Hive Pro

THREAT ADVISORY

Iranian state-sponsored APT group MuddyWater targeting organizations via malicious executables

TA2022024

Threat Level RED

Publish Date – Feb 7, 2022
Updated Date – Mar 11, 2022

United States Cyber Command (USCYBERCOM) and CISA has warned of an ongoing cyber attack by Iranian state sponsored actor named as MuddyWater. This APT group is currently targeting Middle Eastern countries and has also targeted European and North American nations.

The Iranian-backed MuddyWater hacking group is conducting a new malicious campaign targeting private organizations and governmental institutions in Turkey and Middle East. MuddyWater actors have recently been observed using various malware variants of PowGoop, Small Sieve, Canopy (also known as Starwhale), Mori, and POWERSTATS—for loading malware, backdoor access, persistence and exfiltration

MuddyWater actors have been observed exploiting publicly disclosed vulnerabilities and employing open-source tools and strategies to gain access to sensitive data on victims' systems and deploy ransomware. The current attacks are carried out by Muddywater in two different ways. The first method is carried out by crafting a malicious PDF file with an embedded button that, when clicked, downloads an XLS file. The malicious VBA macros in the XLS documents will subsequently commence the infection process and establish persistence by generating a new Registry key. Simultaneously, a VBScript is downloaded using a PowerShell downloader to get the primary payload from the C2. The second infection chain uses a specially crafted EXE file rather than an XLS file, but it still uses the PowerShell downloader, the intermediate VBScript, and inserts a new registry key to obtain persistence.

The Techniques commonly used by Muddywater are:

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
TA0010 - Exfiltration
T1140: Deobfuscate/Decode Files or Information
T1041: Exfiltration Over C2 Channel
T1203: Exploitation for Client Execution
T1083: File and Directory Discovery
T1105: Ingress Tool Transfer
T1047: Windows Management Instrumentation
T1104: Multi-Stage Channels
T1027: Obfuscated Files or Information
T1057: Process Discovery
T1219: Remote Access Software
T1113: Screen Capture
T1518: Software Discovery
T1082: System Information Discovery
T1016: System Network Configuration Discovery
T1049: System Network Connections Discovery

T1033: System Owner/User Discovery
T1555: Credentials from Password Stores
T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control
T1087.002: Account Discovery: Domain Account
T1583.006: Acquire Infrastructure: Web Services
T1071.001: Application Layer Protocol: Web Protocols
T1560.001: Archive Collected Data: Archive via Utility
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1059.001: Command and Scripting Interpreter: PowerShell
T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1059.005: Command and Scripting Interpreter: Visual Basic
T1059.006: Command and Scripting Interpreter: Python
T1059.007: Command and Scripting Interpreter: JavaScript
T1589.002: Gather Victim Identity Information: Email Addresses
T1562.001: Impair Defenses: Disable or Modify Tools
T1559.001: Inter-Process Communication: Component Object Model
T1559.002: Inter-Process Communication: Dynamic Data Exchange
T1036.005: Masquerading: Match Legitimate Name or Location
T1559.001: Inter-Process Communication: Component Object Model
T1559.002: Inter-Process Communication: Dynamic Data Exchange
T1036.005: Masquerading: Match Legitimate Name or Location
T1027.003: Steganography
T1027.004: Compile After Delivery
T1588.002: Obtain Capabilities: Tool
T1137.001: Office Application Startup: Office Template Macros
T1003.001: OS Credential Dumping: LSASS Memory
T1003.004: OS Credential Dumping: LSA Secrets
T1003.005: OS Credential Dumping: Cached Domain Credentials
T1566.001: Phishing: Spearphishing Attachment
T1566.002: Phishing: Spearphishing Link
T1555.003: Credentials from Web Browsers
T1132.001: Data Encoding: Standard Encoding
T1053.005: Scheduled Task/Job: Scheduled Task
T1218.003: Signed Binary Proxy Execution: CMSTP
T1218.005: Signed Binary Proxy Execution: Mshta
T1218.011: Signed Binary Proxy Execution: Rundll32
T1053.005: Scheduled Task/Job: Scheduled Task
T1518.001: Security Software Discovery
T1090.002: Proxy: External Proxy
T1559.001: Inter-Process Communication: Component Object Model
T1559.002: Inter-Process Communication: Dynamic Data Exchange
T1036.005: Masquerading: Match Legitimate Name or Location
T1552.001: Unsecured Credentials: Credentials In Files
T1204.001: User Execution: Malicious Link
T1204.002: User Execution: Malicious File
T1102.002: Web Service: Bidirectional Communication
T1574.002: Hijack Execution Flow: DLL Side-Loading

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
MuddyWater (Static Kitten , Seedworm, TEMP.Zagros, Mercury, TA450, Cobalt Ulster, ATK 51, T-APT-14, ITG17)	Iran	Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israel, Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Pakistan, Russia, Saudi Arabia, Tajikistan, Thailand, Tunisia, Turkey, UAE, Ukraine, USA.	Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthcare, High-Tech, IT, Media, NGOs, Oil and gas, Telecommunications, Transportation.	Information theft and espionage

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2020-1472	Microsoft Windows Server 1903, Server 1909, Server 2004, Server 2008 R2, Server 2012, Server 2012 R2, Server 2016, Server 2019	cpe:2.3:o:microsoft:windows_server:1903:*:*:*:*:*:*:*,cpe:2.3:o:microsoft:windows_server:1909:*:*:*:*:*:*:*,cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*,cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Microsoft Window Netlogon privilege escalation	CWE-330
CVE-2021-34527	Microsoft Windows Server 2010, Server 2013, Server 2016, Server 2019	cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_30:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_14:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_15:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_3:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_4:*:*:*:*:*:*:*	Microsoft Exchange Memory Corruption Vulnerability	CWE-789

Indicators of Compromise (IoCs)

Type	Value
SHA-256	8d6ed63f2ffa053a683810f5f96c76813cdca2e188f16d549e002b2f63cee001, 42aa5a474abc9efd3289833eab9e72a560fee48765b94b605fac469739a515c1, d3ecc4137fc9a6d7418b4780864baf64cf7417d7badf463dff6ea48cd455915b, 9991b185c9e9732501e0c2bd841e32a4022f0735a0527150bc8e64ac363d409d, d9de66497ad189d785d7535ab263e92ffad81df20b903c5e1d36859b4ed38b6d, 5cdc7dd6162a8c791d50f5b2c5136d7ba3bf417104e6096bd4a2b76ea499a2f4, 26ed7e89b3c5058836252e0a8ed9ec6b58f5f82a2e543bc6a97b3fd17ae3e4ec, a8701fd6a5eb45e044f8bf150793f4189473dde46e0af8314652f6bf670c0a34, b726f4dd745891070f2e516d5d4e4f2f1ce0bf3ff685dc3800455383f342e54d, c9931382f844b61a002f83db1ae475953bbab449529be737df1eee8b3065f6eb, fcdd38ff378605c66333429d9df2242fbce25a5f69f4d6d4c11d9613bcb409b0, c13cb1c9277324534075f807a3fcd24d0d3c024197c7437bf65db78f6a987f7a, 450302fb71d8e0e30c80f19cfe7fb7801b223754698cac0997eb3a3c8e440a48, b1e30cce6df16d83b82b751edca57aa17795d8d0cdd960ecee7d90832b0ee76c, 921b4520b75fcd0071944a483d738223b222ba101e70f2950fbfbc22afbdb5d0, d7de68febbbdb72ff820f6554afb464b5c204c434faa6ffe9b4daf6b691d535f, 8b9be9e4d18c5fc71cd12dbfd60ea41eb88a07497e96faa2ba20fdc929b32c0b,

Type	Value
SHA-256	a69fee382cf86f9e457e0688932cbd00671d0d5218f8043f1ee385278ee19c8c, 63e404011aeabb964ce63f467be29d678d0576bddb72124d491ab5565e1044cf, 6910ddb58aee9a77e7bb9cadef9e6280a9b5b495edf0b6538cf8bdc1db8b1f4c, d851badfcf3b3a8b4210bdb33948d0d1d918ec6bf0f1f85cbae6bb8feec7cd74, aa72f1543d4a4e6ecbfc2da0167f5601c5c692bed73243cf01f616bc4af68afe, 7dc49601fa6485c3a2cb1d519794bee004fb7fc0f3b37394a1aef6fceefec0c8, a69fee382cf86f9e457e0688932cbd00671d0d5218f8043f1ee385278ee19c8c, 8f255a1f2e17828a5b9205d6991e2c85c3320311da28048785262396cbc568c7, cddd5514b7ed3d33ff8eaa16b7b71621ced857755246683e0d28c4650ea744bf, b4d0161ecab5a7847d325c88ce1a4fc2ca2e11fad0b77638b63ae1781c8b5793, f6569039513e261ba9c70640e6eb8f59a0c72471889d3c0eaba51bdebb91d285, 28f2198f811bbd09be31ad51bac49ba0be5e46ebf5c617c49305bb7e274b198c, 04d6ed9c6d4a37401ad3c586374f169b0aa8d609710bdcf5434d39e0fd4ed9bd, 69e3a454c191ee38663112cf5358a54cca1229188087ed18e92bc9c59b014912, dc28b5e878152b5305b8d251019895caa56a7a95a68eccb89a6ecc41da8aadb9, dd7ee54b12a55bcc67da4ceaed6e636b7bd30d4db6f6c594e9510e1e605ade92, 4b2862a1665a62706f88304406b071a5c9a6b3093daadc073e174ac6d493f26c, 026868713d60e6790f41dc7046deb4e6795825faa903113d2f22b644f0d21141, 7de663524b63b865e57ffc3eb4a339e150258583fdee6c2c2ca4dd7b5ed9dfe7, 6e50e65114131d6529e8a799ff660be0fc5e88ec882a116f5a60a2279883e9c4, ef385ed64f795e106d17c0a53dfb398f774a555a9e287714d327bf3987364c1b, d77e268b746cf1547e7ed662598f8515948562e1d188a7f9ddb8e00f4fd94ef0, ed988768f50f1bb4cc7fb69f9633d6185714a99ecfd18b7b1b88a42a162b0418, c2badcdfa9b7ece00f245990bb85fb6645c05b155b77deaf2bb7a2a0aacbe49e, f10471e15c6b971092377c524a0622edf4525acee42f4b61e732f342ea7c0df0, cc67e663f5f6cea8327e1323ecdb922ae8e48154bbf7bd3f9b2ee2374f61c5d6, fb69c821f14cb0d89d3df9eef2af2d87625f333535eb1552b0fcd1caba38281f, 202bf7a4317326b8d0b39f1fa19304c487128c8bd6e52893a6f06f9640e138e6, 3fe9f94c09ee450ab24470a7bcd3d6194d8a375b3383f768662c1d561dab878d, a500e5ab8ce265d1dc8af1c00ea54a75b57ede933f64cea794f87ef1daf287a1
IPs	5[.]199[.]133[.]149, 88[.]119[.]170[.]124, 185[.]183[.]97[.]25, 95[.]181.161.81, 178[.]32[.]30[.]3
URLs	hxxp://185.118.167[.]120/, hxxp://137.74.131[.]16:443/, hxxp://185.141.27[.]211:443/, hxxp://149.202.242[.]84:443/, hxxp://172.245.81[.]135:10196/Geq5P3aFpaSrK3PZtErNgUsVCfqQ9kZ9/Pan-op/gallery.jpg, hxxps://snapfile[.]org/d/c7817a35554e88572b7b, hxxps://snapfile[.]org/d/0c88a47c3160338bbb68, hxxp://snapfile[.]org/756a12c43a0fb8d56fbf, hxxps://snapfile[.]org/5bc3985cf17565a97dbd, hxxps://snapfile[.]org/55e1c83e920bb7dc949c, hxxp://canarytokens[.]com/about/d3g23n4gdcrep20q3wzm153xn/index.html, hxxp://canarytokens[.]com/tags/traffic/images/azp6ai8pg5aq0c619ur0qzi6h/, hxxp://canarytokens[.]com/tags/traffic/images/azp6ai8pg5aq0c619ur0qzi6h/post.jsp

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0688

References

https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/
https://otx.alienvault.com/pulse/61f9cc60ec3a15d1cd569f87
https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html
https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-055a