Rewterz Threat Alert - MurenShark APT Threat Actors aka Actor210426 - Active IOCs - Rewterz

Published: 2023-02-15 · Archived: 2026-04-02 11:11:48 UTC

Severity

High

Analysis Summary

In April 2021, researchers identified a new advanced threat entity, Actor210426, which was later named MurenShark. MurenShark is an APT group active in the Middle East, primarily targeting Turkey. This group attacked the Turkish Navy project called “MÜREN” in 2022 and is believed to have shown interest in military projects. In addition to this, it has also been discovered that the group has targeted research institutes, universities and other sensitive targets. This group is known to have rich experience in counter-analysis, reverse traceability and other forms of cyber espionage. It has also been observed that this group has been known to use attack tools and methods to avoid easy detection. The group also uses compromised websites as its file server and command and control (C&C) server, employing split-functionality in order to conceal its activity and extend its reach. It is also believed to be using a known attack tool, called NiceRender, to phish victims.

MurenShark has been linked to various cyber espionage campaigns, including the theft of intellectual property and other sensitive data. The group is known for using a variety of sophisticated tactics, techniques, and procedures (TTPs) to evade detection and maintain persistence within target networks.

Impact

- Penetration Of Targeted Network
- Key Data Theft
- Intellectual Property Theft

Indicators of Compromise

MD5

- 059f01038dfc4c084cb3b9c847c8eab9
- 378ed43137e00a12c3cf013f98c3d653

SHA-256

- 4c04d38ded8afb34af4617b5ed73db263c64593525ea729423838f5b2e4bd975
- 505867bd9495f47db05a249280c1c6a5236ba4ffe305645f54db48527fcb74eb

SHA-1

- 6fd230bc18bd8a8f1c4847212050c56e668cdd66
- 454c3515ee0487c94b4bb4e9f6ebd7b8c2ef192d

Remediation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls
- Maintain cyber hygiene by updating your anti-virus software and implementing a patch management lifecycle.
- Maintain Offline Backups
- Emails from unknown senders should always be treated with caution.
- Never trust or open ” links and attachments received from unknown sources/sender
- Strengthen Endpoint security with antivirus software, firewalls, and other security tools that can help detect and prevent malware infections.
- Implement Access Control policies that restrict access to sensitive data and resources can help limit the damage of a potential breach.
- Assess the organization’s security posture that can help identify vulnerabilities and address them before they can be exploited by threat actors like MurenShark.
