TAG ME IF YOU CAN
A MASSIVE PHISHING CAMPAIGN IN FACEBOOK WATERS

Ido Naor
Sr. Researcher, Global Research and Analysis Team
Kaspersky Lab
Twitter: @idonaor1
GReAT - Kaspersky Lab Elite Team Of Researchers

Global Research & Analysis Team, Since 2008

Threat Intelligence, research and innovation leadership

Focus: APTs, critical infrastructure threat, banking threats, sophisticated targeted attacks.

- A decade in security eco
- Manage regional research in Israel
- Specialties
  - Malware analysis
  - Reverse Engineering
  - Penetration Testing
- Hobby

Responsible Disclosure:

[Logos of Alibaba, Facebook, LinkedIn, Google, WordPress, Starbucks, eBay]
SHOW ME THEM FACTS

How People Access Facebook

<table>
<thead>
<tr>
<th>Device</th>
<th>Percent of Facebook Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop/Laptop</td>
<td>88%</td>
</tr>
<tr>
<td>Smartphone</td>
<td>53%</td>
</tr>
<tr>
<td>Tablet</td>
<td>28%</td>
</tr>
</tbody>
</table>

29% of Americans Use Facebook During Work Hours Every Day

<table>
<thead>
<tr>
<th>Website</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>29.29%</td>
</tr>
<tr>
<td>Gmail</td>
<td>24.26%</td>
</tr>
<tr>
<td>Yahoo Mail</td>
<td>22.82%</td>
</tr>
<tr>
<td>YouTube</td>
<td>14.4%</td>
</tr>
<tr>
<td>Twitter</td>
<td>9.89%</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>6.33%</td>
</tr>
<tr>
<td>Pinterest</td>
<td>4.8%</td>
</tr>
</tbody>
</table>

problem

facebook at Work
SO SHOULDN’T I JUST...
TAG ME IF YOU CAN
JOKES ONLY TECH PEOPLE GET:

WAT?
10,000 MALWARE DOWNLOADS IN <48HRS
FACEBOOK MALWARE: COMPLEX CODE TRAPS VICTIMS INTO TARGETING FRIENDS

After 10,000 Facebook users with Windows PCs were hit by malicious friend notifications, Kaspersky Lab explains the vulnerability and attack.

1. **A Message**
   - Facebook user receives a message that a friend has mentioned them in a comment.
   - Mike has mentioned you in the comments.

2. **Trio of Infection Paths**
   - Victim clicks on link in message and is taken outside Facebook to download malware.
   - If this fails, attacker spams their Facebook chat sending Tiny URL link to download the malware.
   - Attacker adds Facebook post to victim’s timeline with malicious Google shortener link.

3. **Google Chrome Browser Takeover**
   - Malware executes and downloads Chrome browser takeover code.
   - Malicious Chrome opens.
   - Presents ‘Facebook’ page to user – attackers block Facebook anti-virus plugin.
   - Captures traffics and hijacks accounts.

4. **In the Background, another script silently downloads**
   - 1,500 lines of complex code.
   - Obfuscated.
   - Locks the DOM from inspection.
   - Other tricks to protect code from analysis.

5. **Stolen Accounts**
   - Attackers now own victim’s Facebook & Google Drive accounts.
   - Steal everything through the browser.
   - Turn victim into a malware hub and send infected notifications to all their friends.
LESSONS LEARNED

• Zero Days are not alone
  • Online services and social networks vulnerabilities can do as much harm.
• Phishing campaigns ++
  • Traditional phishing is still here, but we must adjust to a new reality
• Malware As A Service – Plug & Play
  • Malware authors are not the criminals, they only sell service to their users.
FLY SAFE, BUT REMEMBER TO...

• Introduce the Facebook malware to employees.
• Engage in phishing/online-safety awareness at your workplace.
  • Address issues raised by employees – take every issue seriously!
  • Commit to a reporting protocol and policy.
• Ensure that endpoint protection is in place and up-to-date.
• Consider inviting external speakers. It really is refreshing.

Have a safe ride online, and may the odds be forever in your favor.
THANK YOU!
Follow me on Twitter: @IdoNaor1