FBI FLASH

FBI LIAISON ALERT SYSTEM
#A-000044-MW

The following information was obtained through FBI investigations and is provided in accordance with the FBI's mission and policies to prevent and protect against federal crimes and threats to the national security.

This Flash has been released TLP:Green: The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

There is no additional information available on this topic at this time.

SUMMARY

The FBI is providing the following information with **HIGH confidence:**

Destructive malware used by unknown computer network exploitation (CNE) operators has been identified. This malware has the capability to overwrite a victim host's master boot record (MBR) and all data files. The overwriting of the data files will make it extremely difficult and costly, if not impossible, to recover the data using standard forensic methods. Analysis of this malware is presented to provide the computer network defense (CND) community with indicators of this malware.

TECHNICAL DETAILS

The FBI is providing the following information with **HIGH confidence:**

This group uses some custom tools that should be immediately flagged if detected, reported to FBI CYWATCH, and given highest priority for enhanced mitigation.

The aforementioned actors have used identified domains names and IP addresses as both source and/or destination IPs. The FBI is distributing the indicators associated with this attack to enable network defense activities and reduce the risk of similar attacks in the future. The FBI has high confidence that these indicators are being used by CNE operators for further network exploitation. The FBI recommends that your organization help victims identify and remove the malicious code.

Below are descriptions of malware and associated malware signatures:
The malware has the following characteristics:

File: d1c27ee7ce18675974edf42d4eea25c6.bin
Size: 268579 bytes (262.3 KB)

MD5: D1C27EE7CE18675974EDF42D4EEA25C6
PE Compile Time: 2014-11-22 00:06:54
Language pack of resource section: Korean

The original filename of this file is unknown, but it was likely “diskpartmg16.exe”. This file serves as a dropper. It drops destructive malware, “igfxtrayex.exe”. When the dropper file was executed, it started a second instance of itself with “-i” as an argument, then terminated.

The second instance of the dropper file installed itself as the “WinsSchMgmt” service with “-k” as a command line argument, started the service, then terminated.

The “WinsSchMgmt” service executed the file with “-k” as an argument, which started another instance of the file using “-s” as an argument.

The “-s” instance dropped and executed “igfxtrayex.exe”, created “net_ver.dat”, and began generating network traffic over TCP ports 445 and 139 to victim IP addresses.

The following files were added:
C:\Documents and Settings\User\Desktop\igfxtrayex.exe
C:\WINDOWS\system32\net_ver.dat

The following strings of interest were in this dropper file:

- - - BEGIN STRINGS - - -
recdiscm32.exe
taskhosts64.exe
taskchg16.exe
rdpshellex32.exe
mobsynclm64.exe
comon32.exe
diskpartmg16.exe
dpnsvr16.exe
expandmn32.exe
hwrcompsvc64.exe
cmd.exe /q /c net share shared$ /delete
\\%\admin$\syswow64
\\%s\admin$\system32
cmd.exe /q /c net share shared$=%SystemRoot%
cmd.exe /q /c net share shared$=%SystemRoot% /GRANT:everyone, FULL
RasSecurity
RasMgrp
cmd.exe /c wmic.exe /node: ”%s” /password: “%s” PROCESS CALL CREATE “%s” >

%s
WinsSchMgmt
Windows Schedule Management Service
- - -END STRINGS - - -

File: net_ver.dat
Size: 4572 bytes (4.5 KB)
MD5: 93BC819011B2B3DA8487F964F29EB934

This is a configuration file containing what appear to be hostnames, IP addresses, and the number 2. Entries in the file have the structure “HOSTNAME | IP Address | 2”. The victim IP addresses in this file correspond with the victim IP addresses listed under the file with MD5 hash D1C27EE7CE18675974EDF42D4EEA25C6 (noted above).

File: igfxtrayex.exe
Size: 249856 bytes (244.0 KB)
MD5: 760c35a80d758f032d02cf4db12d3e55
PE Compile Time: 2014-11-24 04:11:08
Language pack of resource section: Korean

This file is destructive malware: a disk wiper with network beacon capabilities. If “igfxtrayex.exe” is run with no parameters, it creates and starts a copy of itself with the “–i” argument. After 10 minutes, the “igfxtrayex.exe” makes three copies of itself and places them in the same directory it was executed from. These copies are named according to the format “taskhostXX.exe” (where X is a randomly generated ASCII character). These copies are then executed, each with a different argument (one being “-m”, one being “-d” and the other “-w”). Network connection attempts are made to one of three hard-coded IP addresses in a random order to either port 8080 or 8000. If a connection to the IP address cannot be made, it attempts to connect to another of the three IP addresses, until connections to all three IP addresses have been attempted. The following command-line string is then executed: “cmd.exe /c net stop MSExchangeIS /y”. A 120 minute (2 hour) sleep command is issued after which the computer is shutdown and rebooted.

File: iissvr.exe
Size: 114688 bytes (112.0 KB)
MD5: e1864a55d5ccb76af4bf7a0ae16279ba
PE Compile Time: 2014-11-13 02:05:35
Language pack of resource section: Korean

This file when executed starts a listener on localhost port 80. It has 3 files contained in the resource section, all xor’d with 0x63.

File: usbdrv3_32bit.sys
Size: 24280 bytes (23.7 KB)
MD5: 6AEAC618E29980B69721158044C2E544
PE Compile Time: 2009-08-21 06:05:32

This SYS file is a commercially available tool that allows read/write access to files and raw disk sectors for user mode applications in Windows 2000, XP, 2003, Vista, 2008 (32-bit). It is dropped from resource ID 0x81 of "igfxtrayex.exe".

File usbdrv3_64bit.sys
Size: 28120 bytes (27.5 KB)
MD5: 86E212B7FC20FC406C692400294073FF
PE Compile Time: 2009-08-21 06:05:35

This SYS file is a also a commercially available tool that allows read/write access to files and raw disk sectors for user mode applications in Windows 2000, XP, 2003, Vista, 2008 (64-bit). It is dropped from resource ID 0x83 of "igfxtrayex.exe".

RECOMMENDED STEPS FOR INITIAL MITIGATION

The following Snort signature can be used to detect the beacon traffic, though by the time the beacons occur, the destructive process of wiping the files has begun:

Alert tcp any any - > [88.53.215.64, 217.96.33.164, 203.131.222.102] [8080, 8000] (msg: "wiper_callout"; dsize:42; content: "|ff ff ff ff|"; offset: 26; depth: 4; sid: 314;)

The following YARA signatures will detect this malware on the host:

```
rule unknown_wiper_str{

meta: unique string in wiper malware

    strings:

        $STR1 =
"#99E2428CCA4309C68AAF8C616EF3306582A64513E55C786A864BC83DAFE0C78585B692047273B0E55275102C66"
fullword nocase

        $MZ = "MZ"

    condition:
```

```
        $MZ at 0 and $STR1

}

rule unknown_wiper_IPs{

meta:  unique IPs in wiper malware

    strings:

        $IP1 = "203.131.222.102" fullword nocase
        $IP2 = "217.96.33.164" fullword nocase
        $IP3 = "88.53.215.64" fullword nocase
        $MZ = "MZ"

    condition:

        $MZ at 0 and all of them
}

rule unknown_wiper_error_strings{

meta: unique custom error debug strings discovered in the wiper malware

    strings:

        $ERR1 = "$MFT Record read failed." fullword nocase
        $ERR2 = "Drive Boot Sector read failed." fullword nocase
        $ERR3 = "SetFilePointer failed." fullword nocase
        $MZ = "MZ"

  condition:

        $MZ at 0 and all of them
}
```

Reporting Notice

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.