

Forum: [Hack Forums](#)

Thread: [RDG Tejon Crypter V0.7 Private](#)

Apocalypse - October 5, 2010, 6:58 pm

[img]http://i39.[censored].com/14tuayx.png[/img]

- *Anti-Debugger
- *Anti-Sandboxie
- *Anti-virtualpc
- *Realig Sections
- *Anti-IDA Debugger
- *Anti-CWSandbox
- *Anti-Norman Sandbox
- *Anti-Anubis
- *OEP Stolen Bytes (Enhanced)
- *Checksum CRC
- *Anti-OllyDbg
- *Anti-ThreatExpert
- *Anti-JoeBox
- *Anti-VMWARE
- *Anti-VirtualBOX
- *Anti-Debugger2
- *Overlay support (EOF Data)
- *Sleep Sec. Run program after x Seconds.
- *Exceptions (0 to 1000)
- *Get All Privileges
- *Change Icon (Enhanced)

- *OEP Stolen Bytes (Enhanced)
- *Anti Virtual Machine (Max) = Heuristic
- *Anti-SunBelt Sandbox
- *Anti Deep-Freeze
- *Anti-Returnil Vistual System
- *Anti-Malware Defender
- *Anti-Wine(Linux)
- *Anti-Xen Virtual Machine
- *Password Protect
- *Execute With Command Line (parameters)
- *UnHook All API
- *Anti-Attach Loader (Protect RDG Loder)
- *Execute as NT AUTHORITY\SYSTEM

- +v0.7
- *Extract RDG Loader (Stub)
- *Use External Stub (RDG Loader)
- *Anti-Shadow User Pro
- *Anti-Clean Slate
- *Anti Sandbox (Fortres)
- *Run as Fake Process

- *Delete Me (Execute & Delete RDG Loader)
- *I Will Scan w/ AV Online (Use this option for scan yours Protected files with AV's Online :)
- *Anti JoeBox (Enhanced)
- *Anti-Anubis (Enhanced)
- *Anti-CWSandbox (Enhanced)
- *Sleep Sec. Run program after x Seconds. 0 to 999 (Enhanced)
- *Process Ghost
- *Change Process Name

Ask nicely in this thread for download link (Do not PM me)
A 100 post count limit is required. No exceptions ... Unless you're HF L33t

This is for trying to stay FUD/UD longer.

File Info:
Detection rate: 0 on 16 (0%)
Status: CLEAN

Detections

a-squared -
Avast -
AVG -
Avira AntiVir -
BitDefender -
ClamAV -
Comodo -
Dr.Web -
F-PROT6 -
Ikarus T3 -
Kaspersky -
NOD32 -
Panda -
TrendMicro -
VBA32 -
VirusBuster -

Scan report generated by
<http://NoVirusThanks.org>

Download link:
[deleted]
?

zer0day - October 5, 2010, 7:12 pm

Nice try! INFECTED!!!

File Info

Report date: 2010-10-06 03:25:35 (GMT 1)
File name: rdg-tejon-crypter-v0-7-private
File size: 403191 bytes
MD5 Hash: c4d38e050319f09e1cd75bf775bfc696

Status: INFECTED

a-squared - Backdoor.Win32.Poison!IK
Avast - Win32:Malware-gen
AVG - Dropper.Generic2.AXZT
Avira AntiVir - TR/Dropper.Gen
BitDefender - Trojan.Generic.4833946
ClamAV -
Comodo -
Dr.Web -
F-PROT6 -
Ikarus T3 - Backdoor.Win32.Poison
Kaspersky - Backdoor.Win32.Poison.bxkr
NOD32 -
Panda -
TrendMicro -
VBA32 -
VirusBuster - Trojan.VB.KSKH

NoVirusThanks.org

[illegible]
$$[==]$$

Table of Contents

[==]

- General information
- Cannabis C.exe
 - a) Registry Activities
 - b) File Activities

[##]

1. General Information

[##]

[==]

Information about Anubis' invocation

[==]

Time needed: 242 s

Report created: 10/05/10, 15:33:00 UTC

Termination reason: Timeout

Program version: 1.74.3195

[##]

2. Cannabis C.exe

[##]

[==]

General information about this executable

[==]

Analysis Reason: Primary Analysis Subject

Filename: Cannabis C.exe

MD5: c4d38e050319f09e1cd75bf775bfc696

SHA-1: a3545b6d3b906fc1f3d285853b78525155221e74

File Size: 403191 Bytes

Command Line: "C:\Cannabis C.exe"

Process-status

at analysis end: alive

Exit Code: 0

[==]

Load-time DLLs

[==]

Module Name: [C:\WINDOWS\system32\ntdll.dll],

Base Address: [0x7C900], Size: [0x000AF000]

Module Name: [C:\WINDOWS\system32\kernel32.dll],

Base Address: [0x7C800], Size: [0x000F6000]

Module Name: [C:\WINDOWS\system32\MSVBVM60.DLL],

Base Address: [0x73420000], Size: [0x00153000]

Module Name: [C:\WINDOWS\system32\USER32.dll],

Base Address: [0x7E410000], Size: [0x00091000]

Module Name: [C:\WINDOWS\system32\GDI32.dll],

Base Address: [0x77F10000], Size: [0x00049000]

Module Name: [C:\WINDOWS\system32\ADVAPI32.dll],

Base Address: [0x77DD0000], Size: [0x0009B000]

Module Name: [C:\WINDOWS\system32\RPCRT4.dll],

Base Address: [0x77E70000], Size: [0x00092000]

Module Name: [C:\WINDOWS\system32\Secur32.dll],

Base Address: [0x77FE0000], Size: [0x00011000]
Module Name: [C:\WINDOWS\system32\ole32.dll],
Base Address: [0x774E0000], Size: [0x0013D000]
Module Name: [C:\WINDOWS\system32\msvcrt.dll],
Base Address: [0x77C10000], Size: [0x00058000]
Module Name: [C:\WINDOWS\system32\OLEAUT32.dll],
Base Address: [0x77120000], Size: [0x0008B000]

[==]

Run-time DLLs

[==]

Module Name: [C:\WINDOWS\system32\MSCTF.dll],
Base Address: [0x74720000], Size: [0x0004C000]

[==]

Ikarus Virus Scanner

[==]

Backdoor.Win32.Poison (Sig-Id: 45543332)

[==]

2.a) Cannabis C.exe - Registry Activities

[==]

[=-----=]

Registry Values Read:

[=-----=]

Key: [HKLM\SOFTWARE\Microsoft\CTF\SystemShared\],
Value Name: [CUAS], Value: [0], 1 time
Key: [HKLM\SYSTEM\CurrentControlSet\Control\Session Manager],
Value Name: [CriticalSectionTimeout], Value: [2592000], 1 time
Key: [HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers],
Value Name: [TransparentEnabled], Value: [1], 1 time
Key: [HKLM\System\CurrentControlSet\Control\Terminal Server],
Value Name: [TSUserEnabled], Value: [0], 1 time
Key: [HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle],
Value Name: [Language Hotkey], Value: [1], 2 times
Key: [HKU\S-1-5-21-842925246-1425521274-308236825-500\Keyboard Layout\Toggle],
Value Name: [Layout Hotkey], Value: [2], 2 times

[==]

2.b) Cannabis C.exe - File Activities

[==]

[=-----=]

Files Read:

[=-----=]

File Name: [C:\Cannabis C.exe]

[=-----=]

Device Control Communication:

[=-----=]

File: [\Device\KsecDD], Control Code: [0x00390008], 8 times

[=-----=]

Memory Mapped Files:

[=====]

File Name: [C:\WINDOWS\system32\MSCTF.dll]

File Name: [C:\WINDOWS\system32\MSVBVM60.DLL]

File Name: [C:\WINDOWS\system32\imm32.dll]

File Name: [C:\WINDOWS\system32\rpcss.dll]

[##]

International Secure Systems Lab

<http://www.iseclab.org>

Vienna University of Technology Eurecom France UC Santa Barbara

<http://www.tuwien.ac.at> <http://www.eurecom.fr> <http://www.cs.ucsb.edu>

Contact: anubis@iseclab.org

INFECTED!!! Suggest closing thread

Apocalypse - October 5, 2010, 7:17 pm

nn its Fud Friend ?

Pklocus - October 5, 2010, 7:22 pm

This guy is very legit, i have done trades before with him so I'm sure this crypter works great!!! Will test and review later. But I won't use crypted file since I have nemesis for personal crypting

Lucid - October 5, 2010, 7:23 pm

Reported for infected link broski.

zer0day - October 5, 2010, 7:24 pm

(Oct 5, 2010 07:22 PM)pklocus Wrote: [\[CITE\]](#) This guy is very legit, i have done trades before with him so I'm sure this crypter works great!!! Will test and review later. But I won't use crypted file since I have nemesis for personal crypting

Then why did he post a fake scan? ? His scan doesn't even say what file was scanned, no MD5's..NOTHING

spyke8x - October 5, 2010, 7:25 pm

You didn't copy paste your thread right man...it contradicts itself. very suspicious.

EDIT: just checked it has a poison ivy server in it, and anti sandboxie.

Rowdy - October 5, 2010, 7:25 pm

No one download this! He just hacked my friends account.

N3w_2_H@Ck1n™ - October 5, 2010, 7:46 pm

The file posted by the user in this thread was infected. If you downloaded and ran this file, please take the necessary steps to clean your computer (in the spoiler).

Spoiler [\(Click to View\)](#)

These would be:

First, reading [this thread](#)

Taking these steps to download and run MBAM:

Please download [Malwarebytes' AntiMalware](#).

Double click mbam-setup.exe to install the application. Make sure a checkmark is placed next to Update Malwarebytes' Anti-Malware and Launch Malwarebytes' Anti-Malware, then click Finish.

If an update is found, it will download and install the latest version.

Once the program has loaded, select Perform Quick Scan, then click Scan. The scan may take some time to finish, so please be patient.

When the scan is complete, click OK, then Show Results to view the results.

Make sure that everything is checked, and click Remove Selected.

When disinfection is completed, a log will open in Notepad and you may be prompted to restart. Restart if it tells you to.

The log is automatically saved by MBAM and can be viewed by clicking the Logs tab in MBAM.

Keep a copy of the log, you're gonna need it.

Then, follow these steps to post a HJT log:
Download [HijackThis](#) from Trend Micro.

Run the installer. By default, it will install to C:\Program Files\Trend Micro\HijackThis

Once it is done installing, run HijackThis.

Select Do a system scan and save logfile.

Once HijackThis is done scanning, a notepad will pop up with the HJT log.

Copy and paste the contents of the log into your own separate thread at the forum.

The correct forum being [HijackThis Log Analyzer and Tutorials](#).

Title the thread "[HJT LOG] - Your Username - Infected by a HF user"

And include the MBAM log underneath that, so they have both your HJT and MBAM log. Then also give them a link to this thread, and tell them if anything weird is happening to your computer.

Soon a HJT helper will be there to help you.

Thank you ?