New PowerShell-based Backdoor, MuddyWater Similarities

By By: Jaromir Horejsi, Daniel Lunghi Nov 30, 2018 Read time: 5 min (1282 words)

Published: 2018-11-30 · Archived: 2026-04-05 15:51:10 UTC

MuddyWater is a well-known threat actor group that has been active since 2017. They target groups across Middle East and Central Asia, primarily using spear phishing emails with malicious attachments. Most recently they were connected to a campaign in March that targeted organizations in Turkey, Pakistan, and Tajikistanopen on a new tab.

The group has been quite visible since the initial 2017 Malwarebytes reportopen on a new tab on their elaborate espionage attack against the Saudi Arabian government. After that first report, they were extensively analyzedopen on a new tab by other security companies. Through all that, we've only seen minor changes to the tools, techniques and procedures (TTPs) they have used.

However, we recently observed a few interesting delivery documents similar to the known MuddyWater TTPs. These documents are named **Raport.doc** or **Gizli Raport.doc** (titles mean "Report" or "Secret Report" in Turkish) and **maliyeraporti (Gizli Bilgisi).doc** ("finance (Confidential Information)" in Turkish) — all of which were uploaded to Virus Total from Turkey. Our analysis revealed that they drop a new backdoor, which is written in PowerShell as MuddyWater's known POWERSTATS backdoor. But, unlike previous incidents using POWERSTATS, the command and control (C&C) communication and data exfiltration in this case is done by using the API of a cloud file hosting provider.

The screenshots below show the malicious attachments, which are disguised to look real, similar to any typical phishing document. The images show blurry logos that we've identified as belonging to various Turkish government organizations — the logos add to the disguise and lure users into believing the documents are legitimate. Then the document notifies users that it is an "old version" and prompts them to enable macros to display the document properly. If the targeted victims enable macros, then the malicious process continues.

Figure 1. Fake Office document tries to get user to enable malicious macros. The blurred document contains logos of different Turkish government entities

Figure 2. A similar fake Office document has blurred logos for a Turkish government institution related to taxes

The macros contain strings encoded in base52, which is rarely used by threat actors other than MuddyWater. The group is known to use it to encode their PowerShell backdoor.

After enabling macros, a .dll file (with a PowerShell code embedded) and a .reg file are dropped into %temp% directory. The macro then runs the following command:

> "C:\Windows\System32\cmd.exe" /k %windir%\System32\reg.exe IMPORT %temp%\B.reg

Running this registry file adds the following command to the Run registry key:

> rundll32 %Temp%\png.dll,RunPow

Figure 3. Run registry key

We assume that RunPow stands for “run PowerShell,” and triggers the PowerShell code embedded inside the .dll file. The PowerShell code has several layers of obfuscation. The first layer contains a long base64 encoded and encrypted code with variables named using English curse words.

Figure 4. Encrypted PowerShell code

The other layers are simple obfuscated PowerShell scripts. But the last layer is the main backdoor body. This backdoor has some features similar to a previously discovered version of the Muddywater backdoor.

Firstly, this backdoor collects the system information and concatenates various pieces of information into one long string. The data retrieved includes: OS name, domain name, user name, IP address, and more. It uses the separator "::" between each piece of information.

Figure 5. String of system information collected from the victim’s system

The previous MuddyWater version collected similar information but used a different separator:

Figure 6. String of system information collected from the victim’s system, from older Muddywater backdoor sample

As mentioned above, another difference between this and older Muddywater backdoors is that C&C communication is done by dropping files to the cloud provider. When we analyzed further, we saw that the communication methods use files named <md5*(hard disk serial number)*> with various extensions depending on the purpose of the file.

- **.cmd** - text file with a command to execute
- **.reg** - system info as generated by myinfo() function, see screenshot above
- **.prc** - output of the executed .cmd file, stored on local machine only
- **.res** - output of the executed .cmd file, stored on cloud storage

Figure 7. Example of .cmd file content

Figure 8. Example of .reg file content

Figure 9.Example of .res file content

In both the older version of the MuddyWater backdoor and this recent backdoor, these files are used as an asynchronous mechanism instead of connecting directly to the machine and issuing a command. The malware operator leaves a command to execute in a .cmd file, and comes back later to retrieve the .res files containing the result of the issued command.

However, in the older MuddyWater backdoor their content was encoded differently. The files are temporarily stored on compromised websites. The more recent backdoor uses a legitimate cloud storage service provider instead.

The .res file can be decoded by replacing “00” with empty string, then converting from hex to ASCII, then reversing the string. The figure below is the decoded .res file from Figure 9.

Figure 10. Decoded .res file

The backdoor supports the following commands:

- **$upload** - upload a file to file hosting service
- **$dispos** - remove persistence
- **$halt** - exit
- **$download** - download file from a hosting service
- **No prefix** - execute command via Invoke Expression (IEX), a PowerShell command that runs commands or expressions on the local computer

Based on our analysis, we can confirm that the targets were Turkish government organizations related to the finance and energy sectors. This is yet another similarity with previous MuddyWater campaigns, which were known to have targeted multiple Turkish government entities. If the group is responsible for this new backdoor, it shows how they are improving and experimenting with new tools.

Solutions and Recommendations

The main delivery method of this type of backdoor is spear phishing emails or spam that uses social engineering to manipulate targets into enabling malicious documents. It is important that employers and employees across all organizations and enterprises be able to identify phishing attacksopen on a new tab and distinguish legitimate emailsopen on a new tab from malicious ones. Awareness of these threats and the tactics they use is an effective first step.

Telltale signs of social engineering include “too-good-to-be-true” offers and messages that lack context. In general, users should always practice caution when it comes to email. This includes avoiding clicking on links or downloading any documents unless certain that these are legitimate.

Apart from knowledge and awareness of phishing and social engineering, it is also important to be prepared with effective and layered security solutions. Trend Micro™ Deep Discovery™open on a new tab provides detection, in-depth analysis, and proactive response to today’s stealthy malware, and targeted attacks in real time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxingopen on a new tab, and seamless correlation across the entire attack lifecycle, allowing it to detect threats even without any engine or pattern update.

Trend Micro™ Email Securityopen on a new tab is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network.

Trend Micro™ Email Inspectoropen on a new tab and InterScan™ Web Securityopen on a new tab prevent malware from ever reaching end users. At the endpoint level, Trend Micro™ Smart Protection Suitesopen on a new tab deliver several capabilities that minimize the impact of these attacks.

These solutions are powered by the Trend Micro XGen™ security, which provides a cross-generational blend of threat defense techniques against a full range of threats for data centers, cloud environments, networks, and endpoints. It features high-fidelity machine learning to secure the gateway and endpoint data and applications, and protects physical, virtual, and cloud workloads.

Indicators of Compromise

SHA256	Type	Detection Name
41ee0ab77b474b0c84a1c25591029533f058e4454d9f83ba30159cc6309c65d1	Delivery documents	W2KM_POWRUN.A

43080479eb1b00ba80c34272c5595e6ebdc6b0ffabcdc2c40ea2af49fcc43db4	Dropped DLL file	Backdoor.Win32.POWRUN.AA
4f509354d8b3152a40c64ce61f7594d592c1256ad6c0829760b8dbdcb10579a2	Weaponized document	BACKDOOR.WIN32.POWRUN.
685e91bc4e98c38bda7c8e57d5d40a11e7cf48bb43859bb799813f0146a14fcf	Dropped DLL file	BKDR_POWRUN.B
888a6f205ac9fc40d4898d8068b56b32f9692cb75f0dd813f96a7bd8426f8652	Dropped DLL file	Trojan.W97M.POWRUN.AA
0acd10b14d38a4ac469819dfa9070106e7289ecf7360e248b7f10f868c2f373d	Dropped DLL file	BKDR_POWRUN.A
