US Warns Organizations of 'Karakurt' Cyber Extortion Group

By Ionut Arghire on June 02, 2022

Several government agencies in the United States have issued a joint cybersecurity alert to warn organizations about a data extortion group named “Karakurt.”

Also known as the Karakurt Team and Karakurt Lair, the group does not rely on malware to encrypt victims’ files, instead exfiltrating data and threatening to sell it or release it publicly if a ransom is not paid within a specific timeframe.

Typically, the Karakurt hackers give their victims one week to make the payment, with ransom demands ranging between $25,000 and $13 million in Bitcoin, reads the joint alert from 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).

When contacting the victim, the Karakurt actors provide screenshots or copies of stolen files as proof of intrusion. Once the ransom has been paid, the attackers also provide some sort of proof that files have been deleted, and may also share details on how the initial intrusion occurred.

The Karakurt group was also observed harassing victims’ employees, business partners, and clients, in an attempt to pressure the company into making the payment.

Often, the attackers would share samples of stolen data, mainly personally identifiable information (PII), such as Social Security numbers, employment records, and health records, but also private emails, payment accounts, and sensitive business files.

Some victims, however, reported that the attackers "did not maintain the confidentiality of victim information" even if the ransom was paid, the joint advisory says.

Prior to January 2022, the Karakurt group operated a leaks and auction website at https://karakurt[.]group, but the domain went offline in the spring 2022, after reportedly being relocated to 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'," the joint advisory notes.

Karakurt targets organizations regardless of the sector they operate in, mainly using stolen login credentials, through purchased access to compromised systems, or by cooperating with other cybercriminals who already have access to the victims' environments.

Initial access is obtained through exploitation of outdated SonicWall or Fortinet FortiGate VPN appliances, via the Log4Shell vulnerability, via phishing and spearphishing, via stolen VPN or RDP credentials, or via outdated Microsoft Windows Server instances.

Once access to a victim's environment has been obtained, Karakurt actors deploy Cobalt Strike Beacon, employ Mimikatz to extract credentials, achieve persistent remote control using AnyDesk, and use various other tools for privileges elevation and lateral movement.

Data is then compressed and exfiltrated in large amounts, typically using open source applications and File Transfer Protocol (FTP) services.

The threat actors then email ransom notes to the victims' employees, informing them that the organization had been compromised and instructing the victim to access a Tor website to contact Karakurt for negotiation.

"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," the joint advisory reads.

In a recent report, cybersecurity firm AdvIntel noted that Karakurt is part of the Conti network, operating as an autonomous group alongside Black Basta and BlackByte, two other groups that rely on data theft and extortion to monetize access to victims' systems.

Related: **SecurityWeek Cyber Insights 2022: Ransomware**

Related: **US: Hackers Continue Aiding North Korea Generate Funds via Cryptocurrency Attacks**

Related: **US Critical Infrastructure Targeted by AvosLocker Ransomware**

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Foxconn Confirms Ransomware Hit Factory in Mexico