Tens of thousands of Facebook accounts compromised in days by malware

By Dan Goodin

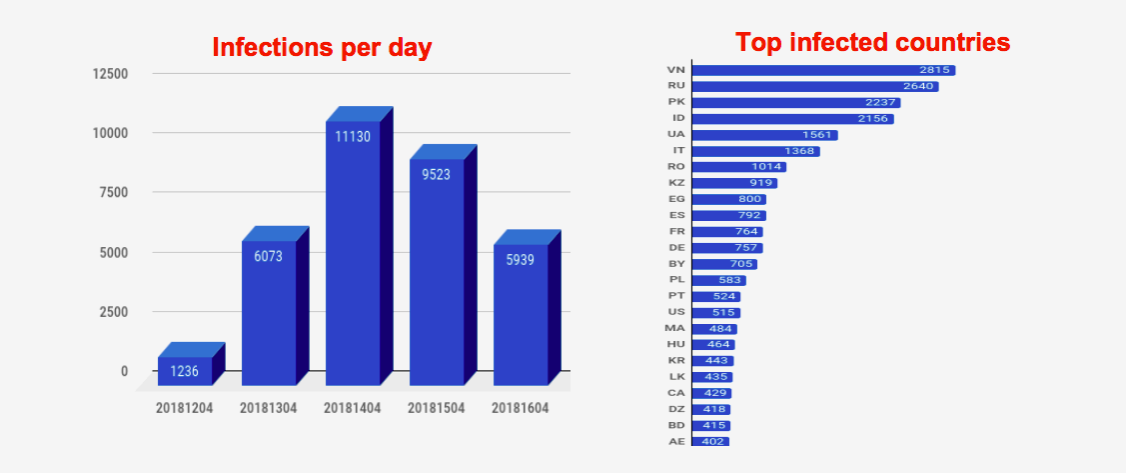
Published: 2018-04-18 · Archived: 2026-04-05 19:49:51 UTC

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.



Credit: Radware

Credit: 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.
