Bloomberg (http://www.bloomberg.com)

Markets (http://www.bloomberg.com/markets) **(I**

TECHNOLOGY

SEE MORE

GLOBALTECH COVERING THE 57 MILLION SQUARE MILES OUTSIDE SILICON VALLEY

(/blogs/technology/global-tech/)

MORE STORIES

Gone in 180 Seconds: Hackers Quickly Raid E-Mails in Search of 'Wire Transfer' and Sex Photos

Save

By Jordan Robertson 2014-11-19T19:01:49Z **- Comments** **Email** **Print**

(/photo/nicholas-cage-/-iBFkUvYvkfP0.html)

Photographer: Buena Vista/Everett Collection

Nicolas Cage in "Gone in 60 Seconds," 2000.

If you fear the website you just visited may have stolen your e-mail password, don't delay taking action. Hackers who use that information to access accounts move at "astonishing" speed, according to a report from Google and the University of California at San Diego.

The new **study (http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf)** offers a revealing look at what cyber-criminals do once they have a person's e-mail account credentials -- and how fast they operate. The research focused on manual-account takeovers, in which hackers go through the labor-intensive process of accessing the accounts using the purloined passwords and sifting through the contents in search of sensitive data. This type of attack is relatively rare -- Google estimates it occurs nine times per million Google users per day -- but the damage is more extensive and severe than the automated scams that make up the majority of threats on the Internet.

For clues about how long hackers stay inside hacked e-mails accounts and what they look for, researchers examined 5,000 Google accounts that had been hijacked. They also used 200 decoy accounts to measure how little time people actually have between the moment their passwords are stolen and when hackers put them to use.

As the chart shows, after intentionally entering decoy credentials in phishing pages targeting Google users, a fifth of those e-mail accounts were accessed by hackers in the first 30 minutes. Within 7 hours: half the accounts.

The shortest amount of time was just a matter of minutes, according to Elie Bursztein, one of the authors and the anti-abuse research lead for Google. The pace is unsettling because even proactive users typically don't move that fast. According to Google, within an hour of a takeover, users reclaim their accounts about a fifth of the time, and within 13 hours, about half have wrested control back from the hackers.

Once the hackers were inside, they spent an average of just three minutes to assess the value of the e-mail accounts before exploiting them or abandoning them in search of more lucrative targets. The fact that some accounts were not exploited suggests that the hackers are "professional," according to the report. In assessing the accounts, cyber-crooks focused on e-mails that were starred, drafts and contact lists to determine the number of possible victims they can scam. The hackers also searched e-mails containing keywords such as "wire transfer" and "bank" (including images of signatures for forgery purposes), as well as "sex," "jpg" and "mov" (for sensitive content that could be used in blackmail).

Source: Elie Bursztein, Borbala Benko, Daniel Margolis, Tadek Pietraszek, Andy Archer, Allan Aquino, Andreas Pitsillidis, Stefan Savage/Google, Inc./University of California, San Diego

Source: Elie Bursztein, Borbala Benko, Daniel Margolis, Tadek Pietraszek, Andy Archer, Allan Aquino, Andreas Pitsillidis, Stefan Savage/Google, Inc./University of California, San Diego

If the hackers liked what they found, they would spend an additional 15 to 20 minutes per account examining e-mails and figuring out ways to make money from the information.

Most of the attacks in this study originated in China, Ivory Coast, Malaysia, Nigeria and South Africa.

What the report tells us is that hackers are getting faster because people and companies are getting faster at spotting fraud. The window of time for an attack is narrowing. That's a good thing.

But in many cases, attackers still have an edge. Bursztein said a good way users can protect themselves is by adding phone numbers and other contact methods to their accounts, so companies can contact them quickly when misbehavior is detected. As the study shows, every minute counts as cyber-crooks move at Internet speed to exploit what has become the main filing cabinet for our personal and financial information.

Related:

- **Hackers Can Steal Data Wirelessly From PCs That Aren't Even Online (http://www.bloomberg.com/news/2014-11-19/hackers-can-steal-data-wirelessly-from-pcs-that-aren-t-even-online.html)**
- **WhatsApp Encrypts User Messages Following Google, Apple (http://www.bloomberg.com/news/2014-11-18/whatsapp-encrypts-user-messages-following-google-apple.html)**

Facebook (https://www.facebook.com/sharer/sharer.php?u=http%3A%2F%2Fwww.bloomberg.com%2Fnews%2F2014-11-19%2Fgone-in-180-seconds-hackers-quickly-raid-e-mails-in-search-of-wire-transfer-and-sex-photos.html)

Twitter (https://twitter.com/share?url=http%3A%2F%2Fbloom.bg%2F1uwYjci&counturl=http%3A%2F%2Fwww.bloomberg.com%2Fnews%2F2014
11-19%2Fgone-in-180-seconds-hackers-quickly-raid-e-mails-in-search-of-wire-transfer-and-sex-photos.html&via=business&text=Gone%20in%20180%20Seconds%3A%20Hackers%20Quickly%20Raid%20E-Mails%20in%20Search%20of%20'Wire%20Transfer'%20and%20Sex%20Photos%20By...)

Google+ (https://plus.google.com/share?hl=en&url=http%3A%2F%2Fwww.bloomberg.com%2Fnews%2F2014-11-19%2Fgone-in-180-seconds-hackers-quickly-raid-e-mails-in-search-of-wire-transfer-and-sex-photos.html)

LinkedIn (http://www.linkedin.com/shareArticle?mini=true&url=http%3A%2F%2Fwww.bloomberg.com%2Fnev
photos.html&title=Gone+in+180+Seconds%3A+Hackers+Quickly+Raid+E-Mails+in+Search+of+%27Wire+Transf
mail+password%2C+don%27t+delay+taking+action.+Hackers+who+use+that+information+to+access+accounts+

PREV

Hackers Can Steal Data Wirelessly From PCs That Aren't Even Online

(/news/2014-11-19/hackers-can-steal-data-

NEXT

Xiaomi's CEO Knows How to Make an Entrance -- and an Exit

(/news/2014-11-19/xiaomi-s-ceo-knows-