Hive Pro

Threat Level

Red

THREAT ADVISORY

# ACTOR REPORT

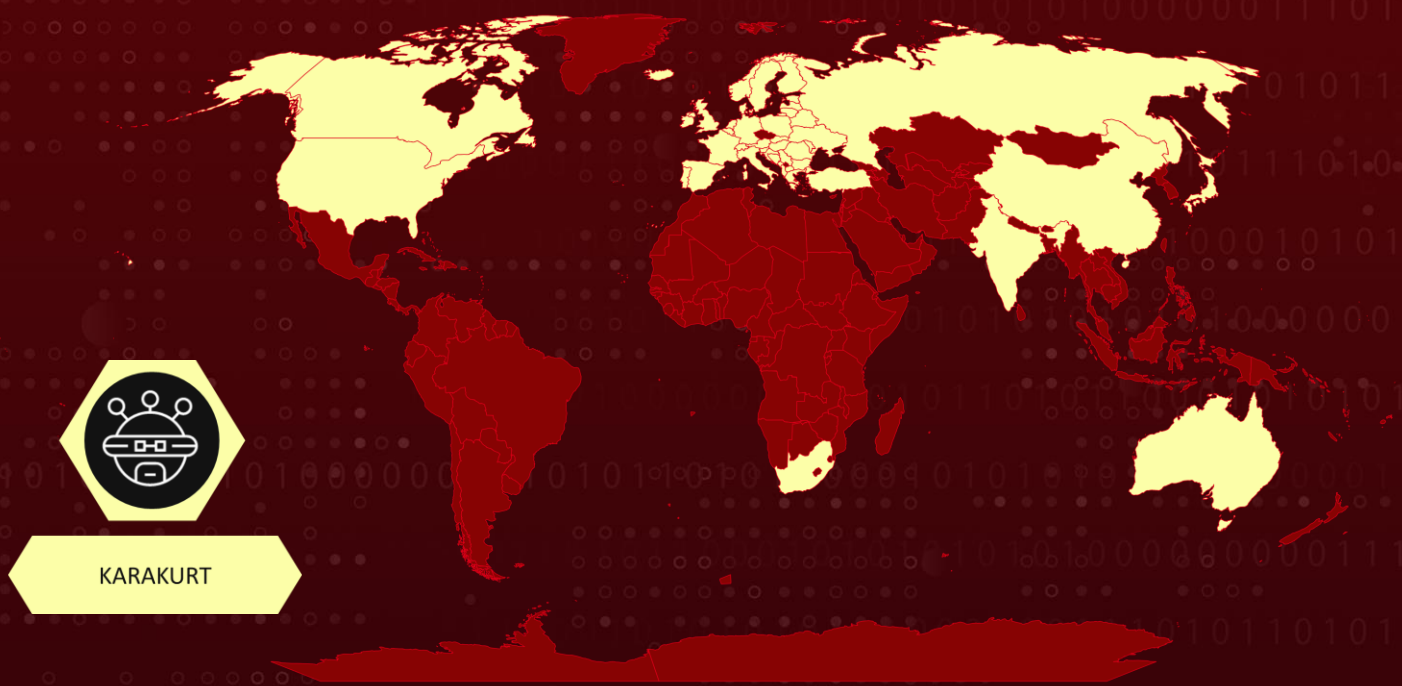
# Healthcare industry tore down by Karakurt ransomware group

| Date of Publication | Admiralty code | TA Number |
| --- | --- | --- |
| August 26, 2022 | A1 | TA2022184 |

# Summary

The Karakurt ransomware group is a recent addition to the list of cybercriminal gangs, with reports of its first appearance in late 2021. Since June 2022, the recent attacks have had an impact on the US healthcare and public health sectors.

## Actor Map



# Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0007**<br>Discovery | **T1083**<br>File and Directory Discovery | **TA0001**<br>Initial Access | **T1078**<br>Valid Accounts |
| **T1190**<br>Exploit Public-Facing Application | **T1566**<br>Phishing | **T1566.001**<br>Spearphishing Attachment | **TA0004**<br>Privilege Escalation |
| **TA0003**<br>Persistence | **T1133**<br>External Remote Services | **TA0005**<br>Defense Evasion | **TA0011**<br>Command and Control |
| **T1219**<br>Remote Access Software | **TA0010**<br>Exfiltration | **T1048**<br>Exfiltration Over Alternative Protocol | **T1567**<br>**Exfiltration Over Web Service** |
| **T1567.002**<br>Exfiltration to Cloud Storage | **TA0043**<br>Reconnaissance | **T1589**<br>Gather Victim Identity Information | **T1589.001**<br>Credentials |
| **T1589.002**<br>Email Addresses | | | |

# Technical Details

**#1** Karakurt's typical two-month dwell period for victim profiling, during which the actors do scanning, reconnaissance, and data collection on the victims. Karakurt gains access by purchasing stolen login credentials.

**#2** After gaining access to a target device, Karakurt actors use Cobalt Strike beacons to examine the network, Mimikatz to retrieve plain-text credentials, AnyDesk to obtain persistent remote control, and other circumstance specific tools to escalate privileges. Eventually threat actor acquires access to files that contain medical and health insurance records that is compressed and exfiltrated.

**#3** Following exfiltration, Karakurt sends the ransom message in "readme.txt" files to the victim organization's employee email accounts. The ransom messages threaten to make the stolen data public or auction it off unless ransom is paid.

## Actor Detail

| NAME | ORIGIN | MOTIVE | TARGET LOCATIONs | TARGET INDUSTRIES |
|---|---|---|---|---|
| Karakurt | Unknown | Financial gain | USA,Hungary,Belarus,Austria,Serbia,Switzerland,Germany,Holy See,Andorra,Bulgaria,United Kingdom, France,Montenegro, Luxembourg,Italy,DenmarkFinland,Slovakia,Norway,Ireland,Spain,Malta,Ukraine,Croatia,Moldova,Monaco,Liechtenstein,Poland Iceland,San Marino, Bosnia and Herzegovina,Albania,Lithuania, NorthMacedonia,Slovenia, Romania,Latvia,Netherlands,Russia,Estonia,Belgium,CzechRepublic(Czechia),Greece,Portugal Sweden,South Africa,Canada ,Japan, Australia,China,Hong Kong,Turkey and India | Energy, Entertainment,Healthcare, Hospitality, Industrial, Manufacturing,Retail and Technology. |

# Indicator of Compromise (IOC)

| TYPE | VALUE |
|---|---|
| SHA-256 | 3e625e20d7f00b6d5121bb0a71cfa61f92d658bcd61af2cf5397e0ae28f4ba56<br>563bc09180fd4bb601380659e922c3f7198306e0caebe99cd1d88cd2c3fd5c1b<br>5e2b2ebf3d57ee58cada875b8fbce536edcbbf59acc439081635c88789c67aca<br>712733c12ea3b6b7a1bcc032cc02fd7ec9160f5129d9034bf9248b27ec057bd2<br>563bc09180fd4bb601380659e922c3f7198306e0caebe99cd1d88cd2c3fd5c1b<br>5e2b2ebf3d57ee58cada875b8fbce536edcbbf59acc439081635c88789c67aca<br>712733c12ea3b6b7a1bcc032cc02fd7ec9160f5129d9034bf9248b27ec057bd2 |
| Emails | mark.hubert1986[at]gmail[.]com<br>karakurtlair[at]gmail[.]com<br>personal.information.reveal[at]gmail[.]com<br>ripidelfun1986[at]protonmail[.]com<br>gapreappballye1979[at]protonmail[.]com<br>confedicial.datas.download[at]protonmail[.]com<br>armada.mitchell94[at]protonmail[.]com |
| SHA1 | c33129a680e907e5f49bcbab4227c0b02e191770030394b7a2642fe962a7705dcc832d2c08d006f58b516e7be14172e49085c4234c9a53c6eb490a45fdb92fac37232790839163a3cae5f37372db72350e50b289c99a35f4ad884b6a3ffb76de4b6ebc147e654c02e75ec78e8307dbdf95e15529aaab5dff4d7f4bb3a23eab33a3a28473292d44c5965ddc9510326c2b20d278080aa0ca563fc3e454a85bb32f86366bb7646dcd1a02700ed4be4272cbff5887af |

## Recent Breaches

https://www.sappi.com/
https://www.calin.gr/
https://methodistmckinneyhospital.com/
https://www.solvgroup.com/
https://www.metapts.com/
https://tombarrow.com/
https://www.trantorinc.com/
http://faberinc.com/index.asp
https://www.goodwillindustries.ca/
https://rewash.jp/
https://waskaganish.ca/
https://meritus.gp/
https://shields.com/
https://www.assuragroup.com.au/
https://www.betterworldbooks.com/
http://hanbell.com.cn/
https://thegreenfactory.net/
https://www.vioramed.com/
https://www.vsoftconsulting.com/
https://okaki.com/
https://charlesriverapparel.com/
https://www.notaire-saindon.com/
https://paraccaflooring.com/
https://www.norwoodhome.com.hk/
https://www.corenetglobal.org/
https://www.fivestarproducts.com/
https://www.lawsonproducts.com/
https://www.catalogicsoftware.com/

## References

https://www.hhs.gov/sites/default/files/karakurt-threat-profile-analyst-note.pdf

# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.


At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**August 26, 2022 • 5:15 AM**



More at www.hivepro.com