Hive Pro

Threat Level

Red

CISA: AA24-290A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

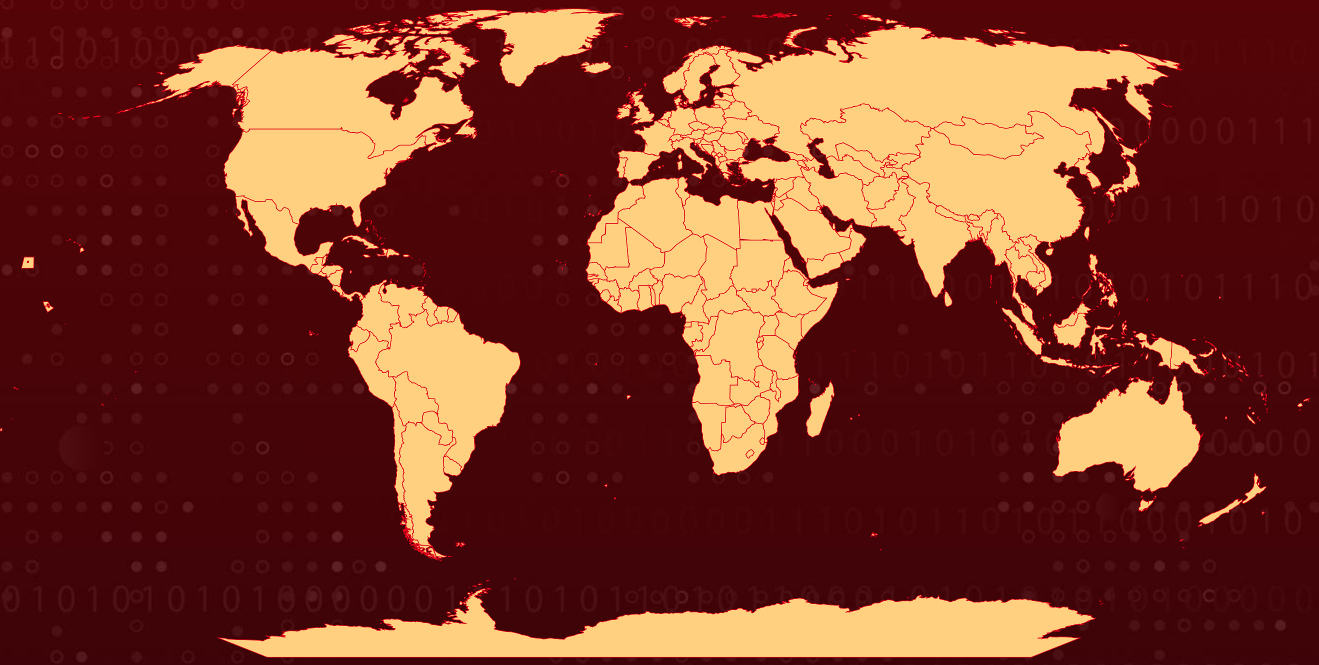
Iranian Cyber Actors Target Critical Infrastructure

Date of Publication	Admiralty Code	TA Number
October 18, 2024	A1	TA2024402

Summary

Attack Began: October 2023
Threat Actors: Iranian Threat Actors
Targeted Industries: Healthcare, government, information technology, engineering, and energy
Targeted Region: Worldwide
Affected Products: Microsoft 365, Azure, and Citrix
Attack: Iranian cyber actors have been targeting critical infrastructure sectors, such as healthcare, government, and energy, using brute force attacks like password spraying and MFA "push bombing" to gain access. They modify MFA registrations to maintain persistent access and conduct network reconnaissance to steal additional credentials. Their methods include exploiting vulnerabilities like Zerologon and using VPNs to mask their activities. The stolen credentials are often sold to cybercriminals, posing a serious threat to organizations.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-1472	ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)	Microsoft Netlogon	✗	✓	✓

Attack Details

#1

Iranian cyber actors have been actively targeting critical infrastructure organizations in the U.S. and allied countries, using a combination of brute force and credential access techniques to compromise systems and networks. The affected sectors include healthcare, government, energy, and information technology, among others. Since October 2023, these actors have employed brute force methods, such as password spraying, to gain unauthorized access to accounts, which are then exploited for further malicious activity.

#2

One of their key tactics is manipulating multi-factor authentication (MFA) through a technique called "push bombing", where legitimate users are overwhelmed with repeated MFA requests until they accidentally approve access. Once the attackers compromise accounts, they frequently modify MFA registrations, allowing them to register their own devices and maintain long-term persistent access to the network. The compromised credentials are often sold to other cybercriminals, enabling additional malicious operations.

#3

After gaining initial access, these actors perform network reconnaissance to gather more credentials and move laterally through the network. Their typical targets include Microsoft 365, Azure, and Citrix systems, and they use virtual private networks (VPNs) to conceal their activities, making it harder for defenders to detect their unauthorized presence.

#4

To deepen their infiltration, the attackers use techniques such as Kerberos ticket harvesting and open-source tools like DomainPasswordSpray for further credential theft. They also leverage Active Directory dumps and Kerberos SPN enumeration to extract sensitive user and system information. These efforts allow the attackers to escalate privileges within the compromised environment.

#5

A critical aspect of their operations includes exploiting vulnerabilities, such as CVE-2020-1472 (Zerologon), which enables them to impersonate domain controllers. They also employ living-off-the-land (LOTL) techniques, utilizing built-in Windows tools to gather intelligence on domain controllers, trusted domains, and administrative accounts. The overarching aim of these attacks is to disrupt essential services, steal valuable data, and sell access for further criminal activities, posing a significant threat to organizations.

Recommendations

Implement Strong Password Policies: Enforce the use of complex passwords that include a mix of upper and lower case letters, numbers, and special characters. Regularly update passwords and ensure that they are not reused across different accounts.

Enable Multi-Factor Authentication (MFA): Require MFA for all user accounts, particularly those with access to sensitive systems and data. Educate users on recognizing and responding to MFA requests to avoid falling victim to push bombing attacks.

Monitor Authentication Logs: Regularly review authentication logs for failed login attempts, suspicious login patterns, and unusual account activities. Set up alerts for multiple failed login attempts and "impossible travel" scenarios where logins occur from distant geographic locations within a short timeframe.

Regularly Update Software and Systems: Ensure that all software, applications, and operating systems are up-to-date with the latest security patches. Perform regular vulnerability assessments to identify and remediate weaknesses in the system.

Limit Access Privileges: Grant users the minimum level of access necessary for their roles to reduce the potential impact of a compromised account. Periodically review user access rights and adjust them as needed based on role changes or departures.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control

T1589 Gather Victim Identity Information	T1588 Obtain Capabilities	T1588.002 Tool	T1078 Valid Accounts
T1078.004 Cloud Accounts	T1133 External Remote Services	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1098 Account Manipulation	T1098.005 Device Registration	T1556 Modify Authentication Process	T1556.006 Multi-Factor Authentication
T1068 Exploitation for Privilege Escalation	T1484 Domain or Tenant Policy Modification	T1484.002 Trust Modification	T1202 Indirect Command Execution
T1110 Brute Force	T1110.003 Password Spraying	T1555 Credentials from Password Stores	T1558 Steal or Forge Kerberos Tickets
T1558.003 Kerberoasting	T1621 Multi-Factor Authentication Request Generation	T1018 Remote System Discovery	T1069 Permission Groups Discovery
T1069.002 Domain Groups	T1069.003 Cloud Groups	T1082 System Information Discovery	T1087 Account Discovery
T1087.002 Domain Account	T1482 Domain Trust Discovery	T1021 Remote Services	T1021.001 Remote Desktop Protocol
T1005 Data from Local System	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1105 Ingress Tool Transfer
T1572 Protocol Tunneling			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	1F96D15B26416B2C7043EE7172357AF3AFBB002A, 3D3CDF7CFC881678FEBCAFB26AE423FE5AA4EFEC

TYPE	VALUE
IPv4	95[.]181[.]234[.]12, 95[.]181[.]234[.]25, 173[.]239[.]232[.]20, 172[.]98[.]71[.]191, 102[.]129[.]235[.]127, 188[.]126[.]94[.]60, 149[.]40[.]50[.]45, 181[.]214[.]166[.]59, 212[.]102[.]39[.]212, 149[.]57[.]16[.]134, 149[.]57[.]16[.]137, 102[.]129[.]235[.]186, 46[.]246[.]8[.]138, 149[.]57[.]16[.]160, 149[.]57[.]16[.]37, 46[.]246[.]8[.]137, 212[.]102[.]57[.]29, 46[.]246[.]8[.]82, 95[.]181[.]234[.]15, 45[.]88[.]97[.]225, 84[.]239[.]45[.]17, 46[.]246[.]8[.]104, 37[.]46[.]113[.]206, 46[.]246[.]3[.]186, 46[.]246[.]8[.]141, 46[.]246[.]8[.]17, 37[.]19[.]197[.]182, 154[.]16[.]192[.]38, 102[.]165[.]16[.]127, 46[.]246[.]8[.]47, 46[.]246[.]3[.]225, 46[.]246[.]3[.]226, 46[.]246[.]3[.]240, 191[.]101[.]217[.]10, 102[.]129[.]153[.]182, 46[.]246[.]3[.]196, 102[.]129[.]152[.]60, 156[.]146[.]60[.]74, 191[.]96[.]227[.]113, 191[.]96[.]227[.]122, 181[.]214[.]166[.]132, 188[.]126[.]94[.]57, 154[.]6[.]13[.]144,

TYPE	VALUE
IPv4	154[.]6[.]13[.]151, 188[.]126[.]94[.]166, 89[.]149[.]38[.]204, 46[.]246[.]8[.]67, 46[.]246[.]8[.]53, 154[.]16[.]192[.]37, 191[.]96[.]150[.]14, 191[.]96[.]150[.]96, 46[.]246[.]8[.]10, 84[.]239[.]25[.]13, 154[.]6[.]13[.]139, 191[.]96[.]106[.]33, 191[.]96[.]227[.]159, 149[.]57[.]16[.]150, 191[.]96[.]150[.]21, 46[.]246[.]8[.]84, 95[.]181[.]235[.]8, 191[.]96[.]227[.]102, 46[.]246[.]122[.]185, 146[.]70[.]102[.]3, 46[.]246[.]3[.]233, 46[.]246[.]3[.]239, 188[.]126[.]89[.]35, 46[.]246[.]3[.]223, 46[.]246[.]3[.]245, 191[.]96[.]150[.]50,

Patch Link

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

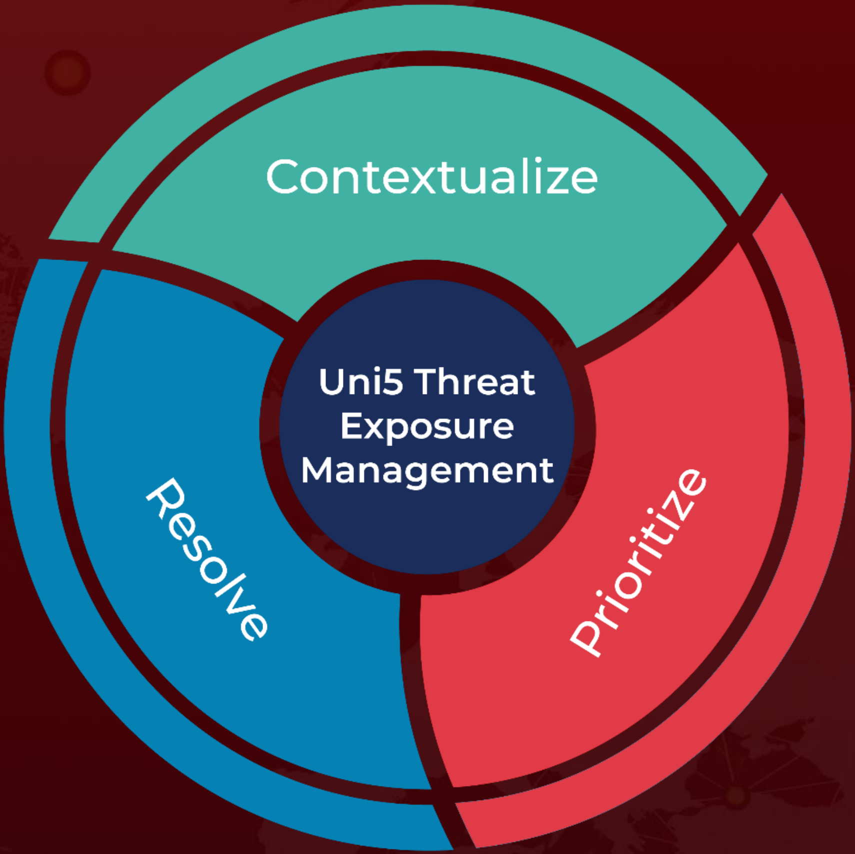
References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a

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 18, 2024 • 7:30 AM

More at www.hivepro.com