



NEW WEKBY ATTACKS USE DNS REQUESTS AS COMMAND AND CONTROL MECHANISM

POSTED BY: Josh Grunzweig, Mike Scott and Bryan Lee on May 24, 2016 11:30 AM

FILED IN: Malware, Threat Prevention, Unit 42
TAGGED: command and control, DNS, pisloader, Wekby

We have observed an attack led by the APT group Wekby targeting a US-based organization in recent weeks. Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of Hacking Team's Flash zero-day exploit

The malware used by the Wekby group has ties to the HTTPBrowser malware family, and uses DNS requests as a command and control mechanism. Additionally, it uses various obfuscation techniques to thwart researchers during analysis. Based on metadata seen in the discussed samples, Palo Alto Networks has named this malware family 'pisloader'.

INFRASTRUCTURE

The pisloader malware family was delivered via HTTP from the following URL. At the time of writing, this URL was still active.

http://globalprint-us[.]com/proxy_plugin.exe

Other samples hosted on this domain include the following:

http://globalprint-us[.]com/proxy_web_plugin.exe

MD5: E4968C8060EA017B5E5756C16B80B012

SHA256:

8FFBB7A80EFA9EE79E996ABDE7A95CF8DC6F9A41F9026672A8DBD95539FEA82A

Size: 126976 Bytes

Compile Time: 2016-04-28 00:38:46 UTC

This discovered file was found to be an instance of the common Poison Ivy malware family with the following configuration data:

Command and Control Address: intranetwabcam[.]com

Command and Control Port: 80

Password: admin Mutex:)!VoqA.I5

The domains witnessed in this attack were all registered very shortly prior to being used. The following domains have been witnessed in this attack:

Domain	Description	Registrant Date	
globalprint-us[.]com	Hosted Malware	2016-04-26	
ns1.logitech-usa[.]com	pisloader C2	2016-04-26	
intranetwabcam[.]com	Poison Ivy C2	2016-04-26	

Additionally, the following IP resolutions have been observed

Domain	IP Address	Registrant Organization	Country of Origin
globalprint-us[.]com	107.180.58[.]70	GoDaddy.com LLC	United States
ns1.logitech-usa[.]com	23.252.166[.]89	NexteCloud L.L.C.	United States
intranetwabcam[.]com	23.252.166[.]99	NexteCloud L.L.C.	United States

INITIAL DROPPER

The following sample was discovered initially and is referenced in the subsequent analysis:

MD5: E8D58AA76DD97536AC225949A2767E05

SHA256: DA3261C332E72E4C1641CA0DE439AF280E064B224D950817A11922A8078B11F1

Size: 126976 Bytes

Compile Time: 2016-04-27 14:37:34 UTC

This particular file has the following metadata properties. The references to 'pisload2' led to the naming of this malware family.

Home
Government
Partners
Unit 42 Threat Intelligence
Technical Documentation
Advanced Endpoint Protection



CATEGORIES & ARCHIVES	
Select a Category	
Select a Month	
	MORE →

RECENT POSTS

Prevention: Changing the Math of Cybersecurity Through Automated Defense

posted by Ryan Gillis on July 4, 2016

Palo Alto Networks News of the Week – July 2, 2016 posted by Anna Lough on July 2, 2016

Channel Scoop — July 1, 2016 posted by Lang Tibbils on July 1, 2016

Here's a Look at the First Palo Alto Networks Intern Tech Week! posted by Courtney Taku on July 1, 2016

Recent MNKit Exploit Activity Reveals Some Common Threads posted by Anthony Kasza on June 30, 2016

MORE -

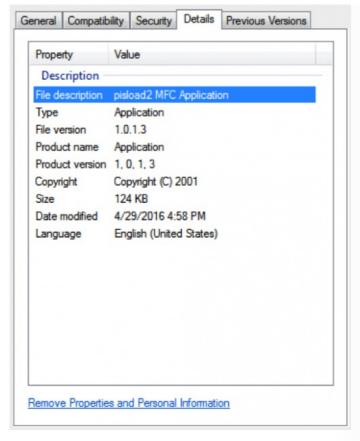


Figure 1 pisloader dropper metadata

The initial dropper contains very simple code that is responsible for setting persistence via the Run registry key, and dropping and executing an embedded Windows executable. Limited obfuscation was encountered, where the authors split up strings into smaller sub-strings and used 'strcpy' and 'strcat' calls to re-build them prior to use. They also used this same technique to generate garbage strings that are never used. This is likely to deter detection and analysis of the sample. The following decompiled code demonstrates this. Comments have been added to show the fully-generated strings.

```
stropy(drum_kny, aCBs);

**referred(arum_kny, aCBs);

**stropy(damnings_data, aTEkk);

**stropy(dam
```

Figure 2 pisloader dropper building strings and setting persistence

In the above decompiled code, we see that the pisloader is generating the following string, which eventually is called to set the Run registry key.

 $cmd.exe/c\ reg\ add\ HKCU\ Software\ Microsoft\ Windows\ Current\ Version\ Run\ /v\ Ism\ /t\ reg_sz\ /d\ "\%appdata\%\ Ism.exe"\ /f$

This particular command will set the

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\lsm registry key with a value of "%appdata%\lsm.exe". After this key is set, the malware proceeds to decrypt a two blobs of data with a single-byte XOR key of 0x54. The resulting data is written to the %appdata%\lsm.exe file path.

After this file is written, the malware executes the newly written Ism.exe file, which contains the pisloader payload.

PAYLOAD

The following sample was discovered and is referenced in the subsequent analysis:

MD5: 07B9B62FB3B1C068837C188FEFBD5DE9

SHA256:

456FFFC256422AD667CA023D694494881BAED1496A3067485D56ECC8FEFBFAEB

Size: 102400 Bytes

Compile Timestamp: 2016-04-27 13:39:02 UTC

The payload is heavily obfuscated using a return-oriented programming (ROP) technique, as

well as a number of garbage assembly instructions. In the example below, code highlighted in red essentially serves no purpose other than to deter reverse-engineering of the sample. This code can be treated as garbage and ignored. The entirety of the function is highlighted in green, where two function offsets are pushed to the stack, followed by a return instruction. This return instruction will point code execution first at the null function, which in turn will point code execution to the 'next_function'. This technique is used throughout the runtime of the payload, making static analysis difficult.

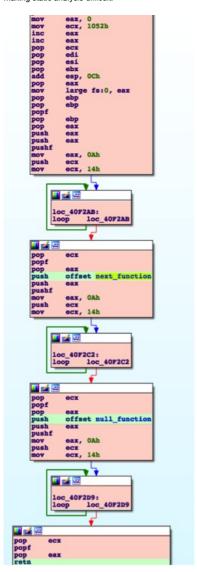


Figure 3 Obfuscated code witnessed in pisloader

The malware is actually quite simplistic once the obfuscation and garbage code is ignored. It will begin by generating a random 10-byte alpha-numeric header. The remaining data is base32-encoded, with padding removed. This data will be used to populate a subdomain that will be used in a subsequent DNS request for a TXT record.

The use of DNS as a C2 protocol has historically not been widely adopted by malware authors. Notable exceptions include the following:

- FrameworkPOS
- C3PRO-RACCOON
- FeederBot
- Morto
- PlugX Variants

The use of DNS as a C2 allows pisloader to bypass certain security products that may not be inspecting this traffic correctly.

```
Domain Name System (query)

[Response In: 1613]

Transaction ID: Oxa45e

□ Flags: 0x0100 Standard query

0... - Response: Message is a query

.000 0... - Opcode: Standard query (0)

... 0. - Truncated: Message is not truncated

... 1 ... - Recursion desired: Do query recursively

... 0. - 2: reserved (0)

... 0 - Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Authority RRs: 0

Queries

□ QOOXHNOCCOMYUWOXCEMYZWWSDPOA7A.ns1.logitech-usa.com: type TXT, class IN

Name: QOOXHNOCCOMYUWOXCEMYZWWSDPOA7A.ns1.logitech-usa.com

[Name Length: 51]

[Label Count: 4]

Type: TXT (Text strings) (16)

Class: IN (0x0001)
```

Figure 4 DNS query for TXT record by malware

The pisloader sample will send a beacon periodically that is composed of a random 4-byte uppercase string that is used as the payload. An example of this can be found below:

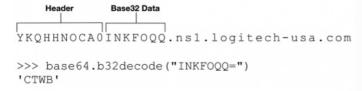


Figure 5 pisloader DNS beacon request

The malware expects various aspects of the DNS responses to be set in a specific way, or else pisloader will ignore the DNS reply. The following DNS flags must be set. Should any additional flags be set, the response will be ignored.

- Response
- Recursion Desired
- Recursion Available

The 'Questions' field must be set to a value of 0x1. The 'Answer Resource Records' field must be set to a value of 0x1. Additionally, the response query subdomain must match the original DNS request.

The remote command and control (C2) server is statically embedded within the malware. A single host of 'ns1.logitech-usa[.]com' is found in this specific sample.

The C2 server will respond with a TXT record that is encoded similar to the initial request. In the response, the first byte is ignored, and the remaining data is base32-encoded. An example of this can be found below.

```
Header Base32 Data

CONUWM3Y

>>> base64.b32decode("ONUWM3Y=")
'sifo'
```

Figure 6 Example TXT response by C2 server

The following commands, and their descriptions are supported by the malware:

- sifo Collect victim system information
- drive List drives on victim machine
- list List file information for provided directory
- upload Upload a file to the victim machine
- open Spawn a command shell

Some examples of these commands being used can be seen below. A mock DNS server was used to generate the commands and receive the resulting data.

Example sending the 'drive' command:

```
1 [+] Sending Command: drive | Encoded: CMRZGSSTF
2 [+] Raw Data Received: UMAVMGAGDØIE5FY7CDHJOHYRB2LR6A
3 [+] Decoded Data Received: A:\|C:\|D:\|
```

```
1 [+] Sending Command: open | Encoded: CN5YGK3Q
2 [+] Raw Data Received: ULCBMGAGCAJVUWG4TPONXWM5BAK5UW4ZDPO5ZSAW2WMV
3 [+] Raw Data Received: ATABMGAGCBNYQDMLRRFY3TMMBRLUGQUQ3POB4XEZLHNE
4 [+] Raw Data Received: HTPDMGAGCCFEQDEMBQHEQE2ZLDOJXXG33GOQQEG33SOB
5 [+] Raw Data Received: BNJWMGAGCDNFXW4LRAEBAWY3BAOJUW0ZDUOMQHEZLTMV
6 [+] Raw Data Received: UARCMGAGCEFYGQUDIKIM5FYVLTMVZHGXCKN5ZWQICHOJ
7 [+] Raw Data Received: UJRAMGAGC0MVUW0XCEMVZWW5DPOA7A
8 [+] Decoded Data Received: Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
10
11 C:\Users\Josh Grunzweig\Desktop>
```

Example sending the 'sifo' command:

```
1 [+] Sending Command: sifo | Encoded: CONUWM3Y
2 [+] Raw Data Received: FUBWMGAGIANQ6TCNZSFYYTMLRRFYYTKMZGMM6VOSKOFVG
3 [+] Raw Data Received: PGHRMGAGIBGJHEWSKPJNICAWZKN5ZWQICHOJ2W46TXMVL
4 [+] Raw Data Received: MMAZMGAGIBN46TMLBRFQZTE
5 [+] Decoded Data Received: 1=172.16.1.153&c=WIN-LJLV2NKIOKP [Josh Gr
```

Example listing the contents of the C:\ drive:

The sife command above uses the printf format string of 'l=%s&c=%s&o=%s'. This is consistent with previous versions of HTTPBrowser, which is another malware family frequently used by the Wekby group.

Additionally, a number of commands themselves, such as the 'list', 'drive', and 'upload' commands are consistent with HTTPBrowser. The formatted responses from these commands are also identical. A known HTTPBrowser sample was spotted with similar metadata as the discussed pisloader sample, which adds further credibility that pisloader is likely a variant of this malware family.

Additionally, the code used to generate these commands is available viaGitHub.

CONCLUSION

The Wekby group continues to target various high profile organizations using sophisticated malware. The pisloader malware family uses various novel techniques, such as using DNS as a C2 protocol, as well as making use of return-oriented programming and other anti-analysis tactics.

Palo Alto Networks customers are protected against this threat in the following ways:

- WildFire correctly identifies all pisloader samples as malicious
- A pisloader AutoFocus tag has been created in order to track this malware family
- All domains/IPs used in this attack have been flagged as malicious.
- An IPS rule has been created to detect pisloader DNS traffic

APPENDIX

External Resources

- https://blog.anomali.com/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysisvia-custom-rop
- http://www.volexity.com/blog/?p=158
- https://www.secureworks.com/research/threat-group-3390-targets-organizations-forcyberespionage
- https://www.zscaler.com/blogs/research/chinese-cyber-espionage-apt-group-leveraging-recently-leaked-hacking-team-exploits-target-financial-services-firm
- https://www.fireeye.com/blog/threat-research/2015/07/demonstrating hustle.html

SHA256 Hashes

da3261c332e72e4c1641ca0de439af280e064b224d950817a11922a8078b11f1
930772d6af8f43f62ea78092914fa8d6b03e8e3360dd4678eec1a3dda17206ed
6852ba95720af64809995e04f4818517ca1bd650bc42ea86d9adfdb018d6b274
9200f80c08b21ebae065141f0367f9c88f8fed896b0b4af9ec30fc98c606129b
4d62caef1ca8f4f9aead7823c95228a52852a1145ca6aaa58ad8493e042aed16
1b341dab023de64598d80456349db146aafe9b9e2ec24490c7d0ac881cecc094
456fffc256422ad667ca023d694494881baed1496a3067485d56ecc8fefbfaeb

Domains ns1.logitech-usa[.]com globalprint-us[.]com intranetwabcam[.]com login.access-mail[.]com glb.it-desktop[.]com local.it-desktop[.]com hi.getgo2[.]com **f g G + 2 COMMENTS** Share your thoughts Marcus on May 26, 2016 9:39 AM said Great article, well written. Yasir Irfan on May 28, 2016 10:27 PM said Very informative and well crafted **POST YOUR COMMENT** Name * Email * Website Post Comment