Agonizing Serpens Attack Detection: Iran-Backed Hackers Target Israeli Tech Firms and Educational Institutions

socprime.com/blog/agonizing-serpens-attack-detection-iran-backed-hackers-target-israeli-tech-firms-and-educational-institutions/

Daryna Olyniychuk

Daryna Olyniychuk

Agonizing Serpens

The increasing menace posed by nation-state actors continuously increases with new sophisticated attack methods adopted by APT collectives and a massive shift towards stealthiness & operational security. Recently, security researchers revealed a destructive campaign against Israeli organizations launched by an Iran-affiliated hacker group dubbed Agonizing Serpens (aka Agrius, BlackShadow). The main objective of this offensive operation was to extract personally identifiable information (PII) and intellectual property from targeted institutions, followed by wiper malware deployment.

Detect Agonizing Serpens Attacks

Being a relatively novel actor in the malicious arena, Iran-affiliated Agonizing Serpens APT has been concentrating its efforts on the Middle East region, with multiple malicious campaigns launched since 2020.

To help security professionals timely detect Agonizing Serpens attacks, SOC Prime Platform for collective cyber defense aggregates a set of curated detection algorithms accompanied by extensive CTI and metadata. All the rules are compatible with 28 SIEM, EDR, XDR, and Data Lake technologies and mapped to MITRE ATT&CK to streamline threat investigation. Just hit the **Explore Detections** button below and drill down to a dedicated content set.

Explore Detections

Additionally, cyber defenders can leverage SOC Prime's Uncoder AI to hunt for relevant IOCs provided by Palo Alto Networks Unit 42 in their investigation covering the latest campaign targeting Israel.

Agonizing Serpens_IOC_Uncoder

Agonizing Serpens Attack Analysis

Agonizing Serpens collective has been continuously attacking Middle Eastern entities since 2020, with data-wiping malware used as a primary weapon in their attacks. The group came into the spotlight with an Apostle wiper used in operations against Israel and the United Arab Emirates. Apostle has been initially disguised as ransomware, covertly destroying the victim's data but in time the malware has been modified to act as an actual ransomware strain. Further, the group switched to Fantasy wiper to proceed with offensive operations against Israel and South Africa.

According to the recent inquiry by Palo Alto Networks Unit42, Agonizing Serpens leveraged three brand-new wipers dubbed MultiLaer, PartialWasher, and BFG, in their latest campaign against Israeli companies, which lasted between January and October 2023. Before switching to the data destruction phase, threat actors exfiltrated sensitive details from targeted database servers using the Sqlextractor tool, explicitly searching for PII and intellectual property details. Further, the stolen info, including passports, email creds, and addresses, has been shared within social media and Telegram messenger to damage the victims' reputation.
Notably, the hackers made their pass to the targeted instances by weaponizing exposed internet-facing servers, with further web shell deployment and reconnaissance activities to steal login details and gain admin rights. According to researchers, data wipers have been used to cover any traces of intrusion and add to the reputational damage consequences.

Growing volumes of cyber attacks by state-backed APT groups and their increasing sophistication require ultra-responsiveness from cyber defenders. Stay ahead of any offensive campaigns with access to the latest detection algorithms from the Threat Detection Marketplace against APTs, malware, and any emerging attacks of any scale.

Table of Contents

Join SOC Prime's Detection as Code platform to improve visibility into threats most relevant to your business. To help you get started and drive immediate value, book a meeting now with SOC Prime experts.

Related Posts