The Record.
Recorded Future® News

IMAGE: MOHAMMAD ALI DAHAGHIN VIA UNSPLASH

James Reddick

May 25th, 2023

Briefs

Iran-linked hackers Agrius deploying new ransomware against Israeli orgs

An Iran-linked advanced persistent threat group is using new ransomware while targeting a familiar adversary in the Middle East, researchers have found.

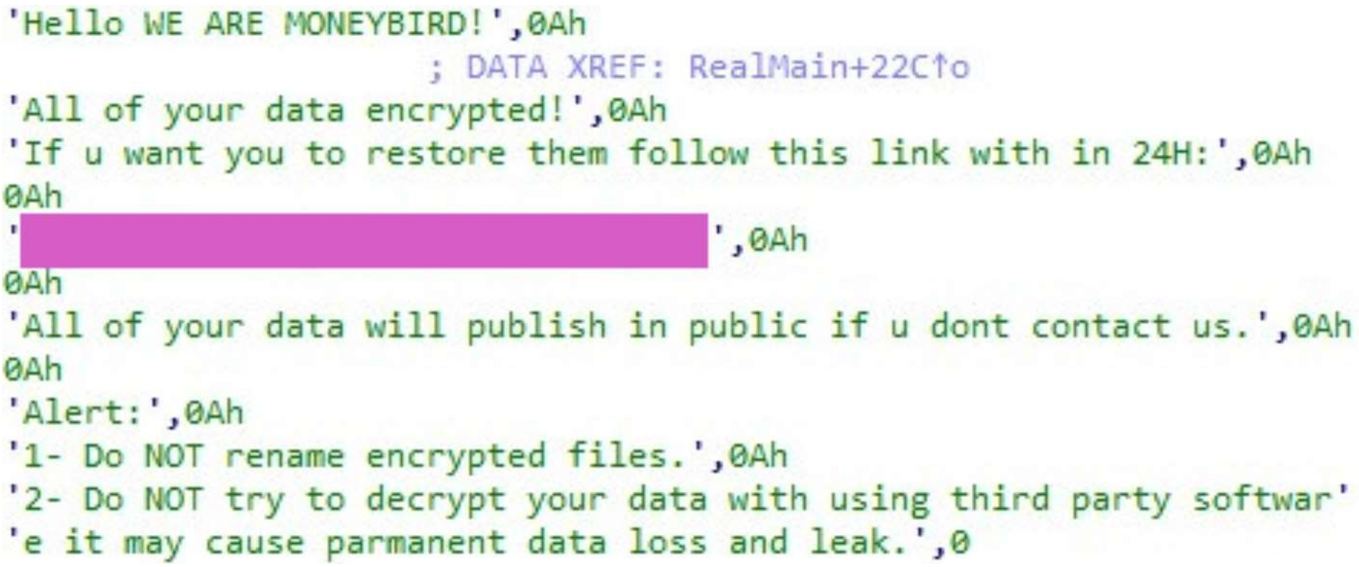
Check Point's Incident Response Team investigated the deployment of the ransomware against Israeli organizations and claimed by a group dubbing itself Moneybird. Researchers found that it bore the hallmarks of Agrius, a hacker group that has been around since 2020 and has attempted to disguise itself with aliases like BlackShadow.

The group is known for having targeted the Israeli insurance company Shirbit with ransomware in late 2020 and Bar-Ilan University in 2021, and for deploying wiper attacks.

According to Check Point investigators, Moneybird is a new product for the group. Most of its previous attacks have been carried out with ransomware called Apostle.

"The use of a new ransomware, written in C++, is noteworthy," they wrote, "as it demonstrates the group's expanding capabilities and ongoing effort in developing new tools."

The researchers did not elaborate on the sort of organizations targeted but said, despite the new payload, the techniques used bore the stamp of Agrius.



```
'Hello WE ARE MONEYBIRD!',0Ah
                      ; DATA XREF: RealMain+22C↑o
'All of your data encrypted!',0Ah
'If u want you to restore them follow this link with in 24H:',0Ah
0Ah
'[redacted]',0Ah
0Ah
'All of your data will publish in public if u dont contact us.',0Ah
0Ah
'Alert:',0Ah
'1- Do NOT rename encrypted files.',0Ah
'2- Do NOT try to decrypt your data with using third party softwar'
'e it may cause parmanent data loss and leak.',0
```

A ransom note from Moneybird. Credit: Check Point

As in previous attacks, the threat actors gained entry via public-facing web servers and the deployment of "unique variants of ASPXSPY" — a malicious script they hid inside "Certificate" text files.

They then moved laterally within networks, conducting reconnaissance and exfiltrating data. The group uses "targeted paths" that program the ransomware to disregard most files on a targeted network, Check Point said.

"Moneybird, like many other ransomware, is a grim reminder of the importance of good network hygiene, as significant parts of the activity could have been prevented early on," the researchers said.

A recent report from Microsoft Threat Intelligence found that the Iranian government is increasingly focused on combining influence operations with cyberattacks. They linked 24 "cyber-enabled operations" to the Iranian government last year, compared to seven the year before, and found a corresponding decline in the sorts of ransomware and wiper attacks typically deployed by Agrius.

This week, however, cyber intelligence firm ClearSky reported that a suspected Iranian APT group had targeted eight Israeli websites connected to shipping and logistics in watering hole attacks — where specific users are targeted by infecting the sites they commonly visit.

ClearSky researchers linked the attacks "with a low confidence" to the Iranian nation-state hacker group Tortoiseshell, also called TA456 and Imperial Kitten.

Tags

Iran Ransomware

Previous article

Next article

JAMES REDDICK

James Reddick has worked as a journalist around the world, including in Lebanon and in Cambodia, where he was Deputy Managing Editor of The Phnom Penh Post. He is also a radio and podcast producer for outlets like Snap Judgment.

Ransomware gang demands €10 million after attacking Spanish council

| January 16th, 2024

UK privacy watchdog to examine practice of web scraping to get training data for AI

| January 15th, 2024

Microsoft to keep all European cloud customers' personal data within EU

| January 13th, 2024

British cosmetics firm Lush confirms cyberattack| January 13th, 2024

FCC presses carmakers, wireless providers to protect domestic abuse survivors from stalking tools

| January 12th, 2024

Further analysis of Denmark attacks leads to warning about unpatched network gear

| January 12th, 2024

Republican lawmakers want answers on SEC social media hack — and soon

| January 11th, 2024

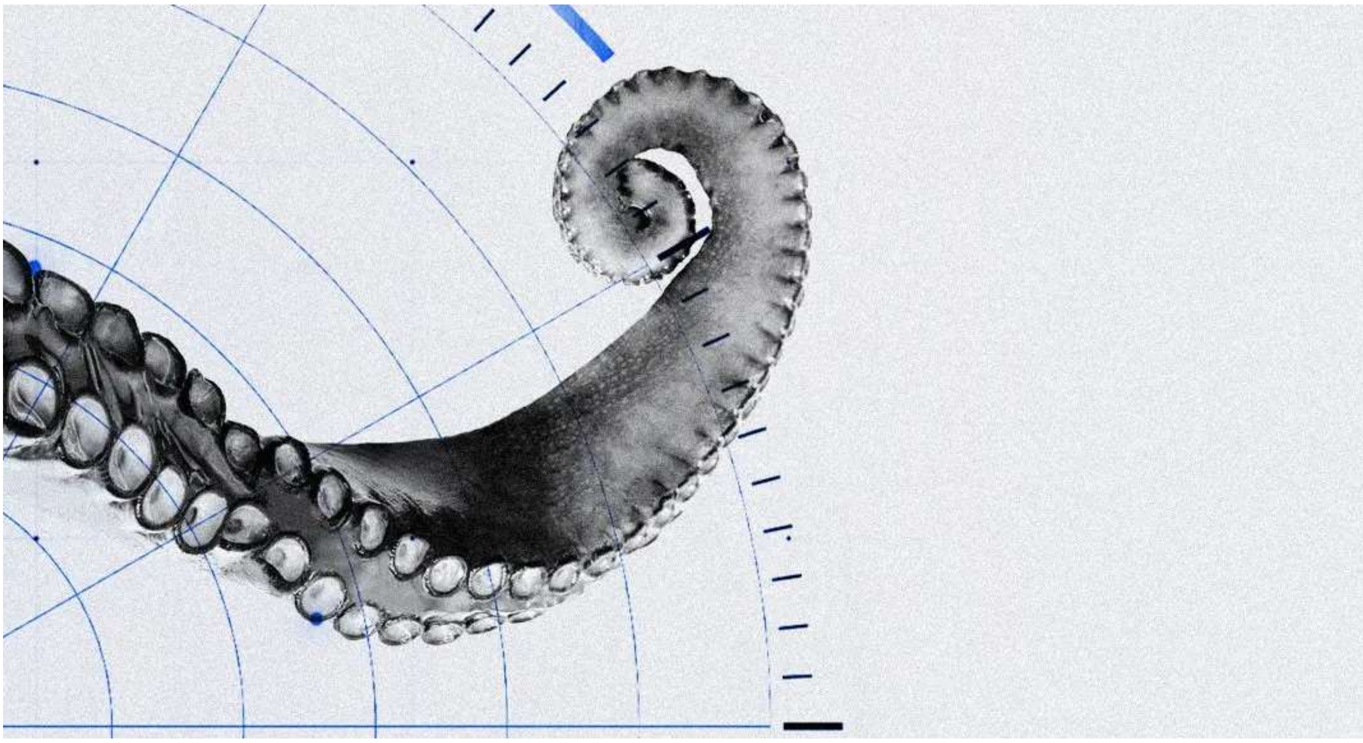
French hacker from 'ShinyHunters' group sentenced to three years in US prison

| January 11th, 2024

SEC's X account compromised, used to spread false bitcoin announcement

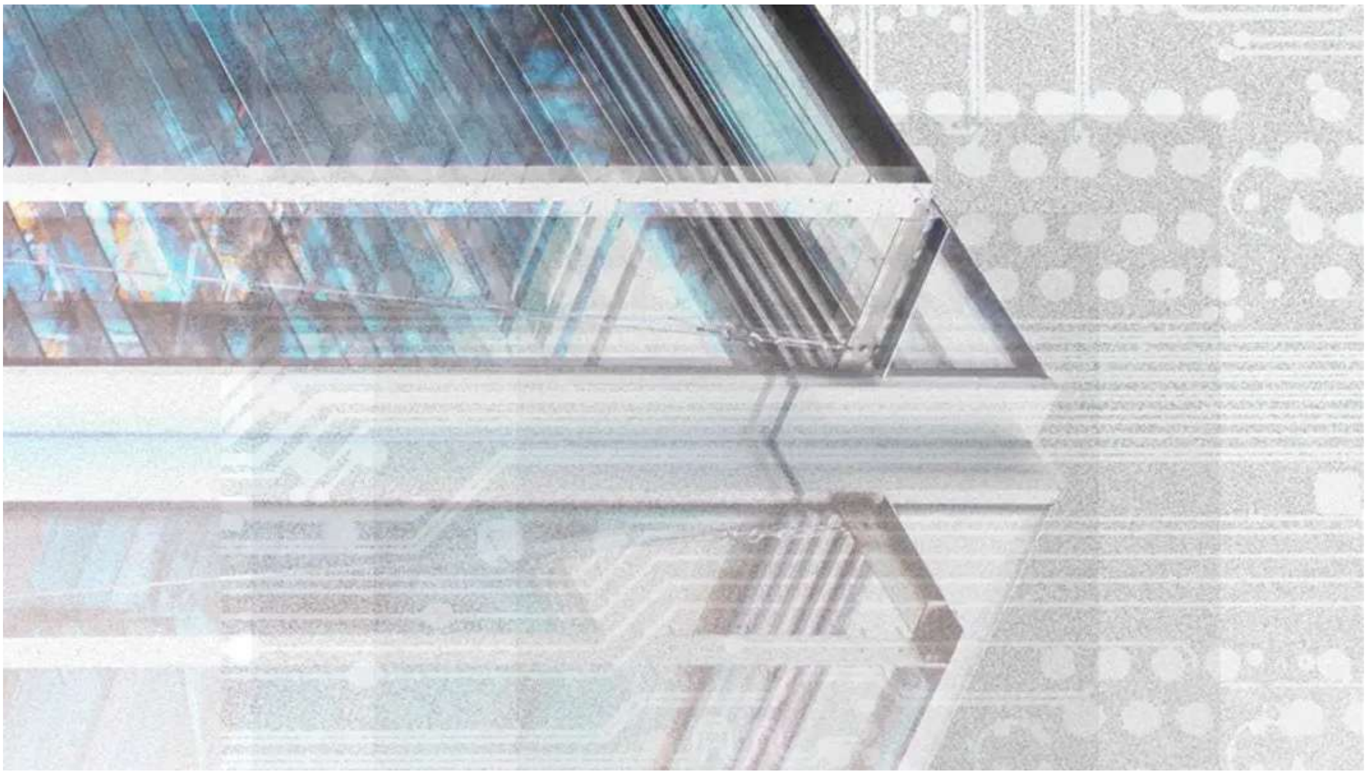
| January 10th, 2024

FLYING UNDER THE RADAR: ABUSING GITHUB FOR MALICIOUS INFRASTRUCTURE



FLYING UNDER THE RADAR: ABUSING GITHUB FOR MALICIOUS INFRASTRUCTURE

2023 ADVERSARY INFRASTRUCTURE REPORT



2023 ADVERSARY INFRASTRUCTURE REPORT

ANNUAL PAYMENT FRAUD INTELLIGENCE REPORT: 2023

ANNUAL PAYMENT FRAUD INTELLIGENCE REPORT: 2023

AGGRESSIVE MALIGN INFLUENCE THREATENS TO SHAPE US 2024 ELECTIONS

AGGRESSIVE MALIGN INFLUENCE THREATENS TO SHAPE US 2024 ELECTIONS

OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK “DOPPELGÄNGER” SIGNALS EVOLVING TACTICS

OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK “DOPPELGÄNGER” SIGNALS EVOLVING TACTICS

The Record.
Recorded Future® News

Privacy About Contact Us