

Karakurt rises from its lair

[accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation](https://www.accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation)

Share

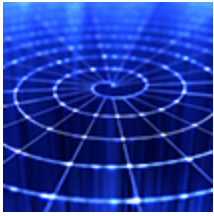
Executive summary

- A previously unconfirmed, financially motivated threat group operating under the self-proclaimed name, “Karakurt” started ramping up attacks late in the third quarter of 2021 and continued into the fourth quarter.
- The presence of Karakurt was first identified in June 2021 as it registered its apparent dump-site domains: karakurt[.]group and karakurt[.]tech, followed by their Twitter handle “karakurlair” in August 2021.
- Accenture Security first observed Karakurt intrusion clusters in September 2021, when multiple sightings occurred within a short timeframe.
- The threat group has claimed to have impacted over 40 victims across multiple industries between September 2021 and November 2021.
- Of note, Karakurt focuses solely on data exfiltration and subsequent extortion, rather than the more destructive ransomware deployment.
- Accenture Security observed the threat group modify its tactics depending on the victim environment, favoring a more “living off the land” approach and often avoiding the use of common post-exploitation tools like Cobalt Strike.
- While Accenture Security identified that the threat group utilized attack infrastructure previously associated with other cybercrime operators, we are not yet able to determine if the threat group operates under an affiliate-based model, or a ransomware-as-a-service (RaaS) operation, based on observed intrusion clusters.
- Accenture Security assess with high confidence that the group's operations have just begun, and that Karakurt activity will likely continue to proliferate into the foreseeable future, impacting additional victims.

The information outlined in this blog is based on information collected from CIFR incident response engagements, threat intelligence insights, open-source intelligence (OSINT) analysis and various media and industry reports.

This is a developing story; additional technical analysis of the intrusion clusters, attacker TTPs and indicators of compromise (IOCs) will be released to the community in a separate blog post.

<<< Start >>>



Diving into double extortion campaigns

READ MORE

<<< End >>>

Summary & timeline

Accenture Security has identified a new threat group, the self-proclaimed Karakurt Hacking Team, that has impacted over 40 victims across multiple geographies. The threat group is financially motivated, opportunistic in nature, and so far, appears to target smaller companies or corporate subsidiaries versus the alternative big game hunting approach. Based on intrusion analysis to date, the threat group focuses solely on data exfiltration and subsequent extortion, rather than the more destructive ransomware deployment. In addition, Accenture Security assesses with moderate-to-high confidence that the threat group's extortion approach includes steps to avoid, as much as possible, drawing attention to its activities.

High level timeline:

<<< Start >>>

KARAKURT TIMELINE

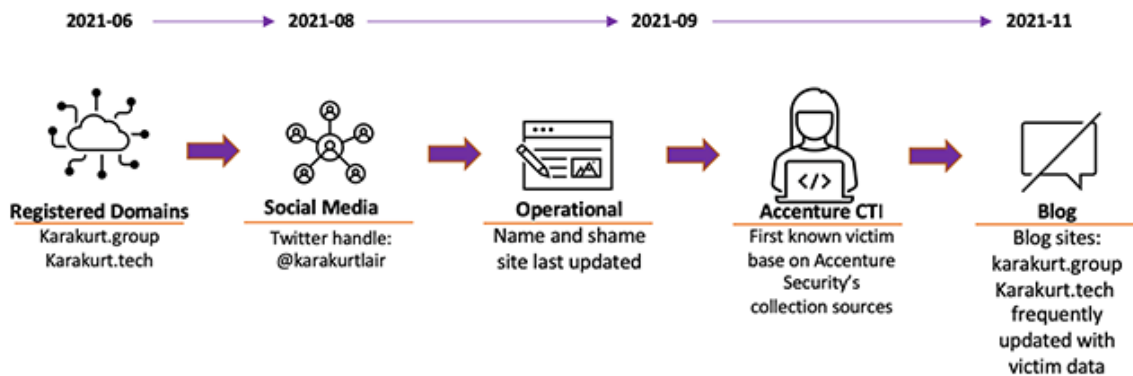


Figure 1. High level Karakurt group website timeline

<<< End >>>


- Karakurt[.]group and karakurt[.]tech – registered on **June 5th, 2021**.
- Twitter handle karakurtlair – created in **August 2021**.
- Karakurt known to be operational as early as **September 2021**, which is when components on its name and shame site were updated.
- First known victim based on Accenture Security’s collection sources and intrusion analysis – **September 2021**.
- First victim revealed on karakurt[.]group on **November 17, 2021**.
- First update to karakurt[.]group “News” page, with volumes 1 – 3 of the threat group’s “Autumn Data Leak Digest” on **November 19, 2021**.
- The fourth installment of “Autumn Data Leak Digest”, released on **November 22, 2021**.

<<< Start >>>



[HOME](#) [AUCTION](#) [NEWS](#) [ABOUT](#) [CONTACT US](#) [Q](#)

NOV 15
2021



Welcome to the Karakurt hacking team website. You can browse and download the files that were leaked. Read our news. Learn more about us and on how we operate.

Figure 2. Karakurt[.] group main page

<<< End >>>

<<< Start >>>



Figure 3. Latest "News" from Karakurt[.] group

<<< End >>>

<<< Start >>>

ABOUT



We thought for a long time what to write on this page. Since you're here - you've got the point by now, right? You probably think that we are nothing more than another team of online scammers trying to make money. In part, this is probably true, but for us the situation looks different. So how are we different in our opinion? We strongly condemn the low threshold of knowledge required now to implement attacks on commercial networks, hacking turns into a routine work, frameworks have simplified the process to trivial button presses. For our part, we try to approach our work as creatively as possible, improving various techniques and deeply immersing ourselves in the study of products related to modern information security tools. If you've been the victim of a hack and data theft, don't be in a rush to blame your security team, it just wasn't their day. The budgets that you spend on the purchase of protective equipment and software can only complicate our work, they can never completely protect you, but we, for our part, love complex tasks very much.

Now a few words on the case. We do not try to harm your processes, delete your data, destroy your business, at least until you yourself give us a reason. We never attack the same target twice. We always adhere to the agreements we have concluded. We do not bargain, never bargain, never bargain at all. The reason is simple - spending considerable time researching the obtained data, including financial indicators, we always know how much you are able to pay so that you do not have to delay salaries or cancel any projects. We know how long it will take for you. Don't try to deceive us. The final storage points for your data are disconnected from the internet, so you won't be able to localize them and deny us access to them.

Sofisticated. Evasive. Deep. Persistent.

Figure 4. Karakurt[.] group "About" page

<<< End >>>

Victimology

Based on our collection sources, Accenture Security is currently aware of over 40 victims spanning multiple industry verticals and size. The Karakurt group does not appear to focus on a specific industry vertical or size. Of known victims, 95% are based in North America with the remaining 5% in Europe. From our investigations into the group's activity, we

determined that it typically uses credential access as the initial vector into victims' networks and utilizes applications already installed to move laterally and exfiltrate data, if available. In addition, the threat group will typically contact the victim multiple times, using different communication methods, to apply additional pressure during extortion attempts. Figure 5 includes the known impacted industry verticals to date, based on Accenture Security's collection sources.

<<< Start >>>

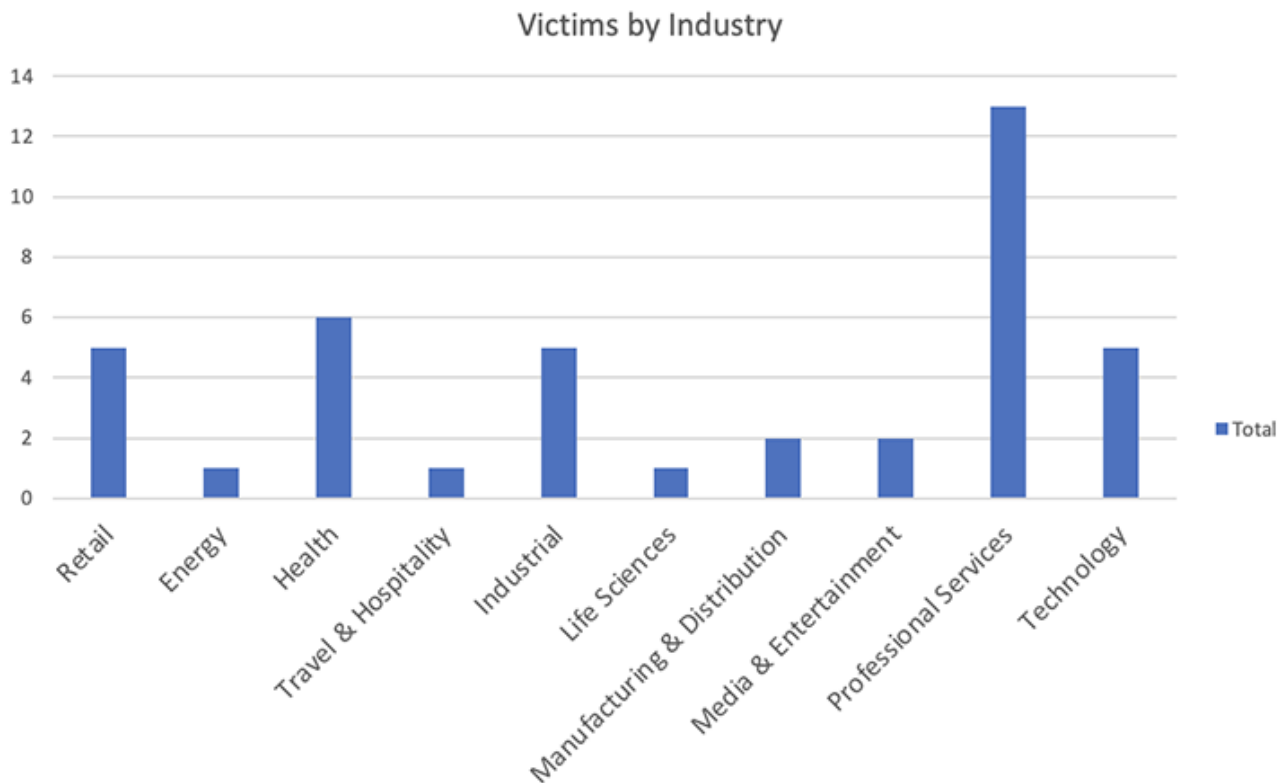


Figure 5. Victim Verticals

<<< End >>>

Compromise activity & detection opportunities

Initial access

The primary method for initial access into victim networks includes internet-facing systems via virtual private network (VPN) using legitimate credentials. Due to a lack of forensic evidence, it is unclear how the credentials were obtained by the threat group. One possibility is exploitation of vulnerable VPN devices, but all cases included inconsistent or absent enforcement of multi-factor authentication (MFA) for user accounts.

In Table 1 below, Accenture Security noted logons from four different hosting providers, to include the autonomous system that currently hosts the Karakurt group's blog site.

Login time	Autonomous system
2021-10-12 07:24:45	RELIABLESITE
2021-09-28 04:22:54	Datasource AG
2021-09-28 03:50:08	DEDIPATH-LLC
2021-09-27 03:41:05	DEDIPATH-LLC
2021-09-23 04:42:20	Clouvider Limited

Persistence

The use of legitimate credentials, service creation, remote management software and distribution of command and control (C2) beacons across victim environments using Cobalt Strike are the predominant approaches used by the threat group to further its foothold and maintain persistence.

However, in recent intrusions, the threat group did not deploy backup persistence using Cobalt Strike. Instead, it persisted within the victim's network via the VPN IP pool or installed AnyDesk to allow external remote access to compromised devices. The group was then able to leverage previously obtained user, service, and administrator credentials to move laterally and take action on objectives.

Privilege escalation

Accenture Security observed the threat group leveraging Mimikatz in at least one intrusion set, as well as PowerShell to dump ntds.dit and exfiltrate it for offline analysis.

However, the threat group appears to escalate privileges using the aforementioned techniques and tools only if needed, typically using previously obtained credentials.

Defense evasion

Using valid credentials, pre-existing "living off the land" tools and techniques and remote management software has enabled the threat group to further evade defenses.

In one intrusion, Accenture Security also observed the threat group avoiding the use of common post-exploitation tools or commodity malware in favor of credential access. This approach enabled it to evade detection and bypass security tools such as common endpoint detection and response (EDR) solutions.

Discovery

If the threat group's preferred tools are not present within victims' networks, it will download common remote management and file transfer utilities via a browser to support subsequent exfiltration activities (e.g., AnyDesk, FileZilla, 7zip, etc.).

The threat group was also observed running internet speed tests via a browser to check for upload speeds before executing exfiltration activities. In addition, the use of Angry IP Scanner was identified in at least one intrusion set.

Lateral movement

The threat group has been known to use AnyDesk, or other available remote management tools, remote desktop protocol (RDP), Cobalt Strike, PowerShell commands and valid credentials taken from initial access to move laterally.

Command and control

In addition to using valid credentials to log into the VPN directly, the threat group has utilized Cobalt Strike for C2 for backup persistence, if needed.

Exfiltration and impact

The threat group has been seen utilizing 7zip and WinZip for compression, as well as Rclone or FileZilla (SFTP) for staging and final exfiltration to Mega.io cloud storage.

The staging directories utilized for exfiltration were C:\Perflogs and C:\Recovery.

<<< Start >>>



Ransomware response and recovery.

READ MORE

<<< End >>>

Suggested mitigations

- Employ robust and routine user-awareness and training regimens for users of all systems.
- Ensure that a robust crisis management and incident response plan are in place in the event of a high impact intrusion.
- Maintain best practices against malware, such as patching, updating anti-virus software, implementing strict network egress policies, and using application whitelisting where feasible.
- Patch infrastructure to the highest available level, as threat actors are often better able to exploit older systems with existing vulnerabilities.

- Ensure all internet-facing security and remote access appliances are patched to the latest versions.
- Disable RDP on external-facing devices and restrict workstation-to-workstation RDP connections.
- Employ a strong corporate password policy that includes industry standards for password length, complexity, and expiration dates for both human and non-human accounts.
- Use MFA where possible for authenticating corporate accounts to include remote access mechanisms and security tools. Admin accounts should be cross-platform MFA enforced.
- Use admin accounts only for administrative purposes and never to connect to the network or browse the internet.
- Do not store unprotected credentials in files and scripts on shared locations.
- Deploy EDR across the environment, targeting at least 90% coverage of endpoint and workload visibility.
- Encrypt data at rest where possible and protect related keys and technology.
- Hunt for attacker TTPs, including common “living off the land” techniques, to proactively detect and respond to a cyber-attack and mitigate its impact.

MITRE ATT&CK

Tactics and techniques observed

Tactic	Technique
Initial access	T1133: External Remote Services T1078: Valid Accounts
Execution	T1059: Command and Scripting Interpreter T1086: PowerShell T1035: Service Execution
Persistence	T1078: Valid Accounts T1050: New Service
Privilege escalation	T1078: Valid Accounts
Defense Evasion	T1078: Valid Accounts T1036: Masquerading T1027: Obfuscated Files or Information
Credential Access	T1110: Brute Force T1003: Credential Dumping

Discovery	T1083: File and Directory Discovery T1082: System Information Discovery T1087: Account Discovery T1135: Network Share Discovery T1069: Permission Groups Discovery T1018: Remote System Discovery T1016: System Network Configuration Discovery
Lateral Movement	T1076: Remote Desktop Protocol T1028: Windows Remote Management
Collection	T1005: Data from Local System T1039: Data from Network Shared Drive
Command & Control	T1043: Commonly Used Port T1105: Remote File Copy T1071: Standard Application Layer Protocol
Exfiltration	T1002: Data Compressed T1048: Exfiltration Over Alternative Protocol
Impact	T1489: Service Stop

If you have an incident or need additional information on ways to prevent, detect, respond to, or recover from, cyberthreats, contact a member of our CIFR team 24/7/365 by phone 888-RISK-411 or email CIFR.hotline@accenture.com

Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates.

Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change. The information in this alert is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. As such, all information and content set out is provided on an “as-is” basis without representation or warranty and the reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion. Accenture accepts no liability for any action or failure to act in response to the information contained or referenced in this alert.

Copyright © 2021 Accenture. All rights reserved.



Cyber Investigations, Forensics and Response (CIFR)

The CIFR team helps Accenture’s global clients prepare for, respond to and recover from cyber intrusions and minimize business impact.

Subscribe to Accenture's Cyber Defense Blog [Subscribe to Accenture's Cyber Defense Blog](#)

[Subscribe](#)
