# Void Manticore Attacking Organizations with Destructive Wiper Malwares

Date: 23rd May 2024 | Severity: Medium

## Summary

Since October 2023, an Iranian group called Void Manticore conducted destructive attacks using wipers and ransomware against Israeli organizations. They leaked data under the 'Karma' persona and used a custom wiper named 'BiBi'. Void Manticore collaborated with another group, "Scarred Manticore," exchanging victims.

## Attack Vectors

- Their tactics were basic but benefited from Scarred Manticore's sophisticated access to high-value targets. The hacking group 'Karma' emerged out of the conflicts in the Middle East, using the 'BiBi' wiper and an anti-zionist persona that opposed Israeli PM Netanyahu.
- While initially seen as typical hacktivists, Karma made a name for itself through a campaign to publicize intrusions of over 40 Israeli entities and data-dumping them. Attribution revealed a high degree of overlap between the leaks of Karma and the victims of the Iranian group Scarred Manticore.
- Digital forensics revealed another postaccess persona, Void Manticore, through a "handoff" process involving web shells and shared credentials that allowed Void Manticore to deploy BiBi on Scarred Manticore's prior victims, Check Point said.
- What is noticeable about the Void Manticore is their use of simple and direct methods of attack, which might be called "quick and dirty." They most often initially compromise internet-connected servers using web shells such as "Karma Shell."
- They use RDP to validate domain admin credentials, drop tunneling shells (like reGeorge), and reconnaissance information. They create their own wipers either to corrupt some specific file types for a targeted effect or destroy the entire partition table, consequently rendering all disk data unavailable.
- This has been done purposely by them because it aligns with their objective of performing quick destructive wiper attacks that follow hand-off access from other groups. Here below, we have mentioned all the wipers used:-
  1. Cl Wiper
  2. Partition Wipers
  3. BiBi Wiper

# Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| File Hash | • D0C03D40772CD468325BBC522402F7B737F18B8F37A89BACC5C8A00C2B87BFC6<br>• DEEAF85B2725289D5FC262B4F60DDA0C68AE42D8D46D0DC19B9253B451AEA25A<br>• 87F0A902D6B2E2AE3647F10EA214D19DB9BD117837264AE15D622B5314FF03A5<br>• 85FA58CC8C4560ADB955BA0AE9B9D6CAB2C381D10DBD42A0BCEB8B62A92B7636<br>• 74D8D60E900F931526A911B7157511377C0A298AF986D42D373F51AAC4F362F6<br>• CC77E8AB73B577DE1924E2F7A93BCFD852B3C96C6546229BC8B80BF3FD7BF24E |
| IPADDRESS | • 64[.]176[.]169[.]22<br>• 64[.]176[.]172[.]235<br>• 64[.]176[.]172[.]165<br>• 64[.]176[.]173[.]77<br>• 64[.]176[.]172[.]101 |

# Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes and block IPs.
- Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.
- Update and Patch operating system, applications, and security software's up to date with latest patches.

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Links

- https://cybersecuritynews[.]com/void-manticore-attacking-organizations/
- https://blog[.]checkpoint[.]com/research/unveiling-void-manticore-structured-collaboration-between-espionage-and-destruction-in-mois/