Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

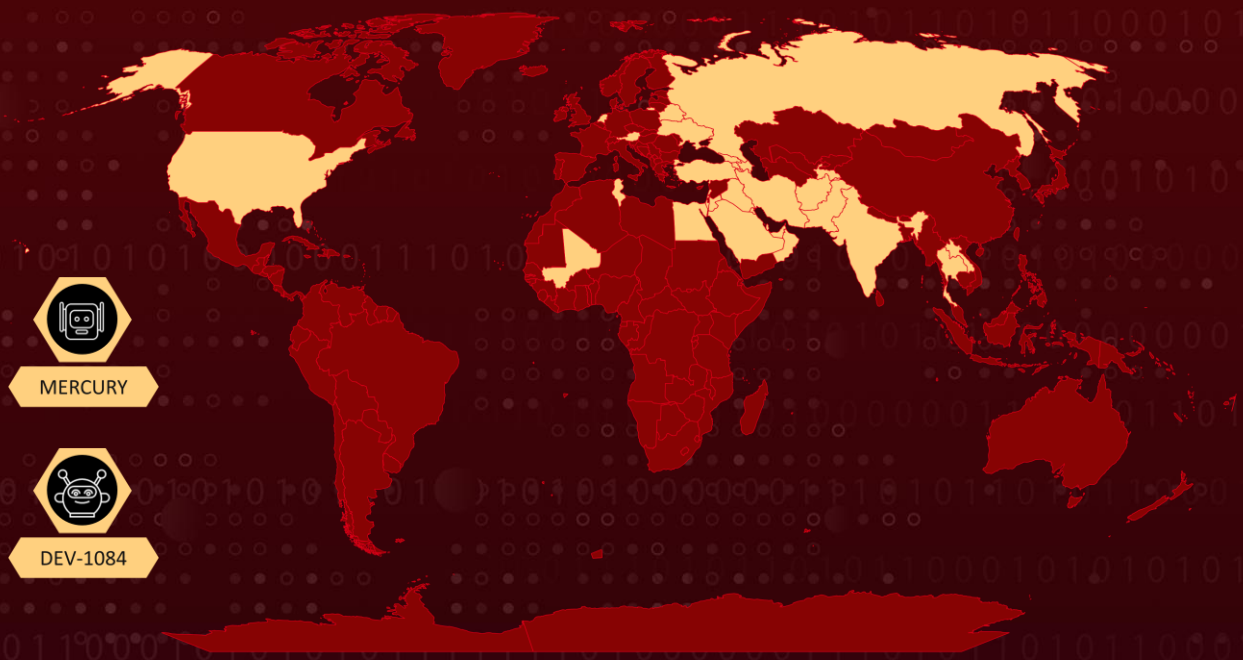
Nation-State Actors MERCURY and Partner DEV-1084 Carry Out Destructive Attack

Date of Publication	Admiralty Code	TA Number
April 13, 2023	A1	TA2023182

Summary

Attack began: July 2022
Threat Actor: **MERCURY** (MuddyWater, Seedworm, TEMP.Zagros, Static Kitten, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17) & **DEV-1084**
Attack Countries: Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Qatar, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkey, UAE, Ukraine, USA
Attack Industry: Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation
Attack: MERCURY, a nation-state actor linked to the Iranian government, worked with another actor, DEV-1084, to carry out a destructive attack targeting both on-premises and cloud environments, using various techniques to maintain persistence and evade detection.

Attack Regions



Attack Details

#1 MERCURY, a nation-state actor with ties to the Iranian government, carried out a destructive campaign that targeted both on-premises and cloud environments. Although the attack was disguised as a ransomware campaign, the real aim was destruction and disruption. MERCURY is believed to have worked together with another actor, DEV-1084, to carry out the attack. It is believed that the attackers gained initial access by exploiting vulnerabilities in unpatched applications. Once inside, the attackers used multiple tools and techniques to maintain their presence and carry out extensive reconnaissance.

#2 They also used highly privileged credentials to cause mass destruction of resources, such as server farms, virtual machines, storage accounts, and virtual networks. Additionally, they sent emails to both internal and external recipients. To evade detection, the attackers used several command-and-control servers and tunnelling tools. They interfered with security tools by using Group Policy Objects and staged the ransomware payload in NETLOGON shares on several domain controllers. Then, they encrypted files on targeted devices and left ransom notes. In order to move from on-premises to the cloud, the attackers compromised two privileged accounts, which they then used to manipulate the Azure Active Directory Connect agent.

Recommendations

- For on-premises environments, it is recommended to prioritize building strong credential hygiene and implementing robust measures to defend against ransomware and human-operated attacks. Enable tamper protection for Endpoint as it prevents malicious apps and actors from tampering or misconfiguring antivirus.
- For Azure AD environments, enabling Conditional Access policies, continuous access evaluation, and searching unified audit logs for the SendAs operation are crucial measures to protect against stolen credentials and other risks. Additionally, referring to Azure Identity Management and access control security best practices can provide further recommendations to secure the environment.
- Block the indicators of compromise related to the attack campaign.

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	TA0011 Command and Control	T1083 File and Directory Discovery	T1190 Exploit Public-Facing Application
T1505 Server Software Component	T1505.003 Web Shell	T1546 Event Triggered Execution	T1546.013 PowerShell Profile
T1518 Software Discovery	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1589 Gather Victim Identity Information
T1589.001 Credentials	T1590 Gather Victim Network Information	T1484 Domain Policy Modification	T1484.001 Group Policy Modification
T1047 Windows Management Instrumentation	T1136 Create Account	T1136.001 Local Account	T1548 Abuse Elevation Control Mechanism
T1548.004 Elevated Execution with Prompt	T1070 Indicator Removal	T1070.004 File Deletion	T1578 Modify Cloud Compute Infrastructure
T1578.003 Delete Cloud Instance	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1572 Protocol Tunneling
T1210 Exploitation of Remote Services	T1003 OS Credential Dumping	T1078 Valid Accounts	T1543 Create or Modify System Process
T1543.003 Windows Service	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1059 Command and Scripting Interpreter
T1046 Network Service Discovery	T1069 Permission Groups Discovery	T1018 Remote System Discovery	T1057 Process Discovery

T1082 System Information Discovery	T1021 Remote Services	T1021.002 SMB/Windows Admin Shares	T1027 Obfuscated Files or Information
T1569 System Services	T1569.002 Service Execution	T1573 Encrypted Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff 80bd00c0f6d5e39b542ee6e9b67b1eef97b2dbc6ec6cae87bf5148f1cf18c260 8dd9773c24703e803903e7a5faa088c2df9a4b509549e768f29276ef86ef96ae 486eb80171c086f4d184423ed7e79303ad7276834e5e5529b199f8ae5fc661f2 f1edff0fb16a64ac5a2ce64579d0d76920c37a0fd183d4c19219ca990f50effc 887ae654d69ac5ccb8835e565a449d7716d6c4747dc2fbff1f59f11723244202 3fba459d589cd513d2478fb4ae7c4efd6aa09e62bc3ff249a19f9a233e922061 0dde13e3cd2dcda522eeb565b6374c97b3ed4aa6b8ed9ff9b6224ea97bf2a584 afd16b9ad57eb9c26c8ae347c379c8e2b82361c7bdff5b189659674d5614854c 3e59d36faf2d5e6edf1d881e2043a46055c63b7c68cc08d44cc7fc1b364157eb 786bd97172ec0cef88f6ea08e3cb482fd15cf28ab22d37792e3a86fa3c27c975 36c71ce7cd38733eb66f32a8c56acd635680197f01585c5a2a846cc3cb0a8fe2 016967de76382c674b3a1cb912eb85ff642b2ebfe4e107fc576065f172c6ef80 3059844c102595172bb7f644c9a70d77a198a11f1e84539792408b1f19954e18 b9cf785b81778e2b805752c7b839737416e3af54f64f1e40e008142e382df0c4 ab179112caadaf138241c43c4a4dccc2e3c67aeb96a151e432cfbafa18a4b436 6485a68ba1d335d16a1d158976e0cbfad7ab15b51de00c381d240e8b0c479f77

TYPE	VALUE
SHA256	b155c5b3a8f4c89ba74c5c5c03d029e4202510d0cbb5e152995ab91e6809bcd7
IPV4	194.61.121[.]86 141.95.22[.]153 193.200[.]16.3 192.52.166[.]191 45.56.162[.]111 104.194.222[.]219 192.169.6[.]88 192.52.167[.]20 146.70.106[.]89 46.249.35[.]243 45.86.230[.]20
Domains	webstore4tech[.]uaenorth.cloudapp.azure[.]com vatacloud[.]com
URLs	hxxps://pairing[.]rport[.]io/qMLc2Wx

References

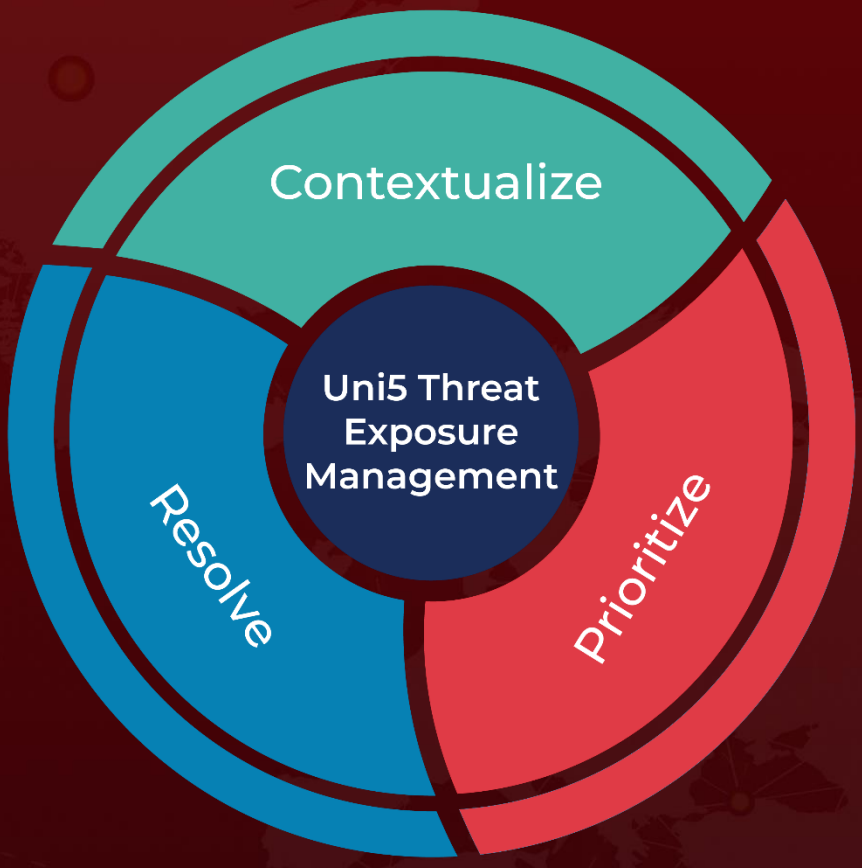
https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/

https://apt.etda.or.th/cgi-bin/showcard.cgi?g=MuddyWater%2C%20Seedworm%2C%20TEMP%2EZagros%2C%20Static%20Kitten

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

April 13, 2023 • 12:30 AM

More at www.hivepro.com