Tens of thousands of Facebook accounts compromised in days by malware

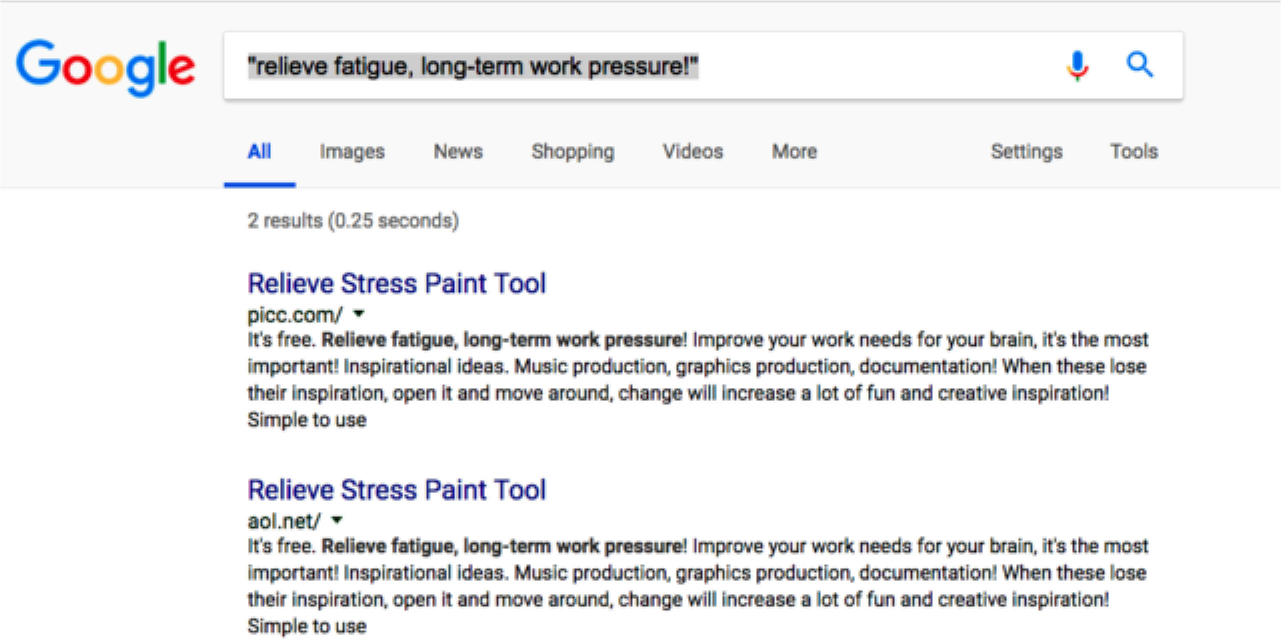
arstechnica.com/information-technology/2018/04/tens-of-thousands-of-facebook-accounts-compromised-in-days-by-malware/

Dan Goodin

Facebook's guidelines visually sum up "offensive things" with this blue text balloon. Meaning, it doesn't resemble a "fully exposed buttock."

Criminals have compromised tens of thousands of Facebook accounts in the past few days using malware that masquerades as a paint program for relieving stress.

"Relieve Stress Paint" is available through a domain that uses Unicode representation to show up as aol.net on search engines and in emails, researchers from security firm Radware said in a post published Wednesday morning. (This query showed the trojan was also available on a domain that was designed to appear as picc.com.) The researchers suspect the malware is being promoted in spam emails.



"relieve fatigue, long-term work pressure!"

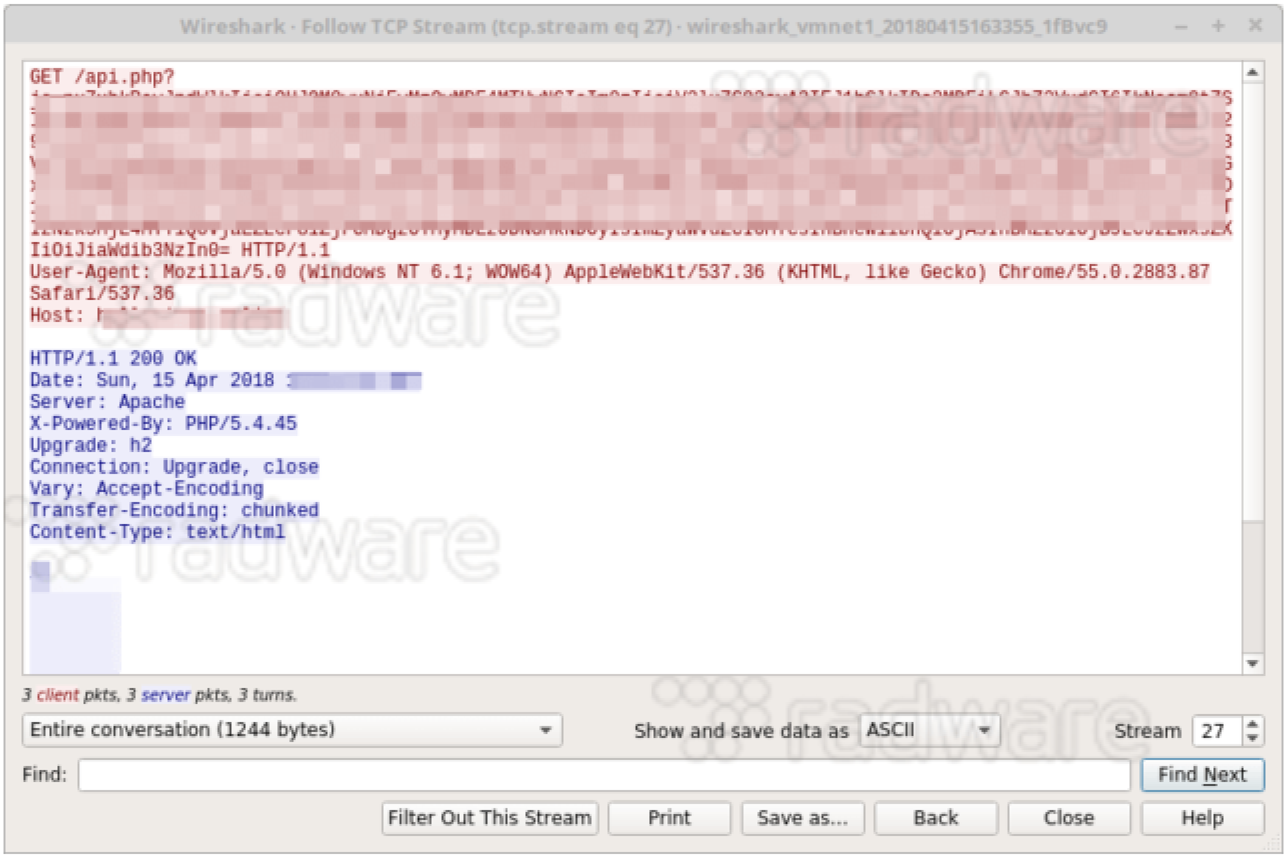
2 results (0.25 seconds)

Relieve Stress Paint Tool
picc.com/ ▾
It's free. **Relieve fatigue, long-term work pressure**! Improve your work needs for your brain, it's the most important! Inspirational ideas. Music production, graphics production, documentation! When these lose their inspiration, open it and move around, change will increase a lot of fun and creative inspiration! Simple to use

Relieve Stress Paint Tool
aol.net/ ▾
It's free. **Relieve fatigue, long-term work pressure**! Improve your work needs for your brain, it's the most important! Inspirational ideas. Music production, graphics production, documentation! When these lose their inspiration, open it and move around, change will increase a lot of fun and creative inspiration! Simple to use

Enlarge

Once installed, the malware acts as a legitimate paint program that changes colors and line size with each user click. Behind the scenes, it copies Chrome data that stores cookies and any saved passwords for previously accessed Facebook accounts.



Wireshark · Follow TCP Stream (tcp.stream eq 27) · wireshark_vmnet1_20180415163355_1fBvc9

```
GET /api.php?
[redacted]
IiOiJiaWdib3NzIn0= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87
Safari/537.36
Host: [redacted]

HTTP/1.1 200 OK
Date: Sun, 15 Apr 2018 [redacted]
Server: Apache
X-Powered-By: PHP/5.4.45
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html

[redacted]
```

3 client pkts, 3 server pkts, 3 turns.

Entire conversation (1244 bytes)

Show and save data as: ASCII

Stream: 27

Find:

Enlarge

Radware

"Stresspaint," as Radware has dubbed the hidden program, continues to copy the Facebook credentials each time a target opens Relieve Stress Paint and each time the computer restarts. The data is sent to a command-and-control server. Radware researchers were able to access the command server's interface, which showed that more than 40,000 computers had been infected by the malware in recent days. In the process, tens of thousands of Facebook accounts were compromised. The interface also compiled any payment details tied to an account, the number of friends the account had, and whether the account was used to manage a page.

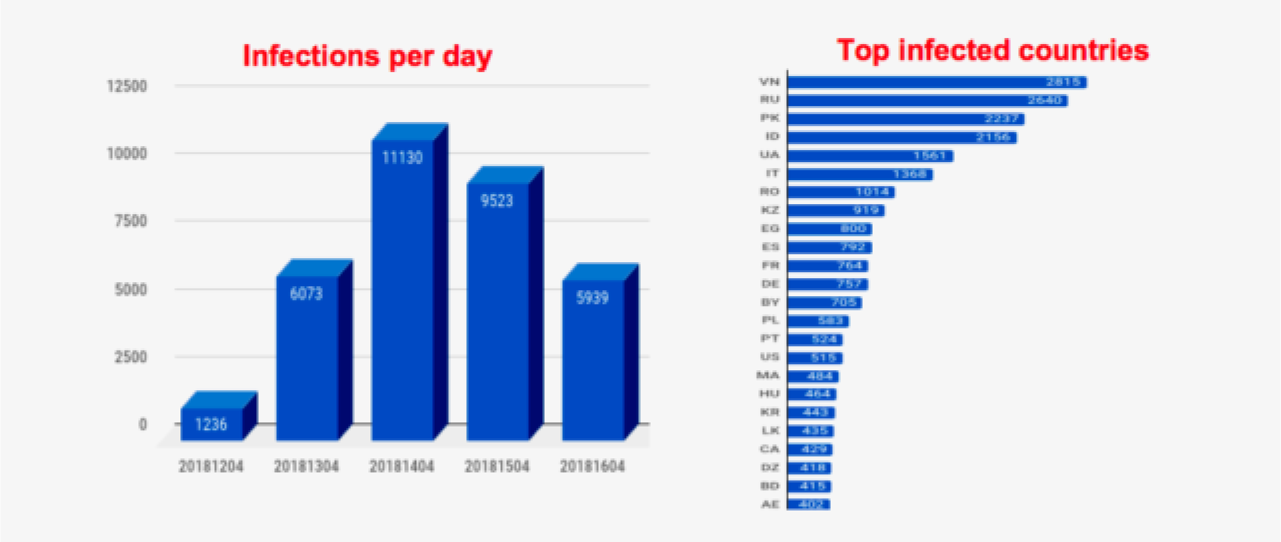
The interface also included a section for viewing credentials for victims' Amazon accounts. It was empty, leading Radware to suspect the attackers hadn't yet enabled code that would actually compromise those accounts. Radware also detected another variant of the malware and saw an indication of it in the control panel.

Stealth

The malware was designed to copy the credentials in a way that wouldn't be detected by antivirus programs. The copying process, for instance, remained active for less than one minute. The malware didn't steal general credentials, and it copied cookies and saved passwords by querying copies of the original cookies and LoginData files rather than through other means.

It remains unclear precisely what the attackers did with data they obtained. Possibilities include selling the data in criminal forums, using it for identity theft or espionage, or using the payment data to buy goods or services on e-commerce sites.

More than five days earlier this week, the malware managed to infect nearly 34,000 computers in two dozen countries.



Enlarge

Radware

Since then, more than 6,000 more infections have occurred.

Anyone who may have been infected by this malware should immediately change their password and should also check the security and login section of their Facebook settings for logins by unrecognized computers. It's always a good idea to protect accounts with multifactor authentication, but it's not yet clear if that protection would have prevented attackers in this campaign from accessing compromised accounts. Because the malware stole both passwords and cookies, it's possible the cookies allowed the attackers to bypass the protection.

In a statement, Facebook officials wrote: "We are investigating these malware findings and we are taking steps to help protect and notify those who are impacted." A spokesman said it wasn't yet clear what effect the attacks had on accounts protected by multifactor authentication.

This ability to infect 40,000 users and compromise tens of thousands of accounts indicates the malware was developed professionally. It wouldn't be surprising to see this group strike again. Radware's blog post is here.