Unknown.exe - Dapato

Malware Analysis Report

ForkBomb Security

Threat Hunting and Intelligence

Prepared by fyezool

fyezool@forkbombsec.com

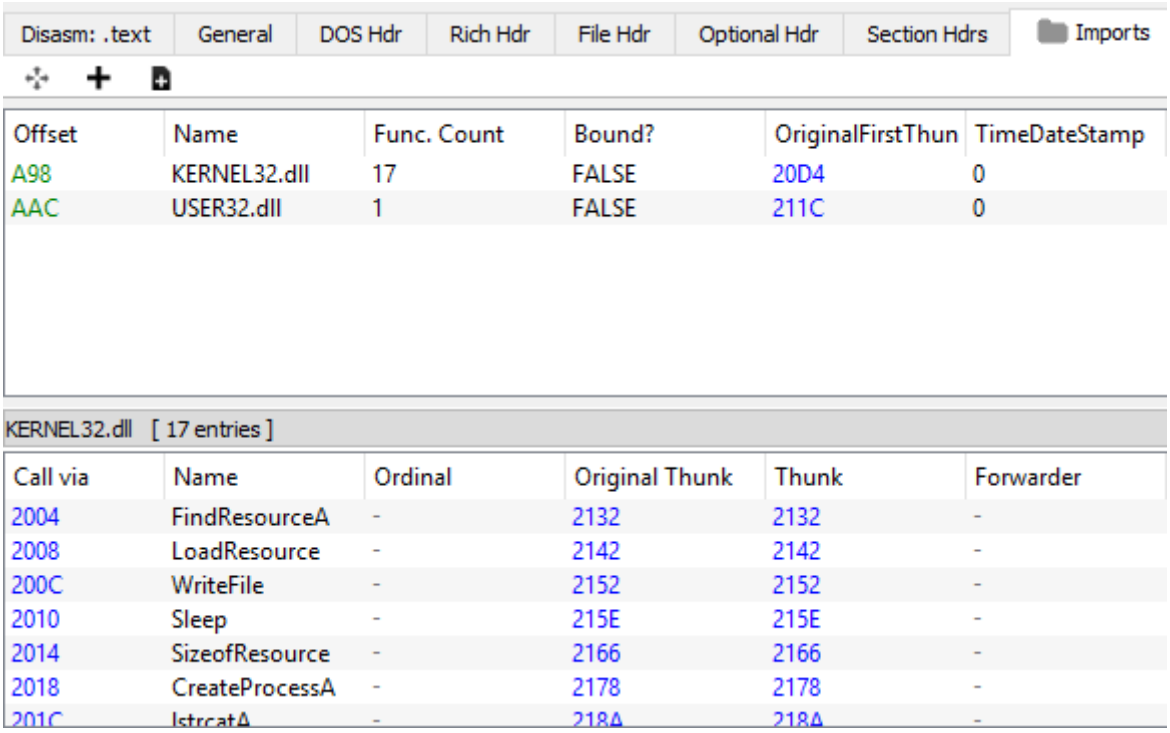
Initial analysis

- Malware Name : Dapato
- Sample file name : Unknown.exe

Hash

- File Type : Windows PE 32 bit
- MD5 : 29f228f3375c489a8a6e31203ab25787
- SHA1 : 14d713a5c8a2fc01fa2f01d993a249b9fb292810

PE header information



On Kernel 32.DLL tab id 2008 and 2018 which is LoadResource and Create ProcessA implied that this malware will infect the host by loading the resource and create a new file.

Virustotal analysis

From the Hash value given, we can search analysis and threat intelligence done reputable site like VirusTotal.

Ad-Aware	Dropped:Trojan.GenericKD.40365887	AegisLab	Trojan.Win32.Dapato.blc
AhnLab-V3	Malware/Win32.Generic.C2683156	Alibaba	TrojanDropper:Win32/Dapato.b0d2e9e3
ALYac	Dropped:Trojan.GenericKD.40365887	Antiy-AVL	Trojan/Win32.Fuery
SecureAge APEX	Malicious	Arcabit	Trojan.Generic.D267EF3F
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	Dropped:Trojan.GenericKD.40365887
BitDefenderTheta	Gen:NN.ZexaCO.34126.CuW@aasJKZg	Comodo	Malware@#2xc1wz93be8u9
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.3375c4

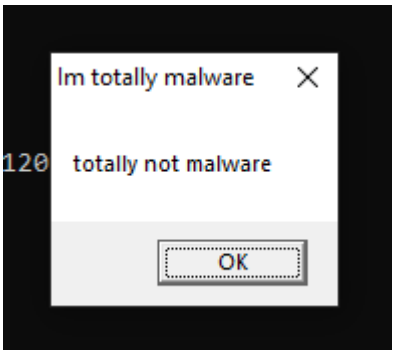
This malware have been detected and logged in database. More info can be found here.

Behavioral analysis

Depends on the type of Malware, once it is executed, some will give impact on the performance of the computer. While some just sit idly hidden in the process waiting for command from C2 or Command Center.

For this malware, what we will monitor is what kind of file and process it create & what is the domain it try to contact once executed.

Post execution



One system dialog poped-up after executed.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.10.111	10.10.10.112	DNS	83	Standard query 0xcaf2 A definitely-not-evil.com
2	0.000028894	10.10.10.112	10.10.10.111	ICMP	111	Destination unreachable (Port unreachable)
3	0.000890596	10.10.10.111	10.10.10.112	DNS	83	Standard query 0xcaf2 A definitely-not-evil.com
4	0.000914591	10.10.10.112	10.10.10.111	ICMP	111	Destination unreachable (Port unreachable)
5	0.006707623	10.10.10.111	10.10.10.112	DNS	83	Standard query 0xcaf2 A definitely-not-evil.com
6	0.006736745	10.10.10.112	10.10.10.111	ICMP	111	Destination unreachable (Port unreachable)
7	0.007498646	10.10.10.111	10.10.10.112	DNS	83	Standard query 0xcaf2 A definitely-not-evil.com
8	0.007518496	10.10.10.112	10.10.10.111	ICMP	111	Destination unreachable (Port unreachable)
9	0.007809595	10.10.10.111	10.10.10.112	DNS	83	Standard query 0xcaf2 A definitely-not-evil.com
10	0.007822347	10.10.10.112	10.10.10.111	ICMP	111	Destination unreachable (Port unreachable)
11	4.650317686	PcsCompu_74:9a:8e	PcsCompu_86:38:14	ARP	60	Who has 10.10.10.112? Tell 10.10.10.111
12	4.650349444	PcsCompu_86:38:14	PcsCompu_74:9a:8e	ARP	42	10.10.10.112 is at 08:00:27:86:38:14
13	5.140308459	PcsCompu_86:38:14	PcsCompu_74:9a:8e	ARP	42	Who has 10.10.10.111? Tell 10.10.10.112
14	5.140888278	PcsCompu_74:9a:8e	PcsCompu_86:38:14	ARP	60	10.10.10.111 is at 08:00:27:74:9a:8e

After that, this malware will try to contact back to its C2 which is ‘definitely-not-evil.com’

Time ...	Process Name	PID	Operation	Path
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\ucrtbase.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\msvcp_win.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\gdi32full.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\gdi32.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\user32.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\imm32.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\imm32.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\imm32.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Users\IEUser\AppData\Roaming\stage2.exe
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\bcryptprimitives.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\cryptbase.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\sspicli.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\rpcrt4.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\SysWOW64\sechost.dll
2:54:0...	Unknown.exe	1528	CreateFile	C:\Users\IEUser\AppData\Roaming\stage2.exe
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\apppatch\sysmain.sdb
2:54:0...	Unknown.exe	1528	CreateFile	C:\Windows\apppatch\sysmain.sdb

In ProcMon, there is one special log entry where Unknown.exe create new file named `stage2` in path `C:\Users\IEUser\AppData\Roaming\stage2.exe`.

Static Code analysis

In order to investigate more, manual static code analysis would be pretty standard practice.

Main / subroutine

```
401150 ; ============== S U B R O U T I N E ============================
401150
401150
401150                  public start
401150 start            proc near
401150                  nop
401151                  push    67616C66h
401156                  push    735F697Bh
40115B                  push    5F796174h
401160                  push    5F74756Fh
401165                  push    5F6F6F74h
40116A                  push    6574616Ch
40116F                  push    746F675Fh
401174                  push    746F6E5Fh
401179                  push    676E6968h
40117E                  push    5F6E695Fh
401183                  push    625F796Dh
401188                  push    6E696172h
40118D                  push    '}'
40118F                  mov     ecx, 0Dh
401194
401194 loc_401194:                              ; CODE XREF: start+45↓j
```

For the subroutine part of the malware, the engineer use lot of `push` as part of his/her technique to hide string in program stack.

Converted / unhide string

```
401150 ; =============== S U B R O U T I N E =======================
401150
401150
401150                 public start
401150 start           proc near
401150                 nop
401151                 push    'galf'
401156                 push    's_i{'
40115B                 push    '_yat'
401160                 push    '_tuo'
401165                 push    '_oot'
40116A                 push    'etal'
40116F                 push    'tog_'
401174                 push    'ton_'
401179                 push    'gnih'
40117E                 push    '_ni_'
401183                 push    'b_ym'
401188                 push    'niar'
40118D                 push    '}'
40118F                 mov     ecx, 0Dh
401194
401194 loc_401194:                             ; CODE XREF: start+45↓j
```

Available strings

Address	Length	Type	String
.rdata:0040...	00000008	C	AppData
.rdata:0040...	0000000B	C	stage2.exe
.rdata:0040...	00000013	C	Im totally malware
.rdata:0040...	00000014	C	totally not malware
.rdata:0040...	0000000D	C	KERNEL32.dll
.rdata:0040...	0000000B	C	USER32.dll
.data:00403...	00000012	C	mmaletyoufinishbut

These are all available string analyze using IDA.