Karakurt extortion group: Threat profile

Published: 2022-06-14 · Archived: 2026-04-05 21:21:59 UTC

Jovi Umawing

June 14, 2022

Jovi Umawing

The FBI (Federal Bureau of Investigation), together with CISA (Cybersecurity and Infrastructure Security Agency) and other federal agencies, recently released a joint cybersecurity advisory (CSA) about the Karakurt data extortion group (also known as Karakurt Team and Karakurt Lair).

Like RansomHouse, Karakurt doesn't bother encrypting data. Instead, it just steals the data and demands a ransom. If the victim organization refuses to pay up, the stolen data is auctioned off or leaked to the public for anyone to scrape and misuse for personal gain.

One may wonder why federal agencies decided to focus on Karakurt when it is a relatively obscure group. It has no prolific attacks attributed to it and doesn't appear to have a high number of attacks under its belt.

According to Bleeping Computer, Karakurt is said to be the "data extortion arm" of the Conti ransomware syndicate. Further evidence from two blockchain traffic firms, Chainalysis and Tetra Defense, can back this up. In a report last month, they assessed"with a high degree of confidence" that Karakurt is "operationally linked to both Conti and Diavol ransomware groups".

Article continues below this ad.

Karakurt extortion group

The Karakurt group got its name from a type of black widow spider. Researchers have pointed outthat the group liken its extortion tactics to a karakurt spider's bite.

> Karakurts poison is very toxic and dangerous. Dont waste your time.
> What would you do? Of course you will have to take an antidote.
> In your situation it means that you still have a chance to survive. But it will cost as double.
> All you need is to accept our terms and conditions without any sort of bargain.

```
Karakurts poison is very toxic and dangerous. Don't waste your time.What would you do? Of course you will have
```

The NCC Group's Cyber Incident Response Team (CIRT) spotlighted Karakurt activities in February 2022. However, Karakurt, known initially as the Karakurt Hacking Team (KHT), has been around since June 2021. This also marked the creation of domains and accounts associated with the group, namely its dump sites and, later on, its Twitter account in August 2021.

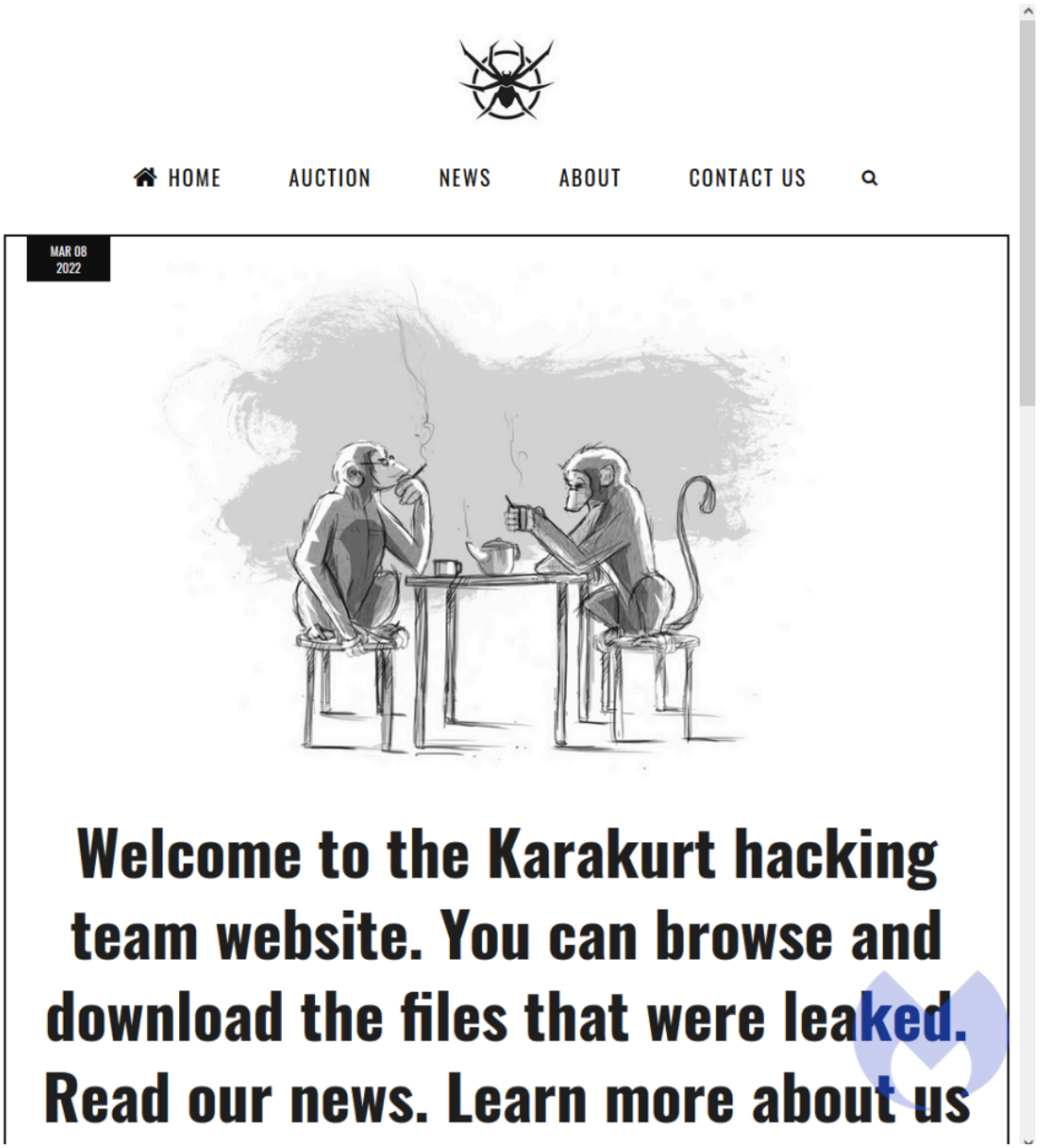
Per a report from Accenture Security, Karakurt wasn't actively extorting until September 2021. After two months, the extortion group had already bagged 40 organizations across multiple industries. However, experts from Digital Shadows seem to dispute this number, claiming that the victim number is more than 80.

Regarding victimization, it's clear that Karakurt isn't picky with what to target. Regarding target locations, the extortion group prefers small organizations based in the US, the UK, Canada, and Germany.

The extortion group targets organizations using single-factor Fortigate VPN (Virtual Private Network) servers using legitimate Active Directory credentials. It is unknown how the group obtains these credentials; however, it's no surprise that they get administrative access and privileges on compromised servers.

From there, Karakurt can use the various tools it has at its disposal. Depending on the goals, the group can do a "living off the land" approach in its tactics, toolset, and intrusion techniques. It can also use common post-exploit tools like Cobalt Strike, AnyDesk, and Mimikatz.

Once Karakurt has the data it wants to exfiltrate, it uses 7zip and WinZip to compress the files before sending them to `Mega.io` via FileZilla or Rclone.



Karakurt demands a ransom ranging from $25,000 to $13M in Bitcoin. The payment deadline is typically seven days after the victim contacts the extortion group.

Splintering into cells

Ransomware groups have been undergoing a new phasefor a few months now. If they're not splitting into smaller groups ("cells") to join other criminal groups, they are rotating their use of malware to avoid the growing US sanctions and pressure from law enforcement.

Since the US officially sanctioned Evil Corp, the Russian group behind the Dridex banking Trojan, things started changing, both on the side of ransomware victims and affiliates that use ransomware. Victims began refusing to pay to comply with sanctions, and these groups started rotating the use of ransomware variants in their campaigns to avoid getting associated with a sanctioned group.

With Conti "gone,"a splintering also happened within the syndicate. Researchers from Advanced Intel have data showing members of the former ransomware syndicate dispersing from the core group to join smaller ransomware groups.

Conti is not affiliated with Evil Corp, but both groups are in a similar bind that affects their profit margins but not enough to make them completely give up a criminal life. Unfortunately, members and affiliates gain from splintering and distancing themselves from these groups.

In an interviewwith the Wall Street Journal, Kimberly Goody, Mandiant's director of cybercrime analysis, said that these changes obscured Evil Corp hackers' identities "at the point of attack, throwing off investigators and sanction-compliant victim companies". The same can be said about former actors associated with the Conti syndicate.

Keep Karakurt away from your network *and*data

We advise organizations to prioritize mitigating steps to keep extortion groups like Karakurt from successfully infiltrating your network. Here are some ways to do that.

- Implement multi-factor authentication (MFA)in every business access point, including single-factor VPN access
- Ensure that all domain control servers are kept updated with the latest patches
- Disable unused ports
- Install an efficient and effective endpoint security solution that focuses on a layered approach to protecting systems and business assets
- Create and implement a recovery plan (if your business doesn't have one already), including how to maintain and retain backups
- Segment your network to keep bad guys from reaching destinations that house your organization's most sensitive and proprietary data
- Audit high-privileged accounts regularly

The federal agencies have more mitigation points in the advisory, which you can find here.

Stay safe!

Source: https://blog.malwarebytes.com/cybercrime/2022/06/karakurt-extortion-group-threat-profile/