Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

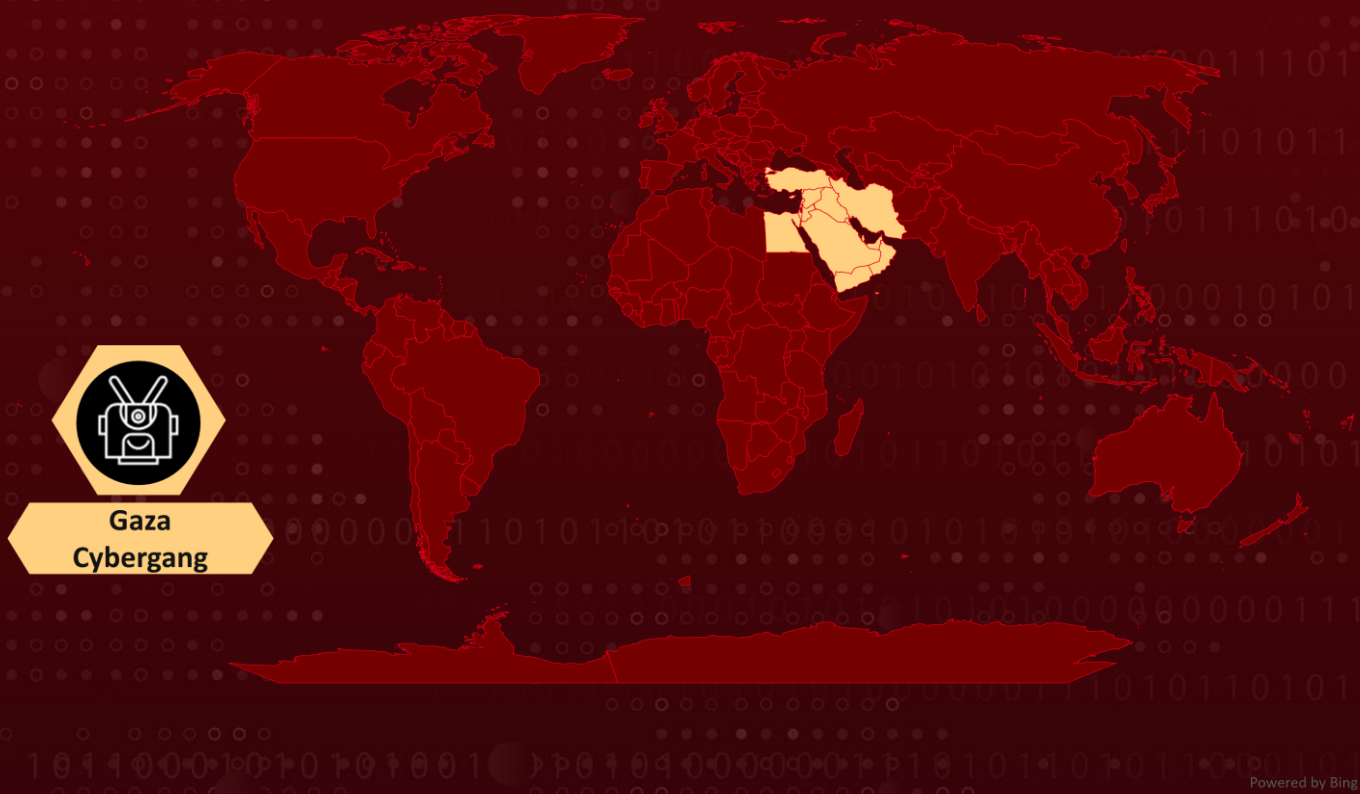
Gaza Cybergang's Pierogi++ Upgrade Takes Center Stage

Date of Publication	Admiralty Code	TA Number
December 18, 2023	A1	TA2023509

Summary

Attack Began: Late 2022 until late 2023
Threat Actor: Gaza Cybergang (aka TA402, Extreme Jackal, Molerats, Gaza Hackers Team, Aluminum Saratoga, ATK 89, TAG-CT5)
Malware: Pierogi++, Micropsia, and BarbWire
Attack Region: Middle East
Attack: The Gaza Cybergang, a sophisticated threat actor, has recently intensified its attacks by deploying an advanced version of the Pierogi backdoor malware. This group focuses its cyber operations primarily on Palestinian entities and Israel, with a historical record of targeting entities across the Middle East.

Attack Regions



Attack Details

#1 The Gaza Cybergang has deployed an iteration of the Pierogi backdoor malware, intensifying its attacks on targets primarily centered around Palestinian entities and Israel. This sophisticated threat actor has enhanced its arsenal by incorporating the Pierogi++ backdoor, initially introduced in 2022 and persistently observed in 2023.

#2 Operating since at least 2012, the Gaza Cybergang boasts a historical record of targeting entities across the Middle East, with a pronounced focus on Israel and Palestine. Their modus operandi frequently involves leveraging spear-phishing techniques to gain initial access. The malevolent actors disseminated the Pierogi++ malware through archive files and malicious Office documents discussing Palestinian subjects in both English and Arabic.

#3 These documents harbored Windows artifacts, housing malicious macros designed to propagate the Pierogi++ backdoor. This versatile malware is equipped to capture screenshots, execute commands, and download files as directed by the attackers. Under the Gaza Cybergang umbrella, activities spanning from late 2021 to late 2023 have encompassed diverse malware variants from the renowned Micropsia family.

#4 Furthermore, the group's operations have unveiled strategic linkages between two distinct campaigns known as Big Bang and Operation Bearded Barbie. Noteworthy malware families within their arsenal include BarbWire, DropBook, LastConn, Molerat Loader, NimbleMamba, SharpStage, Spark, Pierogi, PoisonIvy, and XtremeRAT.

#5 Persistently evolving, the Gaza Cybergang continues to augment its core malware arsenal by repurposing older implementations into new tools. The collusion of its constituent sub-groups, sharing Tactics, Techniques, and Procedures (TTPs), malware, and targets, underscores the unified front maintained by the Gaza Cybergang.

Recommendations

Enhance Network Security Measures: Strengthen network security protocols to guard against potential infiltrations by the Gaza Cybergang and related threat clusters. Employ robust firewalls, and intrusion detection systems, and regularly update security software to mitigate vulnerabilities.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**T1059** Command and Scripting Interpreter
T1083 File and Directory Discovery	**T1082** System Information Discovery	**T1204** User Execution	**T1598** Phishing for Information
T1566.001 Spearphishing Attachment	**T1105** Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1543** Create or Modify System Process
T1587 Develop Capabilities	**T1587.001** Malware		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	003bb055758a7d687f12b65fc802bac07368335e, 19026b6eb5c1c272d33bda3eab8197bec692abab, 20c10d0eff2ef68b637e22472f14d87a40c3c0bd, 26fe41799f66f51247095115f9f1ff5dcc56baf8, 278565e899cb48138cc0bbc482beee39e4247a5d, 2a45843cab0241cce3541781e4e19428dcf9d949, 32d0073b8297cc8350969fd4b844d80620e2273a, 3ae41f7a84ca750a774f777766ccf4fd38f7725a, 42cb16fc35cfc30995e5c6a63e32e2f9522c2a77, 4dcdb7095da34b3cef73ad721d27002c5f65f47b, 5128d0af7d700241f227dd3f546b4af0ee420bbc, 5619e476392c195ba318a5ff20e40212528729ba, 599cf23db2f4d3aa3e19d28c40b3605772582cae, 5e46151df994b7b71f58556c84eeb90de0776609, 5fcc262197fe8e0f129acab79fd28d32b30021d7, 60480323f0e6efa3ec08282650106820b1f35d2f,

TYPE	VALUE
SHA1	694fa6436302d55c544cfb4bc9f853d3b29888ef, 708f05d39df7e47aefc4b15cb2db9f26bc9fad5f, 745657b4902a451c72b4aab6cf00d05895bbc02f, 75a63321938463b8416d500b34a73ce543a9d54d, 95fc3fb692874f7415203a819543b1e0dd495a57, 994ebbe444183e0d67b13f91d75b0f9bcfb011db, aeeeee47becaa646789c5ee6df2a6e18f1d25228, c3038d7b01813b365fd9c5fd98cd67053ed22371, da96a8c04edf8c39d9f9a98381d0d549d1a887e8, ee899ae5de50fdee657e04ccd65d76da7ede7c6f, f3e99ec389e6108e8fda6896fa28a4d7237995be
Domains	aracaravan[.]com, beatricewarner[.]com, bruce-ess[.]com, claire-conway[.]com, delooyp[.]com, escanor[.]live, izocraft[.]com, jane-chapman[.]com, lindamullins[.]info, nicoledotson[.]icu, overingtonray[.]info, porthopeminorhockey[.]net, spgbotup[.]club, stgeorgebankers[.]com, swsan-lina-soso[.]info, theconomics[.]net, wanda-bell[.]website, wayne-lashley[.]com, zakaria-chotzen[.]info

References

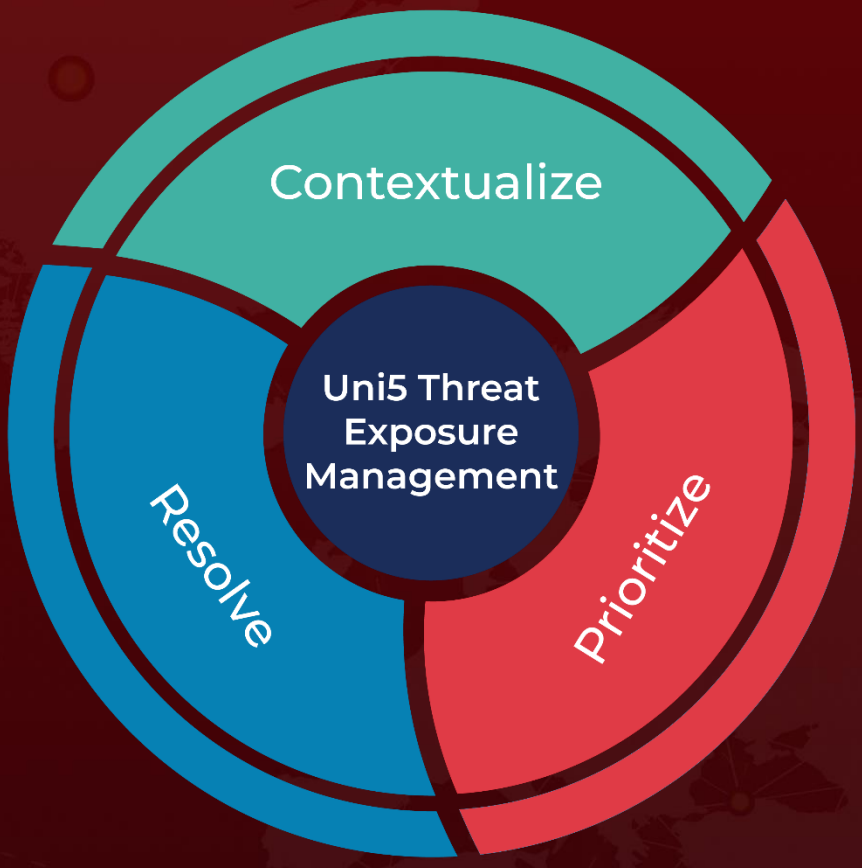
https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/

https://www.hivepro.com/threat-advisory/ta402s-covert-operation-aims-middle-east/

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

December 18, 2023 . 4:30 AM

More at www.hivepro.com