Uttang Dawda

Security Researcher & Trainer

@udawda

udawda@gmail

+1-206-832-6159

Happy with your security?
Let's Talk

Supply Chain Attacks

- Handbrake
- CCleaner
- Transmission
- PyPi
- Asus

Handbrake

Update handbrake to 1.0.7

gsong committed on May 3, 2017 `commit 4097878e65c1de8c69f6e11c45526e4a7220ddc8`

2 Casks/handbrake.rb

```
@@ -1,6 +1,6 @@
 cask 'handbrake' do
   version '1.0.7'
-  sha256 '3cd2e6228da211349574dcd44a0f67a3c76e5bd54ba8ad61070c21b852ef89e2'
+  sha256 '013623e5e50449bbdf6943549d8224a122aa6c42bd3300a1bd2b743b01ae6793'

   url "https://download.handbrake.fr/handbrake/releases/#{version}/HandBrake-#{version}.dmg"
   appcast 'https://github.com/HandBrake/HandBrake/releases.atom',
```

Supply Chain Attacks

- Handbrake
- CCleaner
- Transmission
- Pypi
- Asus

CCleaner 5.33

```
2017-03-11 05:02:39        Event Log:TeamViewer UDP: punch received a=*.*.*.*:64002: (*)
2017-03-11 05:03:48        Event Log:TeamViewer FileWriter: Could not create file C:\Users\x64.dll, Errorcode=5
2017-03-11 05:04:03        Event Log:TeamViewer FileWriter: Could not create file C:\Users\x64.dll, Errorcode=5
2017-03-11 05:04:50        Event Log:TeamViewer FileWriter: Could not create file C:\Users\x64.vbs, Errorcode=5
2017-03-11 05:07:31        Jump List:MRUTime    C:\Users\*********\x64.vbs
2017-03-11 05:07:38        Registry             {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\wscript.exe
```

```
2017-03-12 04:12:36        Event Log:TeamViewer "AddParticipant: [705042190,-1697811015] type=6 name=WIN-FC74JD6H4RJ"
                                                "AddParticipant: [252978432,-1122679512] type=3 name=*********"

2017-03-12 04:12:40        Event Log:TeamViewer "UDP: punch received a=*.*.*.*::63752: (*)"
2017-03-12 04:13:44        Event Log:TeamViewer "ParticipantRemoved: Our own participant was removed,
                                                we must terminate our session"
```

March 11 2017

CCleaner 5.33

```
2017-03-12 04:19:08          File System:Create            C:\windows\prefetch\consent.exe-2D674CE4.pf
2017-03-12 04:19:09          Registry:Modified:UserAssist            C:\ProgramData\CBCB.exe

2017-03-12 04:33:18 Registry:Modified   SOFTWARE\ODBC\ODBC.INI

2017-03-12 04:34:38 Event Log:TS-RCM:1143        The "Limit the size of the entire roaming profile cache"
                    Group Policy setting has been disabled
2017-03-12 04:34:43 Registry:Modified   SYSTEM\ControlSet001\services\SessionEnv
2017-03-12 04:34:43 Event Log:System:7040        Remote Desktop Configuration Service changed from demand start to auto
start

2017-03-12 08:05:48 Registry:Modified   SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf modified
```

March 12 2017

CCleaner 5.33

- July 18 2017 - Avast buys CCleaner
- August 2 2017 - First malicious build injected
- March 8 2018 - Third stage payload discovered

CCleaner 5.33

- First stage : 2.27 million infections
- Second stage : Only 40 computers (Google, Microsoft, Cisco, Intel, Samsung, VMware…) - 0.02% target
- Third stage : 4 computers

Supply Chain Attacks

- Handbrake
- CCleaner
- Transmission
- PyPi
- Asus

Supply Chain Attacks

- Handbrake
- CCleaner
- Transmission : 6500 compromise
- PyPi
- Asus

Supply Chain Attacks

- Handbrake
- CCleaner
- Transmission
- PyPi
- Asus

PyPi

- **acqusition** (uploaded 2017-06-03) - acquisition
- **apidev-coop** (uploaded 2017-06-03) - apidev-coop_cms
- **bzip** (uploaded 2017-06-04) - bz2file
- **crypt** (uploaded 2017-06-03) - crypto
- **django-server** (uploaded 2017-06-02)- django-server-guardian-api
- **pwd** (uploaded 2017-06-02) - pwdhash
- **setup-tools** (uploaded 2017-06-02 08:54:44) - setuptools
- **telnet** (uploaded 2017-06-02 15:35:05) - telnetsrvlib
- **urlib3** (uploaded 2017-06-02 07:09:29) - urllib3
- **urllib** (uploaded 2017-06-02 07:03:37) - urllib3

Supply Chain Attacks

- Handbrake
- CCleaner
- Transmission
- PyPi
- Asus

Asus

- Jan 29 2019 - Attack Discovered in Asus Live Update Tool
- Jan 31 2019 - Asus Notified
- 100,000+ signed infections
- 600 Targeted Mac addresses
- Asushotfix[.]come

Supply Chain Attacks

- Handbrake
- CCleaner
- Transmission
- PyPi
- Asus

Uttang Dawda

Security Researcher & Trainer

@udawda

udawda@gmail

+1-206-832-6159

Happy with your security?
Let's Talk