Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

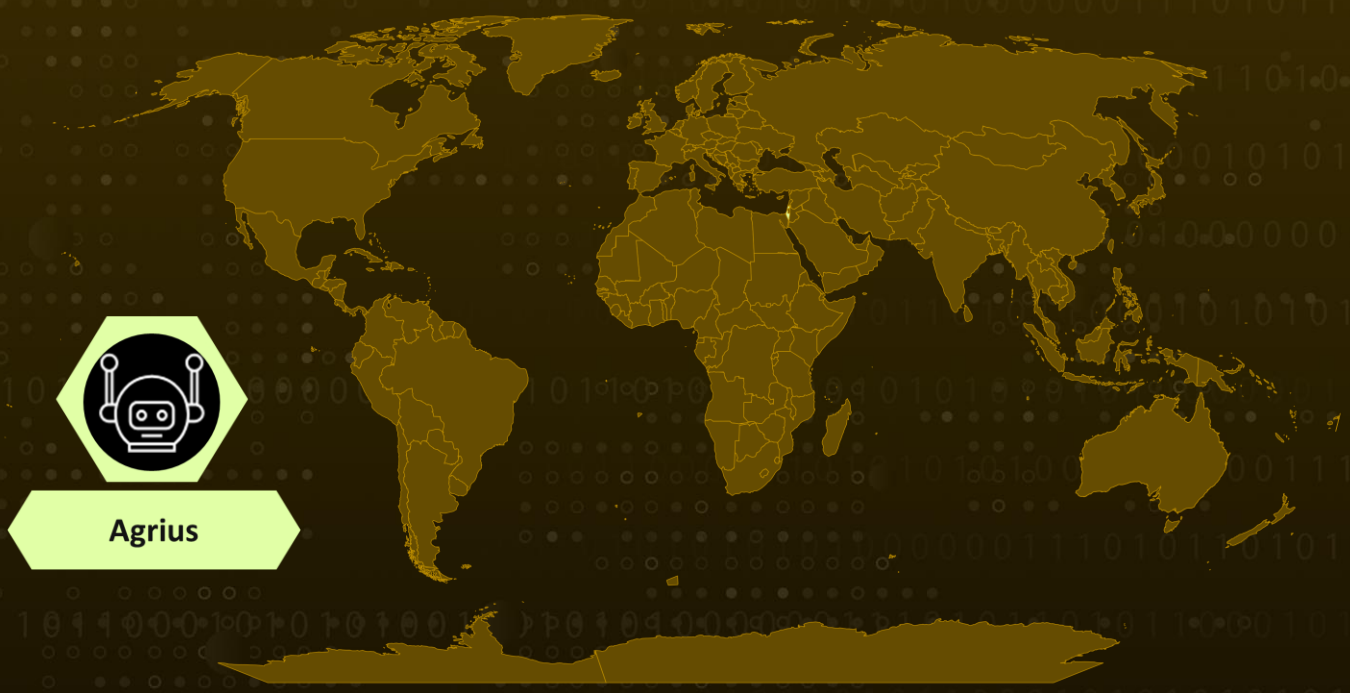
Iran-Backed Agrius APT's Attacks on Israeli Institutions

Date of Publication	Admiralty Code	TA Number
November 7, 2023	A1	TA2023449

Summary

Active Since: 2020
Threat Actor: Agrius (aka Agonizing Serpens, DEV-0227, BlackShadow, SharpBoys, AMERICIUM, Pink Sandstorm)
Malware: MultiLayer, PartialWasher, BFG Agonizer, sqlextractor
Attack Region: Israel
Targeted Industries: Education, Technology
Attack: In a series of harmful cyberattacks that occurred from January 2023 to October 2023, the Iranian-backed Advanced Persistent Threat (APT) group known as Agrius targeted Israel's education and technology sectors with the primary aim of obtaining highly sensitive data.

Attack Regions



Attack Details

#1 A series of destructive cyberattacks, masterminded by the Iranian-backed APT group known as Agrius, also operating under the alias "Agonizing Serpens," commenced in January 2023 and persisted until as recently as October 2023. These attacks were meticulously targeted at Israel's education and technology sectors, with the intent of pilfering highly sensitive data, including personally identifiable information (PII) and intellectual property.

#2 The Agrius APT group, established in 2020, has recently bolstered its capabilities, allocating significant efforts and resources to evade endpoint detection and response (EDR) systems and other security measures. Agrius initially gained access to the targeted environment by exploiting vulnerabilities in internet-facing web servers. Subsequently, they deployed numerous web shells, granting them an initial foothold within the network.

#3 This enabled them to conduct preliminary reconnaissance tasks using tools such as Nbtscan, WinEggDrop, and NimScan through these web shells. The attack strategy involved the acquisition of users' credentials with administrative privileges through techniques like Mimikatz, SMB password spraying, and SMB password brute force. Following this, they attempted to exfiltrate this data to their command and control (C2) servers, making use of publicly available tools like WinSCP and Putty.

#4 After pilfering the data, the attackers implemented various data-wiping mechanisms, designed to conceal their tracks and render the compromised endpoints inoperable. One of these data-wiping tools used by Agrius is a .NET-based malware called "MultiLayer," which includes two additional binaries in its resource section known as "MultiList" and "MultiWip," responsible for carrying out the actual file-wiping process.

#5 The MultiLayer malware shares multiple code similarities with previously employed custom tools, such as "Apostle," "IPsec Helper," and "Fantasy," all linked to the Agonizing Serpens group. In addition, they utilized a data-wiping tool known as "PartialWasher," coded in C++, as well as "BFG Agonizer," which displayed code similarities with an open-source project named "CRYLINE-v5.0," publicly hosted on GitHub.

Recommendations

Access Control: Implement strict access control and the principle of least privilege (PoLP) to limit access to critical systems, reducing the potential impact of malware if it gains access.

Strengthen Web Server Security: Regularly audit and patch vulnerabilities in internet-facing web servers to prevent initial access by attackers. Implement robust access control and authentication mechanisms to limit unauthorized access.

Network Segmentation: Segment your network into isolated zones to limit lateral movement for attackers and reduce the impact of a breach. Deploy network traffic analysis tools to monitor and analyze patterns of communication between endpoints and potential command and control servers

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery
TA0008 Lateral Movement	**TA0009** Collection	**TA0010** Exfiltration	**TA0040** Impact
T1595 Active Scanning	**T1190** Exploit Public-Facing Application	**T1003** OS Credential Dumping	**T1560** Archive Collected Data
T1490 Inhibit System Recovery	**T1574** Hijack Execution Flow	**T1059** Command and Scripting Interpreter	**T1110** Brute Force
T1005 Data from Local System	**T1041** Exfiltration Over C2 Channel	**T1485** Data Destruction	**T1561** Disk Wipe

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	E:\tools2\BFG agonizer\INFECTOR\Dropper\Dropper\Release\Dropper.pdb
File Name	bfg.exe, systems.txt
SHA256	1ea4d26a31dad637d697f9fb70b6ed4d75a13d101e02e02bc00200b42353985c, 62e36675ed7267536bd980c07570829fe61136e53de3336eebadeca56ab060c2, abfde7c29a4a703daa2b8ad2637819147de3a890fdd12da8279de51a3cc0d96d, 63d51bc3e5cf4068ff04bd3d665c101a003f1d6f52de7366f5a2d9ef5cc041a7, 49c3df62c4b62ce8960558daea4a8cf41b11c8f445e218cd257970cf939a3c25, dacdb4976fd75ab2fd7bb22f1b2f9d986f5d92c29555ce2b165c020e2816a200, e43d66b7a4fa09a0714c573fbe4996770d9d85e31912480e73344124017098f9, 2a6e3b6e42be2f55f7ab9db9d5790b0cc3f52bee9a1272fc4d79c7c0a3b6abda, 5d1660a53aaf824739d82f703ed580004980d377bdc2834f1041d512e4305d07, f4c8369e4de1f12cc5a71eb5586b38fc78a9d8db2b189b8c25ef17a572d4d6b7, 13d8d4f4fa483111e4372a6925d24e28f3be082a2ea8f44304384982bd692ec9, a8e63550b56178ae5198c9cc5b704a8be4c8505fea887792b6d911e488592a7c, a112e78e4f8b99b1ceddae44f34692be20ef971944b98e2def995c87d5ae89ee, 38e406b17715b1b52ed8d8e4defdb5b79a4ddea9a3381a9f2276b00449ec8835, f65880ef9fec17da4142850e5e7d40ebfc58671f5d66395809977dd5027a6a3e, ec7dc5bfadce28b8a8944fb267642c6f713e5b19a9983d7c6f011ebe0f663097, c52525cd7d05bddb3ee17eb1ad6b5d6670254252b28b18a1451f604dfff932a4, 8967c83411cd96b514252df092d8d3eda3f7f2c01b3eef1394901e27465ff981,

TYPE	VALUE
SHA256	a2d8704b5073cdc059e746d2016afbaecf8546daad3dbfe4833cd3d41ab63898, 18c909a2b8c5e16821d6ef908f56881aa0ecceeaccb5fa1e54995935fcfd12f7, 2fb88793f8571209c2fcf1be528ca1d59e7ac62e81e73ebb5a0d77b9d5a09cb8, 9165d4f3036919a96b86d24b64d75d692802c7513f2b3054b20be40c212240a5, 1ea4d26a31dad637d697f9fb70b6ed4d75a13d101e02e02bc00200b42353985c, 62e36675ed7267536bd980c07570829fe61136e53de3336eebadeca56ab060c2, abfde7c29a4a703daa2b8ad2637819147de3a890fdd12da8279de51a3cc0d96d
IPv4	185.105.46[.]34, 185.105.46[.]19, 93.188.207[.]110, 109.237.107[.]212, 217.29.62[.]166, 81.177.22[.]182

References

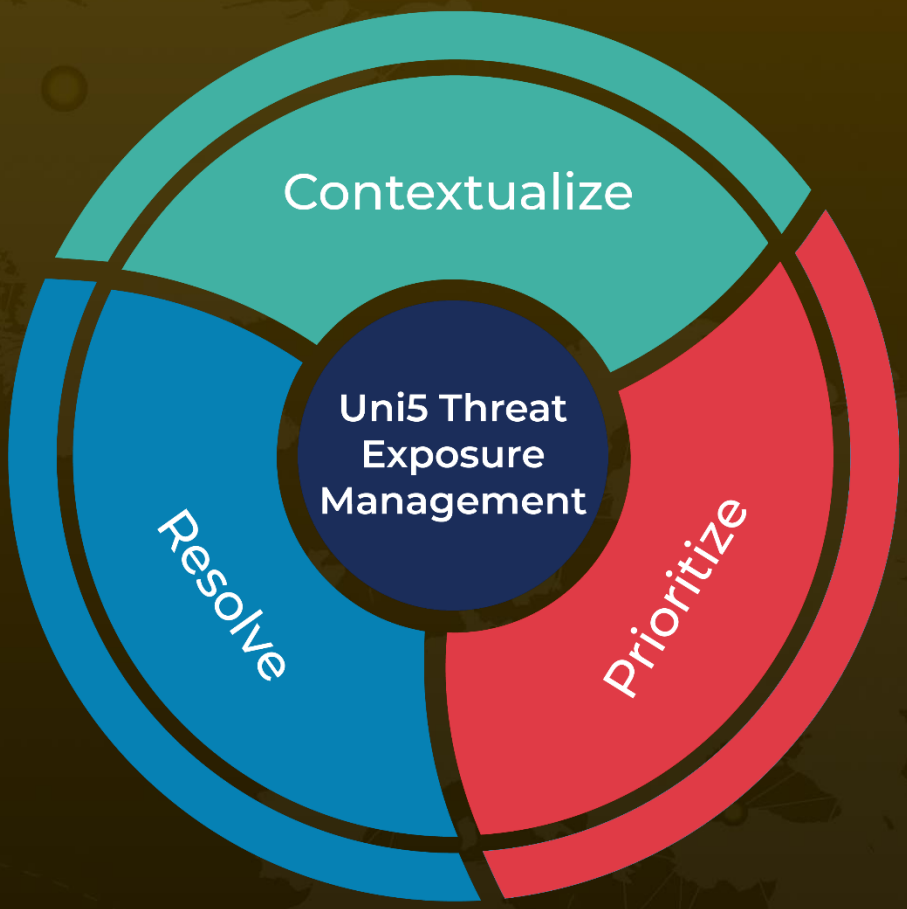
https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

https://www.hivepro.com/threat-advisory/iran-based-agrius-deploys-fantasy-wiper-to-attack-it-firms-in-israel/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 7, 2023 • 5:30 AM

More at www.hivepro.com