Cridex Analysis using Volatility - by Andre' DiMino - samples and memory analysis resources

Archived: 2026-04-05 23:38:03 UTC

Andre' DiMino posted an excellent analysis of Cridex banking malware using Volatility on **sempersecurus.blogspot.com** and if you wish to repeat his steps or interested in this malware, I am posting the corresponding samples. Cridex is a complex financial trojan and is being distributed via spam messages (carrying exe files in zipped attachments) and Blackhole Exploit kit.
The messages have various themes - from UPS, Fedex, USPS to Groupon deals and "HP-scan" and other lures. Some message screenshots and corresponding malware are posted below.

If you are interested in memory analysis, please see the resource section of this post (links to the tools: Volatility, Mandiant Redline, memory dumps and other memory analysis done by Andre' and other researchers)

Download

Download all files listed below (email me if you need the password)

Analysis Preview

Exerpt: Read the full version at **sempersecurus.blogspot.com - Cridex Analysis using Volatility**

> Using the Volatility 'plist' command, we can see a list of the running processes. However it's instructive to use this in conjunction with the 'psscan' command in order to see those processes that have terminated, are unlinked, or hidden. In this case, no discrepancies between the two commands jump out at me, but I do notice a couple of things. First, I see a process, ***reader_sl.exe, PID1640*** start exactly at the same time as its parent process, ***explorer.exe, PID1484***. I see that the parent process ID for *explorer.exe* is *1464*, which is not listed in either 'pslist' or 'psscan'. *reader_sl.exe* is a supposedly a safe process, associated with Adobe Speed Launcher, but the launch chain for this seems odd, so I'll

keep note of this for now. Next, I see a second*wuauclt.exe* process start about 15 seconds after the first. This isn't a major flag, but just something to note.

```
sportivo@saturn:~/programs/Volatility$ python vol.py -f /home/ezio77/cridex.vmem --profile=WinXPSP2x86 pslist -P
Volatile Systems Volatility Framework 2.1_rc3
Offset(P)  Name                PID   PPID   Thds     Hnds   Sess  Wow64 Start                  Exit
---------- ---------------- ------ ------ ------ -------- ------ ------ ------------------- ----------
0x025c89c8 System                4      0     53      240 ------      0
0x024f1020 smss.exe            368      4      3       19 ------      0 2012-07-22 02:42:31
0x024a0598 csrss.exe           584    368      9      326      0      0 2012-07-22 02:42:32
0x02498700 winlogon.exe        608    368     23      519      0      0 2012-07-22 02:42:32
0x0202ab28 services.exe        652    608     16      243      0      0 2012-07-22 02:42:32
0x0202a3b8 lsass.exe           664    608     24      330      0      0 2012-07-22 02:42:32
0x02511360 svchost.exe         824    652     20      194      0      0 2012-07-22 02:42:33
0x02029ab8 svchost.exe         908    652      9      226      0      0 2012-07-22 02:42:33
0x025001d0 svchost.exe        1004    652     64     1118      0      0 2012-07-22 02:42:33
0x023dfda0 svchost.exe        1056    652      5       60      0      0 2012-07-22 02:42:33
0x02495650 svchost.exe        1220    652     15      197      0      0 2012-07-22 02:42:35
0x023dea70 explorer.exe       1484   1464     17      415      0      0 2012-07-22 02:42:36
0x020b17b8 spoolsv.exe        1512    652     14      113      0      0 2012-07-22 02:42:36
0x0207bda0 reader_sl.exe      1640   1484      5       39      0      0 2012-07-22 02:42:36
0x022e8da0 alg.exe             788    652      7      104      0      0 2012-07-22 02:43:01
0x023fcda0 wuauclt.exe        1136   1004      8      173      0      0 2012-07-22 02:43:46
0x0225bda0 wuauclt.exe        1588   1004      5      132      0      0 2012-07-22 02:44:01
```

pslist command

```
sportivo@saturn:~/programs/Volatility$ python vol.py -f /home/ezio77/cridex.vmem --profile=WinXPSP2x86 psscan
Volatile Systems Volatility Framework 2.1_rc3
Offset(P)  Name                PID   PPID PDB        Time created         Time exited
---------- ---------------- ------ ------ ---------- ------------------- -------------------
0x02029ab8 svchost.exe         908    652 0x079400e0 2012-07-22 02:42:33
0x0202a3b8 lsass.exe           664    608 0x079400a0 2012-07-22 02:42:32
0x0202ab28 services.exe        652    608 0x07940080 2012-07-22 02:42:32
0x0207bda0 reader_sl.exe      1640   1484 0x079401e0 2012-07-22 02:42:36
0x020b17b8 spoolsv.exe        1512    652 0x079401c0 2012-07-22 02:42:36
0x0225bda0 wuauclt.exe        1588   1004 0x07940200 2012-07-22 02:44:01
0x022e8da0 alg.exe             788    652 0x07940140 2012-07-22 02:43:01
0x023dea70 explorer.exe       1484   1464 0x079401a0 2012-07-22 02:42:36
0x023dfda0 svchost.exe        1056    652 0x07940120 2012-07-22 02:42:33
0x023fcda0 wuauclt.exe        1136   1004 0x07940180 2012-07-22 02:43:46
0x02495650 svchost.exe        1220    652 0x07940160 2012-07-22 02:42:35
0x02498700 winlogon.exe        608    368 0x07940060 2012-07-22 02:42:32
0x024a0598 csrss.exe           584    368 0x07940040 2012-07-22 02:42:32
0x024f1020 smss.exe            368      4 0x07940020 2012-07-22 02:42:31
0x025001d0 svchost.exe        1004    652 0x07940100 2012-07-22 02:42:33
0x02511360 svchost.exe         824    652 0x079400c0 2012-07-22 02:42:33
0x025c89c8 System                4      0 0x002fe000
```

psscan command

The next useful Volatility command that I use for malware analysis is the 'connections' and the 'connscan'commands. Again, running both of these will allow you to see variances, as 'connscan' will show artifacts from previous connections.

File information

Cridex file analyzed by Andre DiMino

File: readme.exe

Size: 112096

MD5: 734AADD62D0662256A65510271D40048

Other cridex samples:

File: about.exe
Size: 160768
MD5: C497B4D6DFADD4609918282CF91C6F4E

File: **HP_Scan_N989397452.exe**
Size: 80896
MD5: E187763C92E2ACC6BB1C804309EBB381

File: **Booking_Confirmation_08012012.exe**
Size: 98304
MD5: 213D5022047029071AFD372302E07DD8

File: UPS_Label_N8882342.exe
Size: 145408
MD5: 43CD850FCDADE4330A5BEA6F16EE971C

Resources

Memory Analysis links and dumps (in no particular order)

Volatility (Free. Linux)

- Sharing of Forensically Interesting Objects by Andre' DiMino
- Andre' DiMino Using "volatility" to study the CVE-2011-0611 Adobe Flash 0-day
- Zeus Analysis in Volatility 2.0 by malwarereversing
- Abstract Memory Analysis: Zeus Encryption Keys MNIN Security Blog Coding, Reversing, Exploiting
- Carberp Analysis via Volatility by Evilcry - Giuseppe Bonfa
- Volatility 2.0: Timeliner, RegistryAPI, evtlogs and more by JL
- toolsmith: Memory Analysis with DumpIt and Volatility
- ShmooCon 2012: Android Mind Reading: Memory Acquisition and Analysis with DMD and Volatility

Mandiant Redline
(Free. Windows. It is am easy to use new tool with a clean nice user interface, powerful features and integration with IOC - Indicators of Compromise tool)

- Analyze Memory of an infected system with Mandiant's Redline by Lenny Zeltser
- Mandiant Using Redline & OpenIOC to Build Effective Indicators
- SANS blog, Live Memory Forensic Analysis

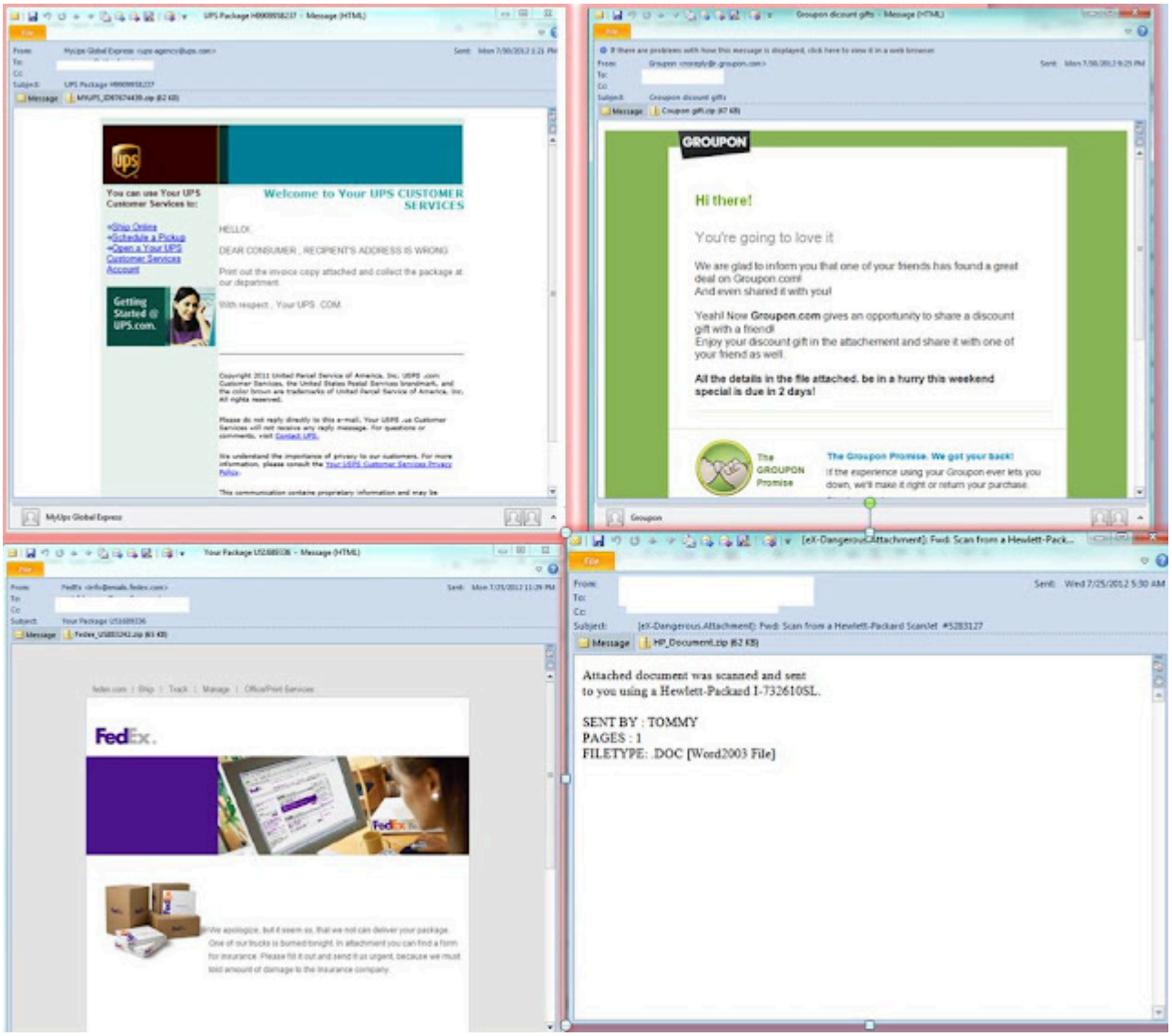
A few public memory dumps are here http://code.google.com/p/volatility/wiki/PublicMemoryImages

Cridex distribution

Email examples

Some of the possible subjects

- Groupon dicount gifts
- UPS Tracking Number H9942472682
- United Postal Service Tracking Number H5642970529
- Fedex Tracking Number
- UPS Your Package H8522250271
- Your Package US168933
- HP-Officejet 10167
- HP Scan 5601



Automatic scans

SHA256: 046a7fac35a29f66e37193a2048f6a324754df131bad07c21f87fc814d7763f5
SHA1: 67e9c32c97b47e058aeee928c4cdc28773883b90
MD5: 734aadd62d0662256a65510271d40048

File size: 109.5 KB (112096 bytes)
File name: 734aadd62d0662256a65510271d40048
File type: Win32 EXE
Detection ratio: 36 / 42
Analysis date: 2012-06-26 15:00:58 UTC (1 month, 1 week ago)
01
More details
Antivirus Result Update
AhnLab-V3 Win-Trojan/Dapato.112096 20120626
AntiVir Worm/Cridex.E.5 20120626
Antiy-AVL Trojan/Win32.Dapato.gen 20120626
Avast Win32:Dropper-gen [Drp] 20120626
AVG PSW.Generic9.CMJF 20120625
BitDefender Trojan.Generic.KDV.647871 20120626
ClamAV - 20120626
Commtouch W32/Zbot.DQ3.gen!Eldorado 20120626
Comodo UnclassifiedMalware 20120626
DrWeb Trojan.DownLoader6.17427 20120626
Emsisoft Worm.Win32.Cridex!IK 20120626
eSafe Win32.PWS.Zbot.Xs 20120624
F-Prot W32/Zbot.DQ3.gen!Eldorado 20120626
F-Secure Trojan.Generic.KDV.647871 20120626
Fortinet W32/Dapato.BHXH!tr 20120626
GData Trojan.Generic.KDV.647871 20120626
Ikarus Worm.Win32.Cridex 20120626
Jiangmin TrojanDropper.Dapato.ize 20120626
K7AntiVirus Spyware 20120625
Kaspersky Trojan-Dropper.Win32.Dapato.bhxh 20120626
McAfee PWS-Zbot.gen.uh 20120626
McAfee-GW-Edition PWS-Zbot.gen.uh 20120626
Microsoft Worm:Win32/Cridex.E 20120626
NOD32 Win32/AutoRun.Spy.Banker.P 20120626
Norman W32/Injector.AQSI 20120625
nProtect Trojan/W32.Agent.112096.B 20120626
Panda Generic Malware 20120625
PCTools Malware.Cridex 20120626
Rising - 20120626
Sophos Troj/DwnLdr-KAY 20120626
TheHacker Trojan/Dropper.Dapato.bhxh 20120625
TrendMicro TROJ_KRYPTIK.MIC 20120626
TrendMicro-HouseCall TROJ_KRYPTIK.MIC 20120625
VBA32 TrojanDropper.Dapato.bhxh 20120625

VIPRE Trojan.Win32.Generic.pak!cobra 20120626
ViRobot Dropper.A.Dapato.112096 20120626
VirusBuster Worm.AutoRun!tSqW3tx0AYY 20120625

#Cridex worm
==========

SHA256: a7e62a16c47fede2772d4f4bf980cdb58b5d110887e001ab632d7f40159dfa13
SHA1: d186e8ebb104ba0d64ad6052107420debef3da00
MD5: c497b4d6dfadd4609918282cf91c6f4e
File size: 157.0 KB (160768 bytes)
File name: KB00385258.exe / about.exe
File type: Win32 EXE
Tags: peexe upx
Detection ratio: 1 / 41
Analysis date: 2012-08-02 19:53:34 UTC (5 hours, 53 minutes ago)
Kaspersky UDS:DangerousObject.Multi.Generic 20120802

http://hookpublications.com/wp-admin/atbilred.html
http://advancementwowcom.org/main.php?page=19152be46559e39d
http://advancementwowcom.org/w.php?f=14095&e=2
Posted 7 hours, 58 minutes ago by BornSlippy
#cridex

http://tevrom.ro/modules/atbilred.html
http://advancementwowcom.org/main.php?page=19152be46559e39d
http://advancementwowcom.org/w.php?f=14095&e=2
Posted 8 hours, 9 minutes ago by BornSlippy
trojan Cridex, payload of Blackhole exploit kit at hxxp://unboxhibernation.org/w.php?f=14095&e=2

http://camas.comodo.com/cgi-bin/submit?
file=a7e62a16c47fede2772d4f4bf980cdb58b5d110887e001ab632d7f40159dfa13

==========

SHA256: 65bd088579107f13bf5e3aaba25b07b413343a823e7a3499d907b1bf564f36e5
SHA1: 7263fe0d3a095d59c8e0c895a9c585e343e7141c
MD5: 43cd850fcdade4330a5bea6f16ee971c
File size: 142.0 KB (145408 bytes)
File name: 43cd850fcdade4330a5bea6f16ee971c
File type: Win32 EXE
Tags: peexe
Detection ratio: 29 / 41
Analysis date: 2012-08-02 17:21:11 UTC (9 hours, 54 minutes ago)
04

More details

Antivirus Result Update

AhnLab-V3 - 20120802

AntiVir TR/Spy.145408.64 20120802

Antiy-AVL - 20120802

Avast Win32:Downloader-PUU [Trj] 20120802

AVG SHeur4.AKQG 20120802

BitDefender Trojan.Generic.KD.684302 20120802

ByteHero - 20120723

CAT-QuickHeal - 20120802

ClamAV - 20120802

Commtouch W32/Trojan3.DWW 20120802

Comodo TrojWare.Win32.Trojan.Agent.Gen 20120802

DrWeb Trojan.Necurs.21 20120802

Emsisoft Trojan.Win32.Buzus!IK 20120802

eSafe Win32.Trojan 20120802

ESET-NOD32 Win32/AutoRun.Spy.Banker.R 20120802

F-Prot W32/Trojan3.DWW 20120802

F-Secure Trojan-Spy:W32/Agent.DUCE 20120802

Fortinet W32/Palevo.EYYX!worm 20120802

GData Trojan.Generic.KD.684302 20120802

Ikarus Trojan.Win32.Buzus 20120802

Jiangmin Backdoor/RBot.obc 20120802

K7AntiVirus Riskware 20120802

Kaspersky P2P-Worm.Win32.Palevo.eyyx 20120802

McAfee PWS-Zbot.gen.ajh 20120802

McAfee-GW-Edition Generic.dx!bf3x 20120802

Microsoft Worm:Win32/Cridex.E 20120802

Norman W32/Troj_Generic.DDRRO 20120802

nProtect Worm/W32.Palevo.145408.AE 20120802

Panda - 20120802

Rising - 20120802

Sophos Troj/Agent-XGF 20120802

SUPERAntiSpyware - 20120802

Symantec W32.Cridex 20120802

TheHacker - 20120801

TotalDefense - 20120802

TrendMicro TROJ_INJECTR.PAL 20120802

TrendMicro-HouseCall TROJ_INJECTR.PAL 20120802

VBA32 - 20120802

VIPRE Trojan.Win32.Generic!BT 20120802

ViRobot Worm.Win32.A.P2P-Palevo.145408.AD 20120802

VirusBuster - 20120802
Comments
Votes
Additional information
Behavioural information
#backdoor bot

http://keaaushoppingcenter.com/mail.htm
online-cammunity.ru:8080/forum/showthread.php?page=5fa58bce769e5c2c
online-cammunity.ru:8080/forum/w.php?f=182b5&e=2

File uploaded for analysis to ;

http://jsunpack.jeek.org/dec/go?report=07777d69d6d6f5e180519988ad3df85613285e58

==========

SHA256: c11a3d4f4630211cd458a022fa8c346d8a1a836561897e9ba6b4098605cf49b7
SHA1: ef006795e39b4cc7469107c0b04d37ca492e062a
MD5: 213d5022047029071afd372302e07dd8
File size: 96.0 KB (98304 bytes)
File name: Booking_Confirmation_08012012.exe
File type: Win32 EXE
Tags: peexe
Detection ratio: 21 / 41
Analysis date: 2012-08-02 13:31:05 UTC (13 hours, 53 minutes ago)
00
More details
Antivirus Result Update
AhnLab-V3 Win32/Cridex.worm.98304.B 20120802
AntiVir TR/Graftor.385561 20120802
AVG SHeur4.AKTK 20120802
BitDefender Trojan.Generic.KDV.686322 20120802
ByteHero - 20120801
CAT-QuickHeal - 20120802
Commtouch W32/Trojan3.DXI 20120802
DrWeb Trojan.Necurs.20 20120802
Emsisoft Worm.Win32.Cridex!IK 20120802
eSafe - 20120731ESET-NOD32 Win32/AutoRun.Spy.Banker.M 20120802
F-Prot W32/Trojan3.DXI 20120802
F-Secure Trojan.Generic.KDV.686322 20120802
GData Trojan.Generic.KDV.686322 20120802
Ikarus Worm.Win32.Cridex 20120802
Kaspersky Worm.Win32.Cridex.gt 20120802

McAfee PWS-Zbot.gen.ajm 20120802
McAfee-GW-Edition - 20120802
nProtect Trojan.Generic.KDV.686322 20120802
Panda Suspicious file 20120802
Sophos Troj/Cridex-O 20120802
SUPERAntiSpyware - 20120802
Symantec W32.Cridex 20120802
TrendMicro PAK_Generic.012 20120802
TrendMicro-HouseCall PAK_Generic.012 20120802
VIPRE Trojan.Win32.Generic!BT 20120802

==========

SHA256: 76b22b77e5df1134619e8ac3fd6a8c8cf72de879e0c4afbd11ebcaa14bc2a38e
SHA1: d64623b8b5bbfa20bb7a08a43d7fed0e7d503e4f
MD5: e187763c92e2acc6bb1c804309ebb381
File size: 79.0 KB (80896 bytes)
File name: smona_76b22b77e5df1134619e8ac3fd6a8c8cf72de879e0c4afbd11ebcaa14bc2a38e.bin
File type: Win32 EXE
Tags: peexe
Detection ratio: 33 / 40
Analysis date: 2012-08-01 23:38:20 UTC (1 day, 3 hours ago)
06
More details
Antivirus Result Update
AhnLab-V3 Win32/Cridex.worm.80896.C 20120801
AntiVir TR/Cehscok.A 20120801
Antiy-AVL - 20120801
Avast Win32:Kryptik-JJP [Trj] 20120802
AVG Generic28.CNKE 20120801
BitDefender Trojan.Generic.KDV.681199 20120802
ByteHero - 20120723
CAT-QuickHeal Trojan.Yakes.ahur 20120801
ClamAV W32.Trojan.Yakes-25 20120801
Commtouch W32/Falab.F.gen!Eldorado 20120801
Comodo TrojWare.Win32.Kryptik.AITM 20120802
DrWeb Trojan.Necurs.21 20120802
Emsisoft Trojan.Win32.Yakes!IK 20120801
ESET-NOD32 Win32/AutoRun.Spy.Banker.R 20120801
F-Prot W32/Falab.F.gen!Eldorado 20120801
F-Secure Trojan:W32/Injector.AA 20120802
Fortinet W32/Kryptik.AB!tr 20120801
GData Trojan.Generic.KDV.681199 20120802

Ikarus Trojan.Win32.Yakes 20120801
Jiangmin Trojan/JboxGeneric.kue 20120801
K7AntiVirus Trojan 20120801
Kaspersky Trojan.Win32.Yakes.ahur 20120801
McAfee PWS-Zbot.gen.air 20120802
McAfee-GW-Edition PWS-Zbot.gen.air 20120801
Microsoft Worm:Win32/Cridex.E 20120802
Norman W32/Troj_Generic.DBZPN 20120801
nProtect Trojan.Generic.KDV.681199 20120801
Panda Generic Trojan 20120801
Rising - 20120801
Sophos Troj/Katusha-AG 20120802
SUPERAntiSpyware - 20120801
Symantec W32.Cridex 20120801
TheHacker Trojan/Yakes.ahur 20120801
TotalDefense - 20120801
TrendMicro TROJ_INJECTR.VYQ 20120802
TrendMicro-HouseCall TROJ_INJECTR.VYQ 20120801
VIPRE Trojan.Win32.Generic!BT 20120802
ViRobot Trojan.Win32.A.Yakes.80896.D 20120801

http://bartblaze.blogspot.com/2012/07/scan-from-hewlett-packard-scanjet.html
Posted 1 week ago by bartblaze
