VALKYRIE COMODO

Summary

File Name: bull_output5C3A480.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

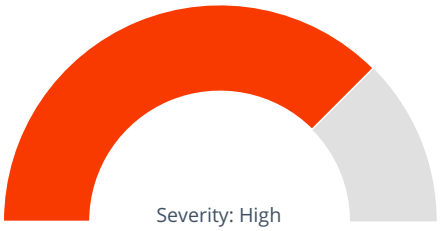
SHA1: 45dc9121c36e92a2dd1389a44c970c23ea31ded0

MD5: 15a91944434e12d73bb7306ad3ccbfee

MALWARE

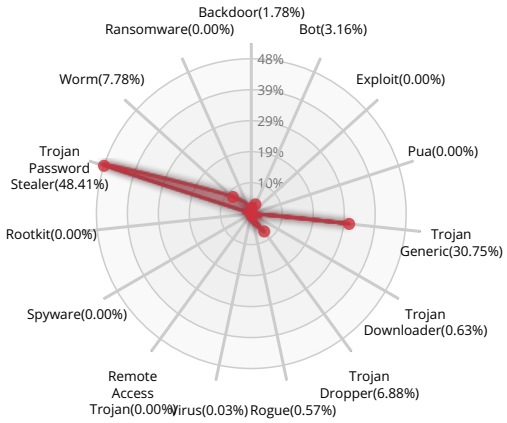
Valkyrie Final Verdict

DETECTION SECTION

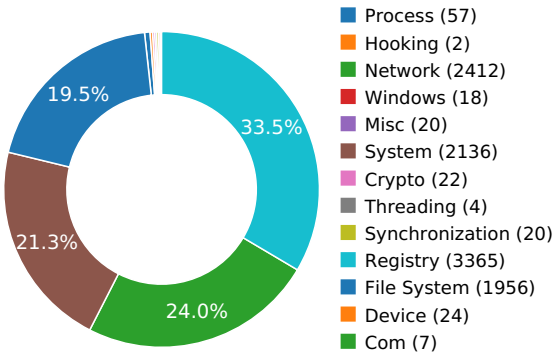


Verdict: Malware

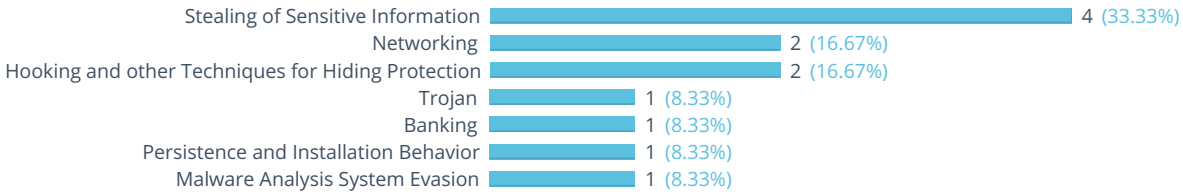
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

TROJAN

Exhibits behavior characteristic of Pony malware — Show sources

NETWORKING

HTTP traffic contains suspicious features which may be indicative of malware related traffic — Show sources

Performs some HTTP requests — Show sources

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers — Show sources

Collects information about installed applications — Show sources

Harvests credentials from local FTP client softwares — Show sources

Harvests information related to installed mail clients — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

Executed a process and injected code into it, probably while unpacking — Show sources

BANKING

Contacts C&C server HTTP check-in (Banking Trojan) — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Deletes its original binary from disk

MALWARE ANALYSIS SYSTEM EVASION

A process created a hidden window — Show sources

VALKYRIE COMODO

Behavior Graph

12:38:45 **12:39:49**

PID 2996

12:38:45 **Create Process** The malicious file created a child process as 45dc9121c36e92a2dd1389a44c970c23ea31ded0.exe **(PPID 1888)**

12:39:12 NtAllocateVirtualMem

12:39:12 Create Process

12:39:13 NtResumeThread

PID 2680

12:39:18 **Create Process** The malicious file created a child process as 45dc9121c36e92a2dd1389a44c970c23ea31ded0.exe **(PPID 2996)**

12:39:21 12:39:21 RegQueryValueExA **[71 times]**

12:39:24 RegSetValueExA

12:39:24 12:39:26 NtReadFile **[16 times]**

12:39:39 ShellExecuteExW

PID 2832

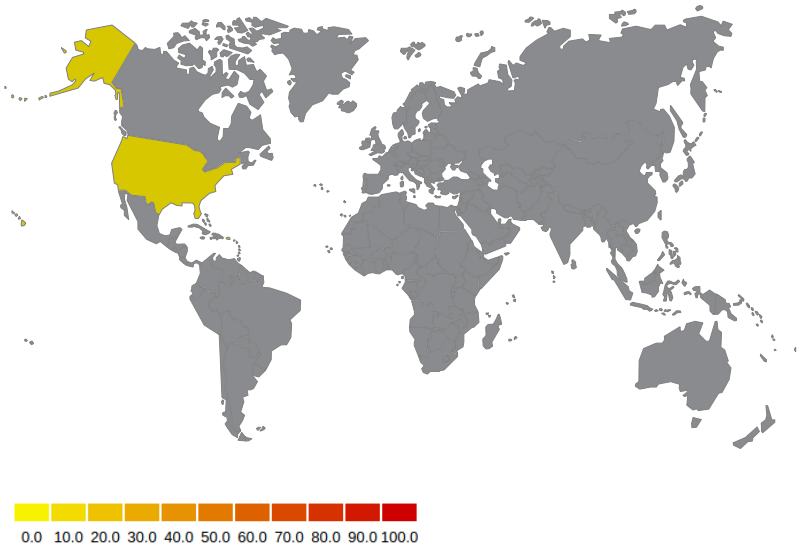
12:39:48 **Create Process** The malicious file created a child process as cmd.exe **(PPID 2680)**

12:39:49 DeleteFileW

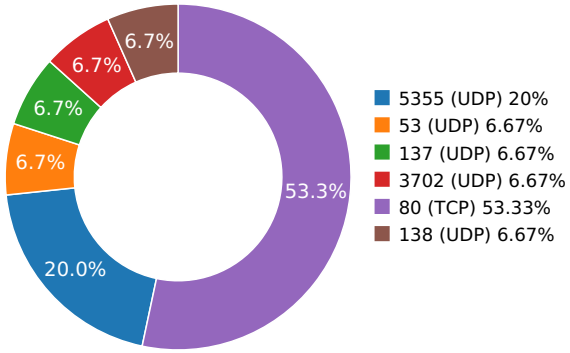
Behavior Summary

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Communications, Inc.	Malware Process
elta-th.com	5.56.133.98	United States	35017	1 Gbits Com	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
elta-th.com	80	POST	1.0	Mozilla/4.0 (compatible; MSIE 5...	3	
Path: /zenn/bull/gate.php **URI:** http://elta-th.com/zenn/bull/gate.php						
elta-th.com	80	GET	1.0	Mozilla/4.0 (compatible; MSIE 5...	1	
Path: /zenn/bull/shit.exe **URI:** http://elta-th.com/zenn/bull/shit.exe						
elta-th.com	80	GET	1.0	Mozilla/4.0 (compatible; MSIE 5...	1	
Path: /cgi-sys/suspendedpage.cgi **URI:** http://elta-th.com/cgi-sys/suspendedpage.cgi						

DNS QUERIES

Request	Type
elta-th.com	A
Answers - 5.56.133.98 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
42.0570130348	Sandbox	5.56.133.98	80
47.3687679768	Sandbox	5.56.133.98	80
52.6983149052	Sandbox	5.56.133.98	80
53.0379650593	Sandbox	5.56.133.98	80
53.2589731216	Sandbox	5.56.133.98	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.11542105675	Sandbox	224.0.0.252	5355
3.2094950676	Sandbox	192.168.56.255	137
3.24683094025	Sandbox	224.0.0.252	5355
3.25459909439	Sandbox	239.255.255.250	3702
5.81853294373	Sandbox	224.0.0.252	5355
9.25352811813	Sandbox	192.168.56.255	138
41.863368988	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 645ccdde38bb039eb271a4f120e6be5f **SHA-1 :** 475a264964d84a2c6c335202262fa6c76275a515 **SHA-256 :** a9b45e98f41bfcc23bc82cf17b3381b9820a2be6c **SHA-512 :** 0f5aa71c7c0b1a574c4a6c306a24006ad175e7c8 **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Local\Temp\24915203.Bat	**Type :** ASCII text, with CRLF, CR line terminators **MD5 :** 3880eeb1c736d853eb13b44898b718ab **SHA-1 :** 4eec9d50360cd815211e3c4e6bdd08271b6ec8e6 **SHA-256 :** 936d9411d5226b7c5a150ecaf422987590a8870c **SHA-512 :** 3eaa3dddd7a11942e75acd44208fbe3d3ff8f400 **Size :** 0.094 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** de20f795b0ea29cbcb8daf8951530db4 **SHA-1 :** 81d7e8a0197a0ea9eba76e4dc856d10aa5ec04d9 **SHA-256 :** f891c989c74d22028cc0dfcd564c186fe6857592c **SHA-512 :** 06ed0fdb0abfcdbc16a7f5adb92ed0c59ba788f08 **Size :** 180.224 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 2ed7b584633888df7f0114fa4ac6dc69 **SHA-1 :** fa8067b3241b8d9258d9fc88f5bd80fca5433b10 **SHA-256 :** 69a0d29dc846c82d785231dbf94e4c4b731ad588 **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1f **Size :** 32.768 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	bull_output5C3A480.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	45dc9121c36e92a2dd1389a44c970c23ea31ded0
MD5:	15a91944434e12d73bb7306ad3ccbfee
First Seen Date:	2017-03-07 08:54:56.269575 (2 years ago)
Number Of Clients Seen:	11
Last Analysis Date:	2017-03-07 08:54:56.269575 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	3
Compilation Time Stamp	0x58ADB83B [Wed Feb 22 16:11:39 2017 UTC]
Translation	0x0409 0x04b0
LegalCopyright	HP
InternalName	Border2
FileVersion	7.07.0007
CompanyName	Denim
LegalTrademarks	HP
Comments	HP
ProductName	HP
ProductVersion	7.07.0007
FileDescription	HP
OriginalFilename	Border2.exe
Entry Point	0x401228 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	245760
Sha256	af6b8c6d776f2b74ba22e5f9c1b4f898d8b091ecc9b01dd719526b83f2682adf
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x389a4	0x39000	5.083291	-
.data	0x3a000	0x27e0	0x1000	0.000000	-
.rsrc	0x3d000	0x928	0x1000	2.313459	-

PE Imports

- MSVBVM60.DLL
  - _CIcos
  - _adj_fptan
  - __vbaVarMove
  - __vbaFreeVar
  - __vbaGosubReturn
  - __vbaFreeVarList
  - _adj_fdiv_m64
  - _adj_fprem1
  - __vbaSetSystemError
  - __vbaHresultCheckObj

- None
- _adj_fdiv_m32
- _adj_fdiv_m16i
- _adj_fdivr_m16i
- _CIsin
- __vbaChkstk
- __vbaGosubFree
- EVENT_SINK_AddRef
- None
- DllFunctionCall
- None
- _adj_fpatan
- None
- EVENT_SINK_Release
- _CIsqrt
- EVENT_SINK_QueryInterface
- __vbaExceptHandler
- None
- _adj_fprem
- _adj_fdivr_m64
- __vbaGosub
- None
- __vbaFPException
- _CIlog
- __vbaNew2
- _adj_fdiv_m32i
- _adj_fdivr_m32i
- _adj_fdivr_m32
- _adj_fdiv_r
- None
- None
- __vbaVarDup
- _CIatan
- __vbaStrMove
- _allmul
- _CItan
- _CIexp
- __vbaFreeObj
- __vbaFreeStr

PE Resources

RT_ICON
RT_GROUP_ICON
RT_VERSION

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS


Computer
11:39 AM


Computer
11:39 AM


Computer
11:38 AM