Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

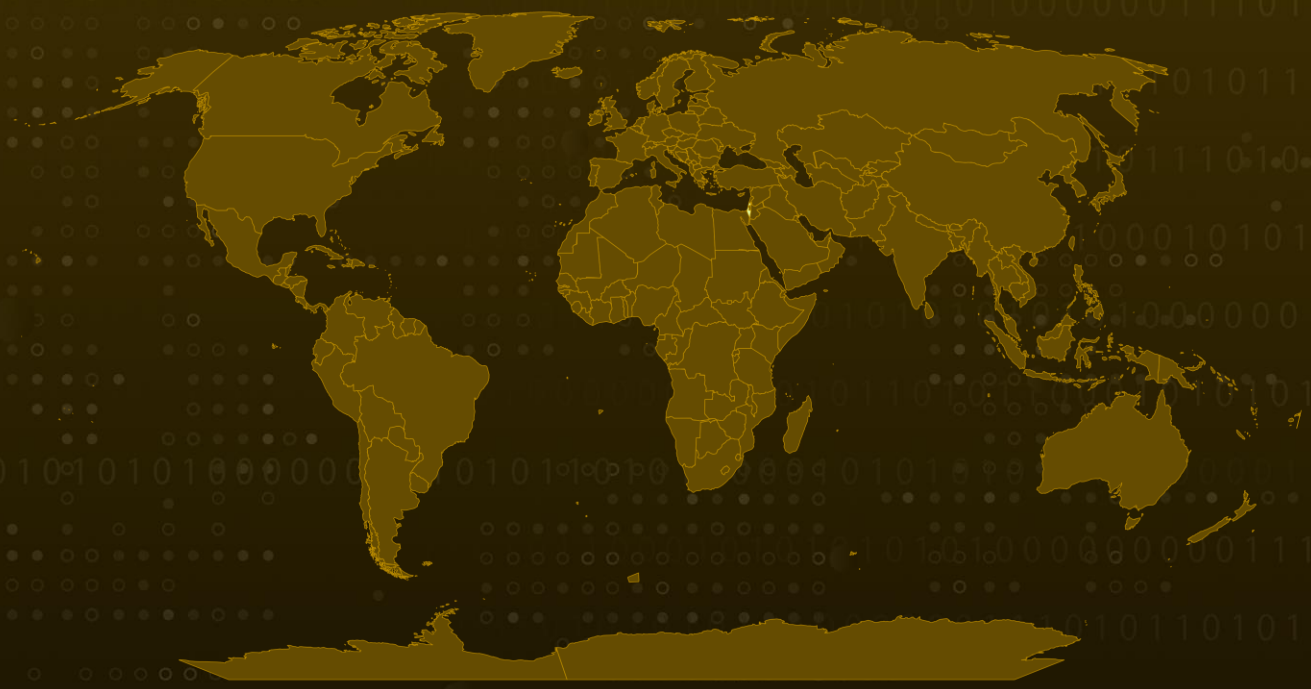
From Bullets to Bytes: The Hamas-Israel Conflict Goes Digital

Date of Publication	Admiralty Code	TA Number
October 31, 2023	A1	TA2023440

Summary

Attack Began: October 2023
Malware: BiBi-Linux
Attack Region: Israel, Palestine
Targeted Sectors: Defense, Government , Law Enforcement, and Political Parties
Attack: In the midst of the ongoing Israeli-Hamas conflict, a group of pro-Hamas hacktivists has emerged, utilizing a sophisticated Linux-based wiper malware known as BiBi-Linux Wiper. In the broader context of the Hamas-Israel conflict, various hacker groups have aligned themselves with either side, launching cyberattacks with the aim of sowing chaos and fear.

Attack Regions



Attack Details

#1 A group of pro-Hamas hacktivists has recently come to light, using a new Linux-based wiper malware known as BiBi-Linux Wiper. Their primary objective is to target Israeli entities during the ongoing Israeli-Hamas conflict. BiBi-Linux Wiper is an advanced x64 ELF executable, meticulously crafted in C/C++, with a file size of approximately 1.2MB.

#2 Notably, this binary was developed using the GCC compiler and lacks any form of obfuscation or protective measures. In the hands of attackers with root permissions, this malicious tool can be used to specify target directories, potentially causing havoc to an entire operating system. In the complex landscape of the Hamas-Israel conflict, various hacker groups are aligning themselves with either side, launching cyberattacks with the deliberate intention of creating chaos and instilling fear.

#3 Pro-Hamas hacking groups have been at the forefront of launching a barrage of DDoS attacks against both government and private Israeli websites. While these attacks have successfully caused temporary disruptions, they have not resulted in lasting damage. What sets this emerging threat apart from others is its reluctance to establish connections with remote Command and Control (C2) servers for data exfiltration.

#4 It also refrains from using reversible encryption algorithms or resorting to ransom notes as coercive tactics to extort payments. Its modus operandi is focused on file corruption, where existing files are overwritten with superfluous data, resulting in damage to both the data and the operational system. To expedite the infection process, this threat leverages multiple threads and utilizes a queue to synchronize their operations.

#5 This suggests that the threat actors prioritize maximizing the impact of their attacks over concerns about their tools being seized and subjected to scrutiny. The suspected Hamas-affiliated threat actor, who operates under the pseudonym Arid Viper (also known as APT-C-23, Desert Falcon, Gaza Cyber Gang, and Molerats), is believed to function as two distinct sub-groups.

#6 Each of these sub-groups is dedicated to engaging in cyber espionage activities targeting selected high-profile individuals of Israeli and Palestinian, backgrounds. The attack strategies orchestrated by this group involve the use of social engineering and phishing attacks as initial intrusion vectors. Subsequently, they deploy a diverse range of customized malware to conduct surveillance on their victims.

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.

Zero Trust Architecture: Consider implementing a Zero Trust security model, which assumes that threats may already exist within the network. Verify and authenticate all users and devices trying to connect to resources, regardless of whether they are inside or outside the network

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

TA0001 Initial Access	**TA0002** Execution	**TA0007** Discovery	**TA0008** Lateral Movement
TA0040 Impact	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.004** Unix Shell
T1072 Software Deployment Tools	**T1083** File and Directory Discovery	**T1082** System Information Discovery	**T1485** Data Destruction

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	23bae09b5699c2d5c4cb1b8aa908a3af898b00f88f06e021edcb16d7d558efad
SHA1	0dbabdc1ae8c3c8a48224ee3c3e8b6a17f41d6e7
MD5	de9da4fcfb8320b9d34239effce1871a
Domains	izocraft[.]com, cricket-live[.]net, sports-et-loisirs[.]net, leaf-japan[.]net, london-sport[.]net, anime-con[.]net, gsstar[.]net, lrxzklwmzxe[.]com, im-inter[.]net, acs-group[.]net, dslam[.]net, it-franch-result[.]info, delooyp[.]com, tophatauc[.]com, gmesc[.]com, seomoi[.]net, jasondixon[.]net

References

https://www.securityjoes.com/post/bibi-linux-a-new-wiper-dropped-by-pro-hamas-hacktivist-group

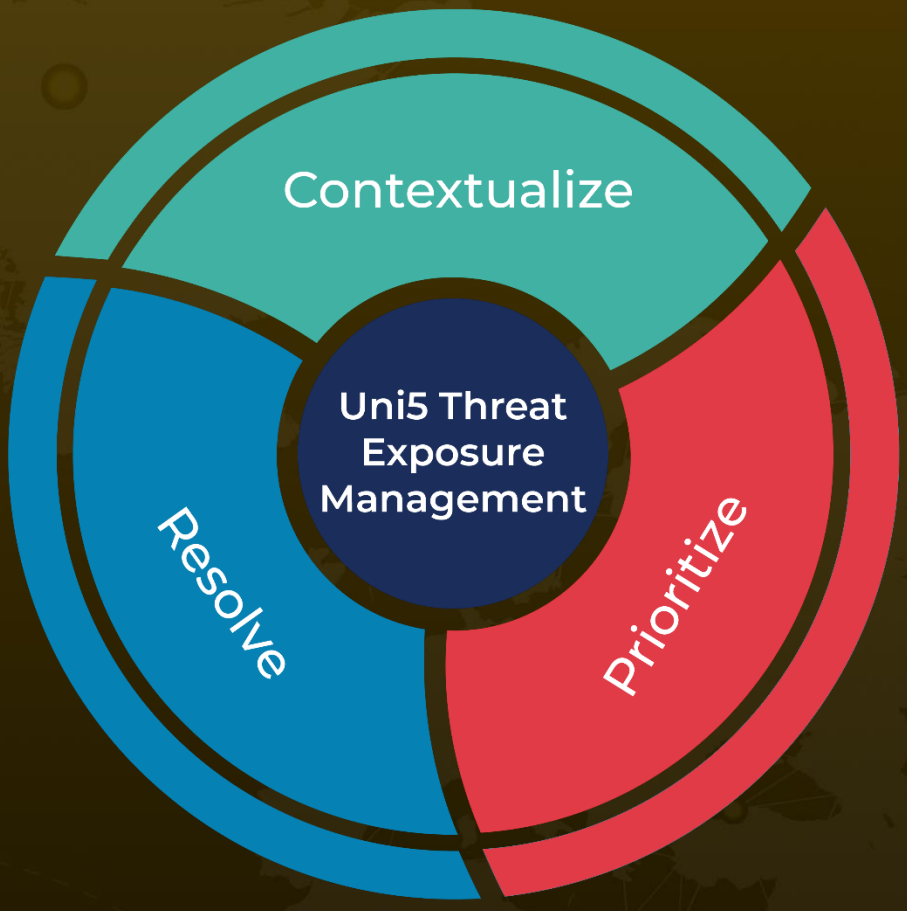
https://blog.checkpoint.com/security/evolving-cyber-dynamics-amidst-the-israel-hamas-conflict/

https://blog.sekoia.io/aridviper-an-intrusion-set-allegedly-associated-with-hamas/

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

October 31, 2023 • 4:30 AM

More at www.hivepro.com