THREAT BULLETINS

Joint Alert: Iranian Government-Sponsored MuddyWater Actors Conducting Malicious Cyber Operations

TLP:WHITE

Feb 24, 2022

The United States Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the US Cyber Command Cyber National Mission Force (CNMF), and the United Kingdom’s National Cyber Security Centre (NCSC-UK) have observed a group of Iranian government-sponsored advanced persistent threat (APT) actors, known as MuddyWater, conducting cyber espionage and other malicious cyber operations targeting a range of government and private-sector organizations across sectors in Asia, Africa, Europe, and North America.

MuddyWater is a subordinate element within the Iranian Ministry of Intelligence and Security (MOIS). This APT group has conducted broad cyber campaigns in support of MOIS objectives since approximately 2018. MuddyWater actors are positioned both to provide stolen data and access to the Iranian government and to share these with other malicious cyber actors.

MuddyWater actors are known to exploit publicly reported vulnerabilities and use open-source tools and strategies to gain access to sensitive data on victims' systems and deploy ransomware. These actors also maintain persistence on victim networks via tactics such as side-loading dynamic link libraries (DLLs), to trick legitimate programs into running malware, and obfuscating PowerShell scripts to hide command and control (C2) functions. FBI, CISA, CNMF, and NCSC-UK have observed MuddyWater actors recently using various malware, variants of PowGoop, Small Sieve, Canopy (also known as Starwhale), Mori, and POWERSTATS, along with other tools as part of their malicious activity.

Health-ISAC is releasing this intelligence report for your increased security awareness. This intelligence advisory provides observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) associated with this Iranian government-sponsored APT activity to aid organizations in the identification of malicious activity against sensitive networks. The original alert, Alert (AA22-055A): Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks, can be accessed here.

FBI, CISA, CNMF, and NCSC-UK have observed the Iranian government-sponsored MuddyWater APT group employing spearphishing, exploiting publicly known vulnerabilities, and leveraging multiple open-source tools to gain access to sensitive government and commercial networks.

As part of its spearphishing campaign, MuddyWater attempts to coax their targeted victim into downloading ZIP files, containing either an Excel file with a malicious macro that communicates with the actor's C2 server or a PDF file that drops a malicious file to the victim's network. MuddyWater actors also use techniques such as side-loading DLLs to trick legitimate programs into running malware and obfuscating PowerShell scripts to hide C2 functions.

Additionally, the group uses multiple malware sets, including PowGoop, Small Sieve, Canopy/Starwhale, Mori, and POWERSTATS, for loading malware, backdoor access, persistence, and exfiltration.

See below for descriptions of some of these malware sets, including newer tools or variants to the group’s suite:

PowGoop

MuddyWater actors use new variants of PowGoop malware as their main loader in malicious operations; it consists of a DLL loader and a PowerShell-based downloader. The malicious file impersonates a legitimate file that is signed as a Google Update executable file

According to samples of PowGoop analyzed by CISA and CNMF, PowGoop consists of three components:

- A DLL file is renamed as a legitimate filename, Goopdate[.]dll, to enable the DLL side-loading technique. The DLL file is contained within an executable, GoogleUpdate[.]exe.
- A PowerShell script obfuscated as a .dat file, goopdate[.]dat, used to decrypt and run a second obfuscated PowerShell script, config.txt.
- config[.]txt, an encoded, obfuscated PowerShell script containing a beacon to a hardcoded IP address.

These components retrieve encrypted commands from a C2 server. The DLL file hides communications with MuddyWater C2 servers by executing with the Google Update service.

Small Sieve

According to a sample analyzed by NCSC-UK, Small Sieve is a simple Python backdoor distributed using a Nullsoft Scriptable Install System (NSIS) installer, gram_app[.]exe. The NSIS installs the Python backdoor, index[.]exe, and adds it as a registry run key, enabling persistence.

MuddyWater disguises malicious executables and uses filenames and Registry key names associated with Microsoft's Windows Defender to avoid detection during a casual inspection. The APT group has also used variations of Microsoft and Outlook in its filenames associated with Small Sieve.

Small Sieve provides the basic functionality required to maintain and expand a foothold in victim infrastructure and avoid detection by using custom string and traffic obfuscation schemes together with the Telegram Bot application programming interface (API). Specifically, Small Sieve’s beacons and taskings are performed using Telegram

API over Hypertext Transfer Protocol Secure (HTTPS), and the tasking and beaconing data are obfuscated through a hex byte-swapping encoding scheme combined with an obfuscated Base64 function.

Canopy

MuddyWater also uses Canopy/Starwhale malware, likely distributed via spearphishing emails with targeted attachments. According to two Canopy/Starwhale samples analyzed by CISA, Canopy uses Windows Script File ([.]wsf) scripts distributed by a malicious Excel file.

In the samples CISA analyzed, a malicious Excel file, Cooperation terms[.]xls, contained macros written in Visual Basic for Applications (VBA) and two encoded Windows Script Files. When the victim opens the Excel file, they receive a prompt to enable macros. Once this occurs, the macros are executed, decoding and installing the two embedded Windows Script Files.

The first [.]wsf is installed in the current user startup folder for persistence. The file contains hexadecimal (hex)-encoded strings that have been reshuffled. The file executes a command to run the second [.]wsf.

Mori

MuddyWater also uses the Mori backdoor that uses Domain Name System tunneling to communicate with the group's C2 infrastructure.

According to one sample analyzed by CISA, FML[.]dll, Mori uses a DLL written in C++ that is executed with regsvr32[.]exe with export DllRegisterServer; this DLL appears to be a component to another program. FML[.]dll contains approximately 200MB of junk data in a resource directory 205, number 105. Upon execution, FML[.]dll creates a mutex, 0x50504060, and performs the following tasks:

- Deletes the file FILENAME[.]old and deletes file by registry value. The filename is the DLL file with an [.]old extension.
- Resolves networking APIs from strings that are ADD-encrypted with the key 0x05.
- Uses Base64 and JavaScript Object Notation (JSON) based on certain key values passed to the JSON library functions. It appears likely that JSON is used to serialize C2 commands and/or their results.

- Communicates using HTTP over either IPv4 or IPv6, depending on the value of an unidentified flag, for C2.
- Reads and/or writes data from the following Registry Keys, HKLM\Software\NFC\IPA and HKLM\Software\NFC\(Default).

POWERSTATS

This group is also known to use the POWERSTATS backdoor, which runs PowerShell scripts to maintain persistent access to the victim systems.

CNMF has posted samples further detailing the different parts of MuddyWater’s new suite of tools, along with JavaScript files used to establish connections back to malicious infrastructure, to the malware aggregation tool and repository, Virus Total. Network operators who identify multiple instances of the tools on the same network should investigate further as this may indicate the presence of an Iranian malicious cyber actor.

MuddyWater actors are also known to exploit unpatched vulnerabilities as part of their targeted operations. FBI, CISA, CNMF, and NCSC-UK have observed this APT group recently exploiting the Microsoft Netlogon elevation of privilege vulnerability (CVE-2020-1472) and the Microsoft Exchange memory corruption vulnerability (CVE-2020-0688).

The second .wsf also contains hex-encoded strings that have been reshuffled. This file collects the victim system’s IP address, computer name, and username. The collected data is then hex-encoded and sent to an adversary-controlled IP address.

Reference(s)	Mitre, NCSC, cisa, Mitre, cybercom, Virus Total

Recommendations
Protective Controls and Architecture

- **Deploy application control software to limit the applications and executable code that can be run by**

users. Email attachments and files downloaded via links in emails often contain executable code.

Identity and Access Management

- **Use multi-factor authentication where possible,** particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Limit the use of administrator privileges.** Users who browse the internet, use email and execute code with administrator privileges make for excellent spearphishing targets because their system, once infected, enables attackers to move laterally across the network, gain additional accesses, and access highly sensitive information.

Phishing Protection

- **Enable antivirus and anti-malware software and update signature definitions in a timely manner.** Well-maintained antivirus software may prevent the use of commonly deployed attacker tools that are delivered via spearphishing.
- **Be suspicious of unsolicited contact via email or social media from any individual you do not know personally.** Do not click on hyperlinks or open attachments in these communications.
- **Consider adding an email banner to emails received from outside your organization and disabling hyperlinks in received emails.**
- **Train users through awareness and simulations to recognize and report phishing and social engineering attempts.** Identify and suspend access of user accounts exhibiting unusual activity.
- **Adopt threat reputation services at the network device, operating system, application, and email service levels.** Reputation services can be used to detect or prevent low-reputation email addresses, files, URLs, and IP addresses used in spearphishing attacks.

Vulnerability and Configuration Management

- **Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.**
- Prioritize patching known exploited vulnerabilities.

Sources

CNMF Article: Iranian Intel Cyber Suite of Malware Uses Open Source Tools
MITRE ATT&CK: MuddyWater

Alert (AA22-055A): Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

Alert ID 6cac04c3

View Alert

Tags MuddyWater threat actor, MuddyWater threat actor group, MuddyWater APT, Iranian Hacker, Iranian Hackers, APT, Iran, Iranian, APTs, MuddyWater

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

FBI The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI’s 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.