Fareit Malware Uses Different File Hash for Each Attack to Avoid AV Detection

By Catalin Cimpanu 3 Oct 2015, 02:39 GMT

Fareit info stealer and malware downloading trojan to use a different file hash with every new infection, as Cisco's Talos team reports.

Fareit now uses different file hashes per infec...

Fareit, a trojan specialized in breaching user computers, talking to a C&C (command-and-control) server, and then downloading nasty malware on their systems, has been around since 2012. While in the beginning it was a benign malware downloader, over time it has evolved into a talented information stealer, that's mainly specialized in extracting passwords from Web browsers.

We saw it stealing data from Fargo clients in 2013, and even earlier this year, when criminals were changing DNS entries to point unsuspecting users to servers where Fareit was hosted.

Fareit hides behind chameleon-like tactics

This time around, Cisco's Talos security team has stumbled upon a new version of this malware family that behaves like a chameleon, changing its file hash with each infection, even if the file name remains the same.

The first samples were seen in July of this year, and the malware's creators opted for this tactic to avoid hash- and signature-based detection methods.

"One possible reason for this might be, that the mechanism which they use to download additional malware files or modules (e.g. cclub02.exe), need fixed names or paths (like http://IP/cclub02.exe) and is not flexible enough to handle on-the-fly generated file names on a per victim/campaign base," explains the Talos Group's Earl Carter & Holger Unterbrink. "This could also indicate a pay-per-infection botnet, but of course, this is speculation until we reverse engineer the local binaries and analyze the server command and control software."

Around 2,500 Fareit samples detected, leading back to 2 IP addresses

Cisco's security products recorded 2,455 Fareit samples, but only 23 of them shared the same hash. Digging deeper into the data, they've also noticed that all these samples communicated with only 2 C&C servers, hosted at 89.144.2.115 and 89.144.2.119.

For most of the detected Fareit samp ost of the binary files infected with the malware getti

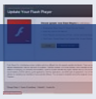
There was, though, one malware sar sample had been detected at the start of March 2

Cars Exposed to Hacking Inside Car Dealerships

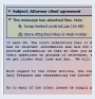
MORE ON: CAR HACKING

The evidence points that this campaign is run by the same group and despite the cyber-criminals' effort to use different file hashes, Cisco's team says that a simple string match against the static file names should protect users from further infections.

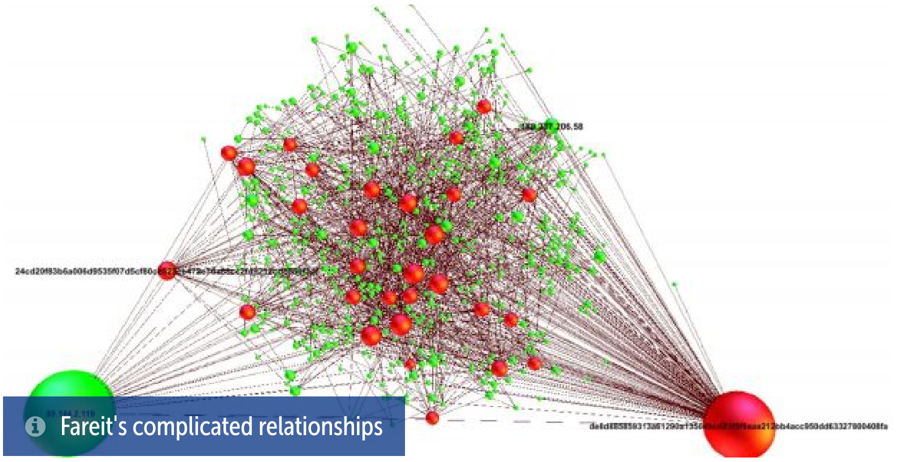
MORE ON THIS TOPIC



Flash Player "Pro" Update Seeps in Fareit Info Stealer



Latest Upatre Trojan Version Targets Windows XP Users



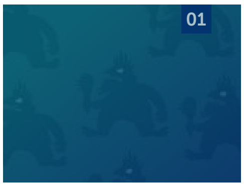
Fareit's complicated relationships

CHECK OUT THE GALLERY (4 Images)

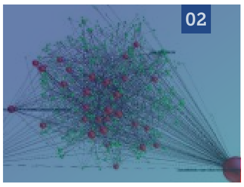
SHARE TWEET SHARE SUBSCRIBE

#Fareit, #info stealer, #malware, #downloader, #file hash

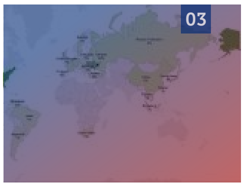
Fareit malware campaign, July 2015 (4 Images)



01



02

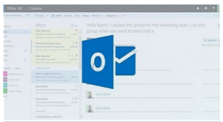


03

```
                       File
bb73e9d6cb8d97b9f3ecf2 rain
d9895587bcbc6e649b691d cclu
912f6fdee713971fdd4cc1 aris
249ef91ff6ed382739c6e1 trah
c1c4ba7ddaf8e8c6192be7 suba
f941e9c743f1ddc0949e0f b0be
80d72606137ea998399380 cclu
b792851aba542f5034f273 trah
ef81a7f272daf88124b1b9 aris
1d6d252410c2ffc6eee631 b0be
88b642d24dc4deb442dd28 trah
```

Hot right now · Latest news

Apple Acquires Deep Learning Perceptio Startup to Boost iOS' Image



Hackers Breach Microsoft OWA Server, Steal 11,000 User Passwords

Microsoft Addresses Privacy Concerns in Windows 10 Build 10558, Data

No, Microsoft Is Not Buying Canonical

Information-Stealing Fareit Malware Used Against Wells Fargo Customers

Dvreza Banking Trojan

MORE +

RELATED APPS

UnReader: Encrypt your text files with ease and decrypt them by either selecting

Crypt-O: Efficiently create and manage secure and custom databases with the

EventSentry Light: Complex utility for monitoring and saving log files regarding

Encoding Decoding Free:

MORE +

Processing Efficiency - Bloomberg

Collection Still Enabled

1 Comment

Share your thoughts on this story!

SUBMIT

FreebeeDiane
4 Oct 2015, 01:56 GMT

This is why tradition signature based malware detection should now be considered obsolete. Behavioral based and heuristic based protection and healthy browsing habits are all that's left. Strong hips and firewall based protection on clients devices and of course super good back up habits. One thing that really annoys be with current anti-malware is they do not tell you when they think the infection occurred. One way to simply make sure all traces of malware are destroyed would be to rollback from backups to the previous day.
Oh well, wishful thinking. It will appear we are in the hands of old style thinking and unless anti-malware companies get current and upgrade their trade. With over 85 thousand new malware occurring every week, it's a doomsday scenario. Good Luck!

– REPLY

I ❤ SOFTPEDIA® Like 202K +1 56K Follow 13K Search here...