEs
- Log4j "Log4Shell" Apache Logging Services vulnerability (CVE-2021-44228)
- Phishing and spearphishing
- Malicious macros within email attachments
- Stolen virtual private network (VPN) or Remote Desktop Protocol (RDP) credentials
- Outdated Fortinet FortiGate SSL VPN appliances/firewall appliances 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, install Mimikatz to pull plain-text credentials, use AnyDesk to obtain persistent remote control 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, such as Filezilla, and cloud storage services including rclone and Mega.nz.

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 opens 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.

Reference(s)	CISA

Recommendations

- 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).

Sources

AA22-152A: Karakurt Data Extortion Group

Alert ID af4da83b

View Alert

Tags Karakurt Data Extortion Group

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**