Stresspaint Malware Steals Facebook Credentials and Session Cookies

bleepingcomputer.com/news/security/stresspaint-malware-steals-facebook-credentials-and-session-cookies/

Catalin Cimpanu

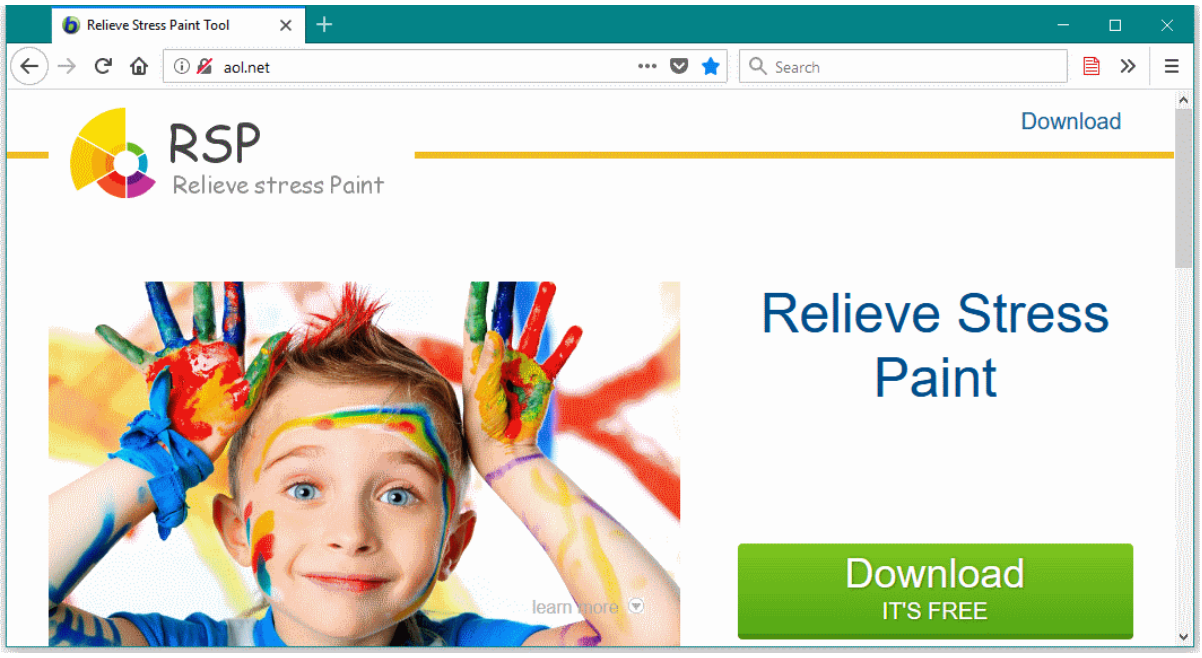
By
Catalin Cimpanu

- April 18, 2018
- 09:10 AM
- 0

Security researchers have spotted a new information stealer that collects Chrome login data from infected victims, along with session cookies, and appears to be looking for Facebook details in particular, according to a Radware threat alert the company shared with this reporter.

The new trojan, named Stresspaint, has been found hidden inside a free Windows application named "Relieve Stress Paint," distributed via aol.net —a domain that uses Unicode characters, which when converted to Punycode spell out xn--80a2a18a.net, instead of the real aol.net.

Radware believes crooks are using email and Facebook spam to direct users to this misleading website.



Users who download this app get a legitimate drawing tool, but the app also runs other files in the background. According to Radware researchers, the drawing app also runs:

Temp\\DX.exe - the main Stresspaint module that remains persistent on the system
Temp\\updata.dll - possibly used later on for credential/cookie stealing purposes

The malware then sets the following Windows registry key to gain boot persistence and run Stresspaint's DX.exe file with every PC boot:

```
HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\Updata
```

According to the Radware team, the value of this registry key is DX.exe [parameter].

"We have seen two different parameters which may indicate two different infection campaigns that the author wants to track," the Radware team says. "This is also represented in the [Stresspaing] control panel."

Stresspaint also creates another registry key. This one holds each infected victim's GUID in the form of "[5 random letters/numbers]HHMMSSYYYYMMDD".

```
HKCU\Software\Classes\VirtualStore\MACHINE\SOFTWARE\RelieveStressPaint\guid
```

Stresspaint steals Chrome login data and session cookies

Stresspaint then makes copies of Chrome's login data and cookies databases, which it stores at the following locations:

```
AppData\Local\Google\Chrome\User Data\Default\Login Data11111
AppData\Local\Google\Chrome\User Data\Default\Cookies11111
```

The malware makes copies of these files so it can run all the queries and operations it needs to extract login credentials and cookie files stored in the user's Chrome browser.

Crooks accessing Facebook accounts to harvest data

The malware then takes the collected login data and session cookies, encrypts it, and uploads it to a remove C&C panel, along with the user's GUID.

Radware researchers tracked this data to a control panel available in the Chinese language. The control panel has dedicated sections for displaying Facebook credentials, and another one for Amazon data. This latter section is empty, suggesting attackers have not focused on extracting the Amazon details from the stolen data just yet.

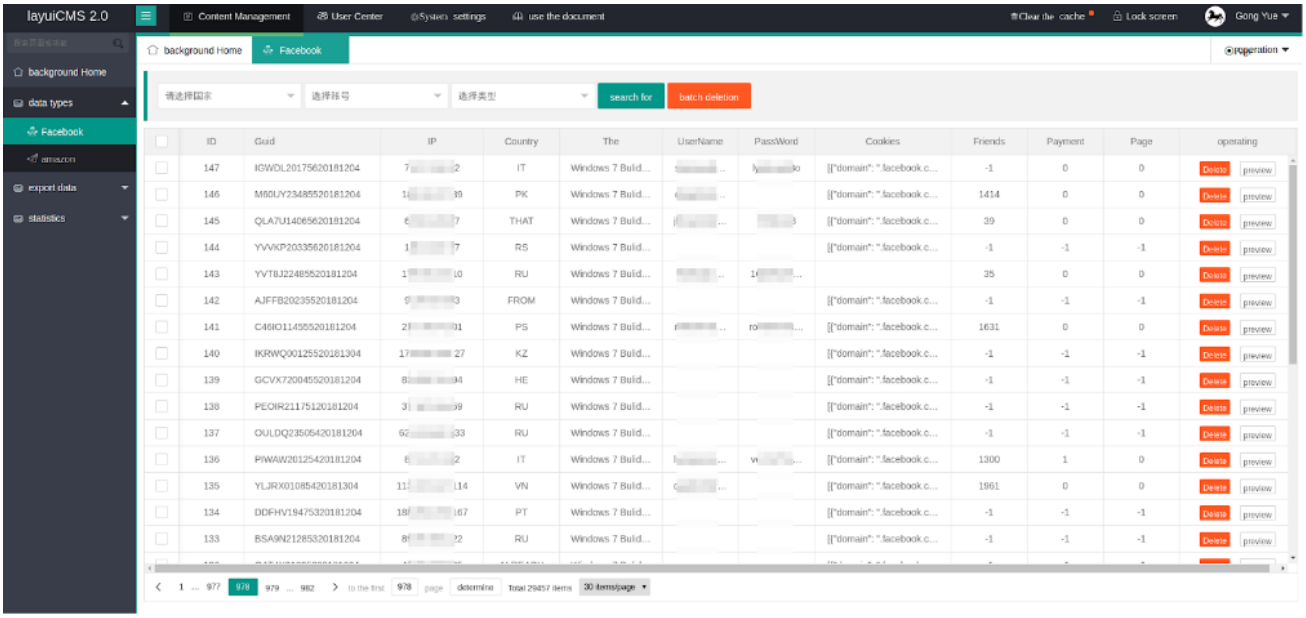


Figure 8: Users' data

Researchers say crooks are actively validating Facebook credentials and session cookies by logging into accounts and collecting additional data such as each user's number of friends, whether the account manages a Facebook Page or not, and if the account has a payment method saved in its settings.

Stresspaint infected over 35,000 users

Radware says it identified over 35,000 infected users, most based in Vietnam, Russia, and Pakistan. The trojanized painting app was first seen at the start of the month, but crooks started its mass-distribution only over the weekend.

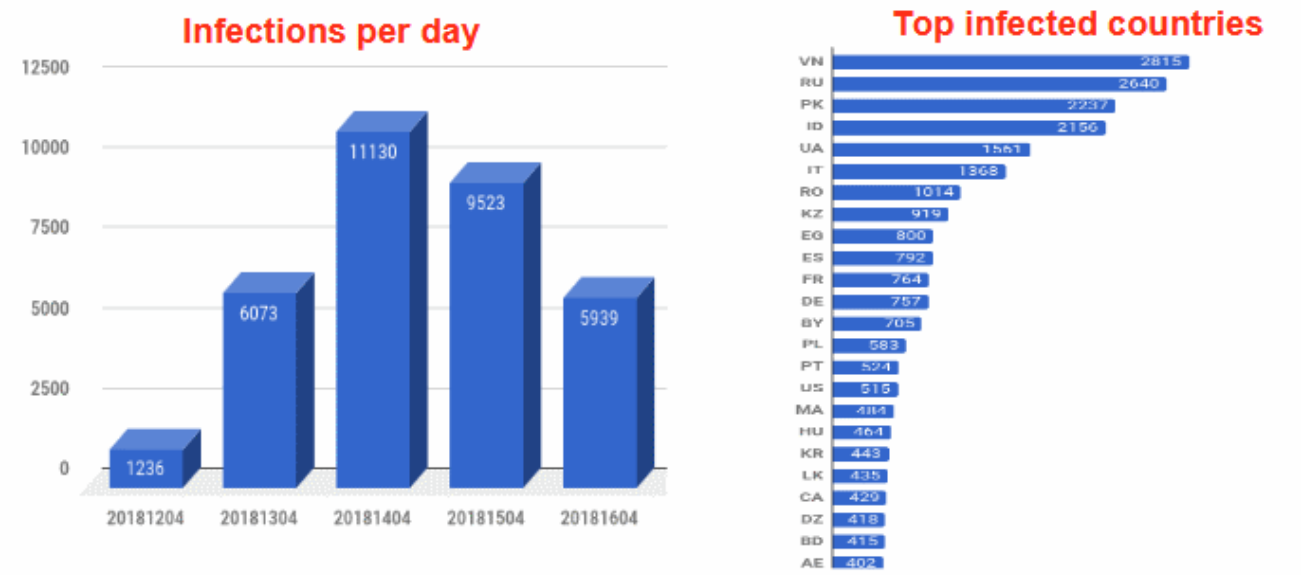


Figure 1 & 2: Breakdown of malware by infections and geographies

While the malware is currently pretty well detected on aggregated virus-scanning services like VirusTotal, Stresspaint initially flew under the radar of some security software because it made copies of Chrome's login and cookies databases and queried the copies instead of attempting to access the original files, usually kept under surveillance by most security software.

Researchers have notified Facebook of the malware's credentials harvesting operations and have also reached out to the domain registrar where the malicious aol.net domain was registered, asking for it to be taken down.

UPDATE 1: Between the time we received the threat alert and publication time, Radware researchers have spotted changes to Stresspaint's inner workings, as the malware now uses a new format for the GUID, and some of the files and registry keys created on infected hosts also vary slightly. Nonetheless, besides cosmetic changes to file names and registry keys, the same modus operandi remains.

UPDATE 2: The Radware threat alert is now live, here.

Related Articles:

Eternity malware kit offers stealer, miner, worm, ransomware tools

German automakers targeted in year-long malware campaign

Ukraine warns of “chemical attack” phishing pushing stealer malware

RIG Exploit Kit drops RedLine malware via Internet Explorer bug

- Facebook
- Information Stealer
- Malware

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

You may also like: