The Washington Post

The Switch

Inside the world of professional e-mail account hijackers

By Andrea Peterson November 6, 2014

E-mail accounts serve as a sort of hub for online identities -- with logins for social media and financial services often tied to them. So when e-mail accounts are hacked, it can be emotionally and financially taxing.

Hackers use two primary approaches to take over e-mail accounts: automated and manual. Automated attacks involve huge networks of computers called botnets that systematically attempt to log in to a large number of accounts. In manual attacks, a person breaks into individual e-mail accounts and combs their content for potentially valuable information.

A new report from Google suggests that the perpetrators of manual account hijacking often approach this type of digital invasion as a job.

"These are really professional people with a very specific playbook on how to scam victims," says Elie Bursztein, the lead author of the report. While the volume of these attacks are low -- nine incidents per million users per day, according to Google's analysis -- their toll can be devastating.

The report, released Thursday on Google's security blog, is the result of years of research by a team that works on account abuse.

"When [hijackers] get into an account, they will spend around 3 minutes assessing it," Bursztein says. "If an account isn't interesting, they will just drop it and move on." But if they find information they consider valuable, hackers will often spend more than 20 minutes looking for the best ways to squeeze the most out of it -- locking out the legitimate account holder by changing the password, searching for other accounts associated with the e-mail, such as online banking or social media accounts, and scoping out new new victims.

The hackers might, for example, send e-mails to members of your address book -- begging them for money due to an unforeseen circumstance, like being mugged in a foreign country. That can be really distressing for some recipients, Bursztein says. "If your mother gets this e-mail, she'll be very worried. There's emotional distress that's generated by this beyond the financial costs."

The hijacker may also send phishing e-mails to your contacts. Phishing is a type of social engineering where an attacker tries to trick a user into submitting login credentials to n fake site controlled by the hacker. It's one of the best known kinds of attacks, but Google's research suggests that it can be very effective -- especially if links to such sites are sent from the e-mail of someone you trust.

According to the report, people in the contact list of a hijacked account are 36 times more likely to be hijacked themselves. Some 14 percent of people visiting fake login pages submitted some sort of credentials, Google found, while the most convincing phishing site they uncovered had a 45 percent success rate, and even the most poorly done site tricked 3 percent of people. The company said it is constantly searching the Internet, flagging suspicious sites in an attempt to warn users.

Google tested the efficiency of some phishing sites by submitting credentials for dummy accounts they created -- and found that the hackers moved fast: 20 percent of the credentials were used within 30 minutes, and 50 percent were tried within seven hours.

The researchers observed that hijackers seemed to work in specific shifts. "They are professional in the sense that they almost have office hours," says Bursztein. "For the groups that we're able to track, they work maybe not eight hours a day, but a really normal schedule with lunch breaks, for instance."

A group of attackers would often use the same tools and tactics, would appear to coordinate when it came to distributing new targets and would share information, the report says. This professionalization has a lot in common with the structures found in other types of cybercrime -- like credit card theft rings, which experts say include systematic hierarchies and are believed to be primarily run by gangs out of Eastern Europe.

The geographic location of hijackers is hard to determine, Google says, because traffic may be routed through proxies. But IP addresses associated with account takeover attempts were most likely to be associated with China and Malaysia, and attackers often search for Chinese language terms.

Google uses automated systems that seek to identify potentially suspicious logins before they occur. "There are about 120 signals we combine into a verdict about the validity of a login," says Bursztein. "If we have some suspicion, we will ask you for a knowledge test -- like what's your phone number or where you logged in from last."

But hijackers adapt quickly to new security tactics, he says. For instance, when the company started doing those knowledge tests, the hackers started phishing for that same type of information.

Perhaps the most frustrating part of this work for Bursztein is that there are already security feature available that can dramatically decrease, if not eliminate, manual hijacking attacks.

"This should not happen," he says. "We have the perfect defense against it, and we would love to have more people using it." That perfect defense is two-factor authentication, a system where users provide a secondary way to verify their identity -- often a code sent to their mobile phone via text message. Google also recently unveiled an even more secure form of two-factor that relies on a physical key in the form of a USB drive that users can plug in during the login process to verify their identity.

Bursztein says Google had a robust debate about whether to release the hijacking report, knowing that perpetrators would likely read it and perhaps adjust their tactics. But ultimately, the company decided that providing greater transparency about why it pursues some security measures might help users understand them better -- and perhaps encourage more people to take advantage of two-factor and other enhanced security features.

Have more to say on this topic? Join us today for our weekly live chat, Switchback. We'll kick things off at 11 a.m. Eastern time. You can submit your questions now, right here.

3 Comments

Andrea Peterson covers technology policy for The Washington Post, with an emphasis on cybersecurity, consumer privacy, transparency, surveillance and open government. Follow @kansasalps