Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

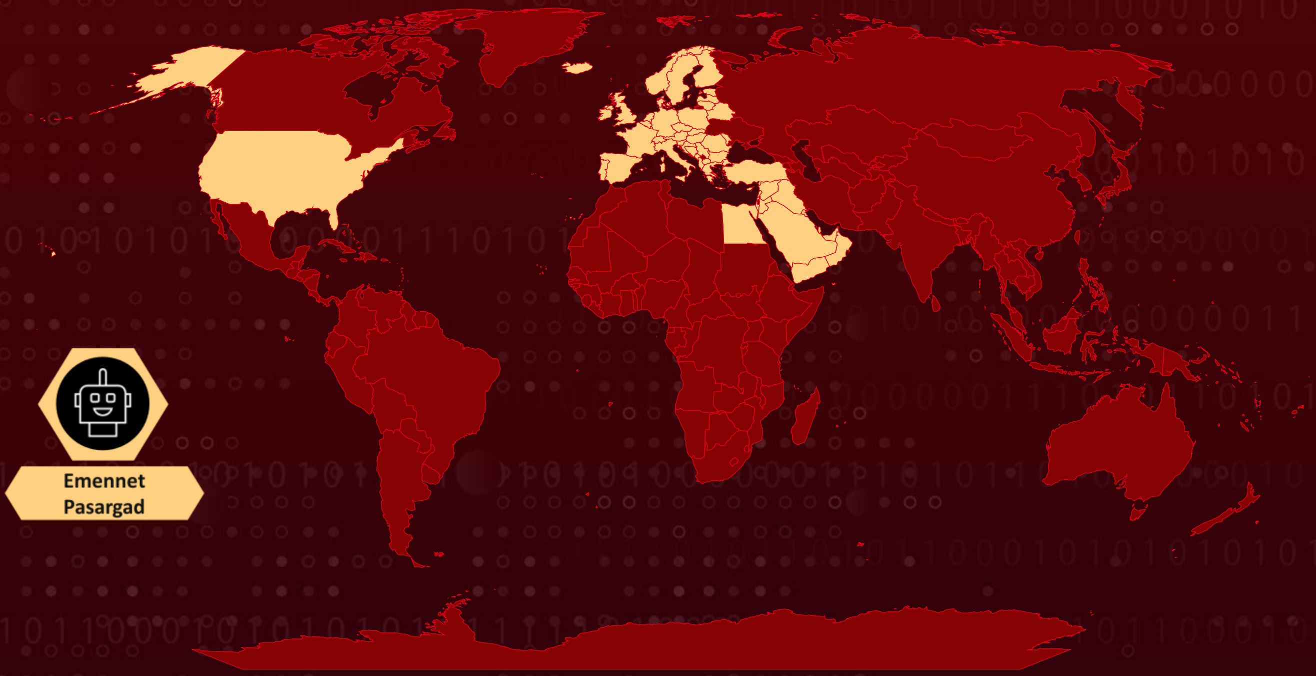
Hack, Leak, Repeat – Emennet Pasargad’s Quest to Destabilize Israel

Date of Publication	Admiralty code	TA Number
November 7, 2024	A1	TA2024420

Summary

Active Since: 2020
Threat Actor: Emennet Pasargad (aka Holy Souls, Vice Leaker, Haywire Kitten, Neptunium, Cotton Sandstorm, DEV-0198, Yellow Dev 19, Magic Kitten, Black Magic, ViceLeaker, kalin3t, Eeleyanet Gostar, EeleyanetGostar, Net Peygard Samavat, Hackers of Savior, Deus, Group 42, Voyeur, MARNANBRIDGE)
Attack Countries: Israel, Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen, Germany, United Kingdom, France, Italy, Spain, Poland, Romania, Netherlands, Belgium, Czech Republic, Sweden, Portugal, Greece, Hungary, Austria, Belarus, Switzerland, Bulgaria, Serbia, Denmark, Finland, Norway, Slovakia, Ireland, Croatia, Bosnia and Herzegovina, Moldova, Lithuania, Albania, Slovenia, Latvia, North Macedonia, Estonia, Luxembourg, Montenegro, Malta, Iceland, Andorra, Liechtenstein, Monaco, San Marino, Holy See, United States, Isle of Man, Faeroe Islands
Targeted Industries: Government, Energy, Financial, High Tech, NGOs, Civil Society, Shipping, Transportation, Political, Military, Airline, Manufacturing, Media, Travel, Hotels, Airlines, Oil, Petrochemical, Telecommunications

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Actor Details

#1

The Iranian cyber group Emennet Pasargad, operating under the corporate name Aria Sepehr Ayandehsazan (ASA) since mid-2024 also known as Cotton Sandstorm, Marnanbridge, and Haywire Kitten has a legally registered presence in Iran, ostensibly for financial and HR purposes.

#2

Emennet Pasargad's cyber operations have pursued four main objectives: destabilization, retaliation, intimidation, and undermining international support for Israel. Collectively, these goals aim to erode confidence in Israel's information ecosystem and spread confusion. In mid-2023, Emennet Pasargad reportedly began using multiple front hosting providers to manage its infrastructure and increase operational concealment.

#3

Rather than relying solely on third-party hosting resellers, the group established its network of resellers, sourcing server space from European providers, including entities in Lithuania, the United Kingdom, and Moldova. This network enables the group to deploy servers for various cyber activities and provide technical support to Lebanon-based individuals, including hosting services for regionally affiliated websites.

#4

By mid-2024, Emennet Pasargad had expanded its cyber-enabled information operations, leveraged a range of cover personas and targeted major events, such as the 2024 Summer Olympics, where they reportedly compromised a French commercial display provider. Additionally, the group has undertaken projects to collect video content from IP cameras and explore online AI resources.

#5

Focused on hack-and-leak campaigns, Emennet Pasargad has targeted organizations primarily in Israel but has also impacted entities in France, Sweden, and the U.S. Their reconnaissance includes using online datasets for research on individual and organizational targets, as well as open-source intelligence tools like Shodan, IP2Location, and Subdomain Finder. For access and exploitation, they employ commercial tools like Masscan, Acunetix, Burp Suite, and SQLMap.

#6

The group has used automated password-guessing techniques and various online resources for hash cracking. Their exploitation toolkit includes software for endpoint data collection and remote command execution. Emennet Pasargad has also deployed a modified Google Chrome Installer MSI file that, while appearing to install Chrome, executes an additional file, bd.exe. This obfuscated remote access trojan (RAT), built under the project name "bd," gathers system data and connects to a designated server when supplied with a de-obfuscation key.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Emennet Pasargad (aka Holy Souls, Vice Leaker, Haywire Kitten, Neptunium, Cotton Sandstorm, DEV-0198, Yellow Dev 19, Magic Kitten, Black Magic, ViceLeaker, kalin3t, Eeleyanet Gostar, EeleyanetGostar, Net Peygard Samavat, Hackers of Savior, Deus, Group 42, Voyeur, MARNANBRIDGE)	Iran	Israel, Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen, Germany, United Kingdom, France, Italy, Spain, Poland, Romania, Netherlands, Belgium, Czech Republic, Sweden, Portugal, Greece, Hungary, Austria, Belarus, Switzerland, Bulgaria, Serbia, Denmark, Finland, Norway, Slovakia, Ireland, Croatia, Bosnia and Herzegovina, Moldova, Lithuania, Albania, Slovenia, Latvia, North Macedonia, Estonia, Luxembourg, Montenegro, Malta, Iceland, Andorra, Liechtenstein, Monaco, San Marino, Holy See, United States, Isle of Man, Faeroe Islands	Government, Energy, Financial, High Tech, NGOs, Civil Society, Shipping, Transportation, Political, Military, Airline, Manufacturing, Media, Travel, Hotels, Airlines, Oil, Petrochemical, Telecommunications
	MOTIVE		
	Information Operations, Espionage, Financial Gains		

Recommendations

Patch and Update Vulnerable Software: Regularly update and patch all software and systems, particularly addressing known vulnerabilities. Ensure your software remains up to date by regularly checking for and applying the latest security updates and patches from the vendor patches can help prevent exploitation by threat actors like Emennet Pasargad.

Enable Network Segmentation and Access Control: Segment critical infrastructure and sensitive data from general user networks. Use access control lists (ACLs) to restrict traffic flow between network segments, reducing the risk of lateral movement in case of a breach.

Implement Application Whitelisting: Use application whitelisting to allow only pre-approved applications to execute on critical systems. This can prevent unauthorized or malicious software from running, minimizing the risk of malware infection.

Deploy Secure Configuration Baselines and Continuous Monitoring: Establish secure configuration baselines for all systems, especially internet-facing services. Use continuous monitoring to enforce these configurations and alert on any deviations from established security settings.

Implement Robust Data Loss Prevention (DLP) Controls: Deploy DLP solutions to monitor, control, and prevent unauthorized data exfiltration. Configure DLP policies to restrict sensitive data transfer, especially over email and cloud storage, and monitor for unusual data movement.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0006 Credential Access
TA0011 Command and Control	T1596 Search Open Technical Databases	T1589 Gather Victim Identity Information	T1589.002 Email Addresses
T1589.003 Employee Names	T1591.001 Determine Physical Locations	T1595.002 Vulnerability Scanning	T1590.001 Domain Properties
T1595.001 Scanning IP Blocks	T1596 Search Open Technical Databases	T1650 Acquire Access	T1583 Acquire Infrastructure
T1587 Develop Capabilities	T1190 Exploit Public-Facing Application	T1110.001 Password Guessing	T1110.002 Password Cracking
T1071.001 Web Protocols	T1219 Remote Access Software		

Indicator of Compromise (IOCs)

TYPE	VALUE
Domains	onlinelive[.]info, zeusistalking[.]io, zeusistalking[.]net, zeusistalking[.]com, rgud-group[.]net, rgud-group[.]com, cyberflood[.]io, cybercourt[.]io, pro-today[.]org, il-cert[.]net
File Name	First.exe
SHA256	4431b2a4d7758907f81fb1a0c1e36b2ce03e08d43123b1c398487770afd20727, 6f765dda126e830c6cd2c7938dbb970d03be728e82c00388903a4ef3f9ecc853
IPv4	5[.]230[.]56[.]148, 77[.]91[.]74[.]158, 195[.]26[.]87[.]80, 213[.]109[.]147[.]97, 185[.]110[.]188[.]112, 45[.]140[.]146[.]139, 45[.]84[.]0[.]237, 45[.]140[.]146[.]197, 45[.]140[.]146[.]137, 45[.]84[.]0[.]254, 45[.]142[.]212[.]21, 45[.]140[.]146[.]108, 45[.]140[.]146[.]208, 213[.]109[.]147[.]63, 146[.]19[.]254[.]61, 31[.]42[.]177[.]114, 45[.]143[.]167[.]87, 45[.]143[.]166[.]233
IP Range	85[.]206[.]170[.]160 - 85[.]206[.]170[.]191, 85[.]206[.]167[.]224 - 85[.]206[.]167[.]255, 85[.]206[.]169[.]64 - 85[.]206[.]169[.]79, 85[.]206[.]169[.]80 - 85[.]206[.]169[.]95

CVEs

The Emennet Pasargad threat actor strategically leveraged the following vulnerabilities to broaden its impact and target victims via compromised devices. For quick access, patch links for each exploited CVE are hyperlinked via the checkmarks labeled under ‘Patch Link.’

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH LINK
CVE-2019-9546	SolarWinds Orion Privilege Escalation Vulnerability	SolarWinds Orion Platform before 2018.4 Hotfix 2	✗	✗	✓
CVE-2009-1151	phpMyAdmin Remote Code Execution Vulnerability	phpMyAdmin	✗	✓	✓
CVE-2014-0160	Heartbleed (OpenSSL Information Disclosure Vulnerability)	OpenSSL	✓	✓	✓
CVE-2016-10033	PHPMailer Remote Code Execution Vulnerability	PHPMailer before 5.2.18	✗	✗	✓
CVE-2017-0213	Microsoft Windows Privilege Escalation Vulnerability	Microsoft Windows	✗	✓	✓
CVE-2017-14723	WordPress SQL Injection Vulnerability	WordPress Before version 4.8.2	✗	✗	✓
CVE-2017-14726	WordPress Cross-site Scripting Vulnerability	WordPress Before version 4.8.2	✗	✗	✓
CVE-2017-5611	WordPress SQL Injection Vulnerability	WordPress before 4.7.2	✗	✗	✓
CVE-2017-5930	PostfixAdmin authenticated Remote Command Execution Vulnerability	PostfixAdmin before 3.0.2	✗	✗	✓
CVE-2017-5963	Caddy Cross-Site Scripting (XSS) Vulnerability	Caddy before 7.2.10	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH LINK
CVE-2017-8295	WordPress Security Bypass Vulnerability	WordPress versions up to the latest 4.7.4	✗	✗	✓
CVE-2018-1000001	Linux Buffer Underflow Vulnerability	glibc 2.26 and earlier	✗	✗	✓
CVE-2018-7600	Drupal Core Remote Code Execution Vulnerability	Drupal Core	✗	✓	✓
CVE-2018-8639	Win32k Elevation of Privilege Vulnerability	Microsoft Windows	✗	✗	✓
CVE-2019-0044	Juniper Denial of Service (DoS) Vulnerability	Juniper Networks SRX5000 Series	✗	✗	✓
CVE-2019-0232	Apache Tomcat Remote Code Execution Vulnerability	Apache Tomcat CGI Servlet	✗	✗	✓
CVE-2019-0708	Microsoft Remote Desktop Services Remote Code Execution Vulnerability	Microsoft Remote Desktop Services	✗	✓	✓
CVE-2019-9621	Zimbra Server-Side Request Forgery (SSRF) Vulnerability	Zimbra Collaboration Suite	✗	✗	✓

References

https://www.ic3.gov/CSA/2024/241030.pdf

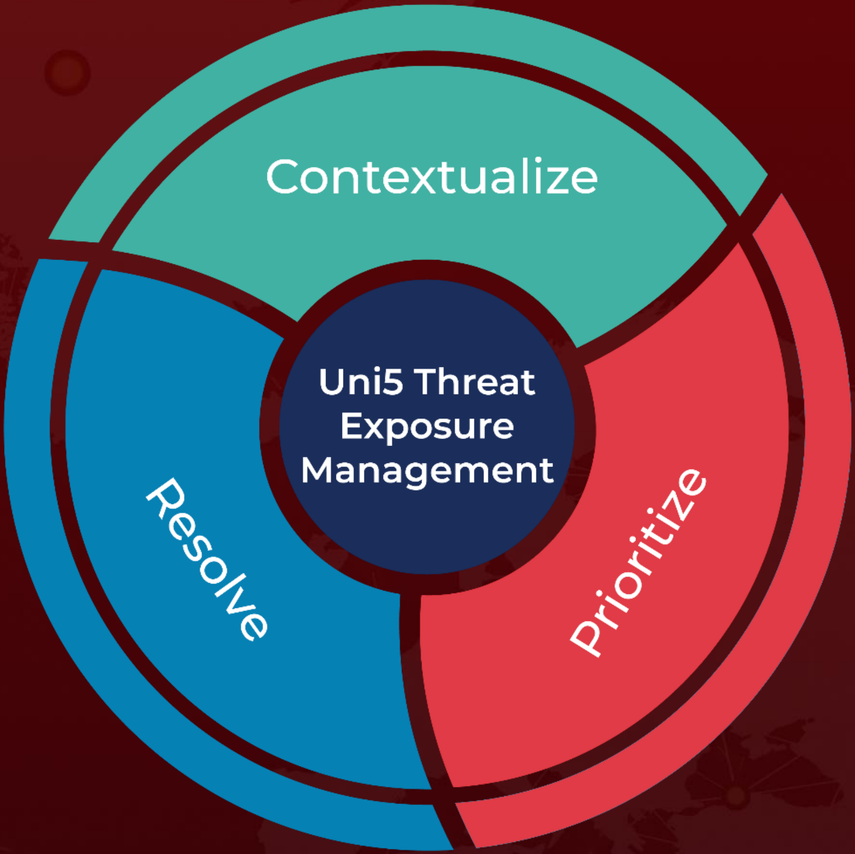
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas

https://www.ic3.gov/CSA/2022/220126.pdf

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, 2024 • 9:30 PM

More at www.hivepro.com