The Slingshot Project

Measuring, analyzing, and defending against targeted attacks

Stevens Le Blond
Software security model

- Obscurity
- Reactivity
- Correctness
- Isolation

Diagrams showing various software security models and their components.
Skype enables large-scale IP tracking...
... and targeted tracking

Stevens

I would like to use you as an example to show that I can find the IP of anyone who has logged on Skype in 72 hours. Is that OK with you?

You can use me as an example. I don't care if my IP address is private or not!

BTW, am I to understand that you know what P2P downloads I have made?

Everybody was very impressed with your visit, and we'd be delighted if you could do a post-doc here.
Four years later...

DoS me!

- Blacklisted: 77
- Realtime Visitors: 13
- Total Resolves: 629435
- Server Status: Online

Username: Paul, Francis

Resolve
Open research problems

• Traffic analysis (Aqua project):
  – Can break most anonymity networks
    • e.g., >98.3% of anonymous VoIP calls traced after one month based on real voice workload
  – Can we build apps that resist traffic analysis?

• Targeted attacks (this talk):
  – How are they carried out today?
  – What does it teach us about defenses?
Targeted attacks

Stuxnet: 2010

RSA watering-hole attack: 2012

Targets:
- Government
- Company
- NGO/Civilians

Entice *specific* users, organizations, or communities into installing malware

2014 peer-reviewed studies on targeted attacks
Outline

Attacker(s)

Email services

Target(s)

• How specialized is command and control?
• How sophisticated is social engineering?
• What are the most common attack vectors?

Data

Malware

Social engineering

Attack vectors

Future work

NGO
A look at targeted attacks through the lense of an NGO

Joint work with: Adina Uritesc, Cedric Gilbert, Zheng Leong Chua, Prateek Saxena, Engin Kirda
Outline

Attacker(s)

Data
Malware
Social engineering
Attack vectors
Future work

Email services

Gmail
Hotmail
Yahoo!

Target(s)

NGO

• How specialized is command and control?
• How sophisticated is social engineering?
• What are the most common attack vectors?
Our dataset of targeted attacks

- Contacted >100 NGOs in 2013
- Collaborate with a targeted human-rights NGO (WUC) representing the *Uyghur*
- Two NGO affiliates share >1.5k suspicious emails (>1.1k w/ malware)
- Attack numerous related targets with same emails (via To or Cc)
What organizations are being targeted?

<table>
<thead>
<tr>
<th>Organization</th>
<th># Recipients</th>
<th># Emails</th>
</tr>
</thead>
<tbody>
<tr>
<td>World Uyghur Congress (WUC)</td>
<td>53</td>
<td>2,366</td>
</tr>
<tr>
<td>East Turkestan Union in Europe (ETUE)</td>
<td>7</td>
<td>153</td>
</tr>
<tr>
<td>Australian Uyghur Association</td>
<td>3</td>
<td>129</td>
</tr>
<tr>
<td>Euro-Asia Foundation in Turkey</td>
<td>2</td>
<td>101</td>
</tr>
<tr>
<td>Uyghur Canadian Association</td>
<td>6</td>
<td>98</td>
</tr>
<tr>
<td>Germany Uyghur Women Committee</td>
<td>2</td>
<td>82</td>
</tr>
<tr>
<td>Radio Free Asia (RFA)</td>
<td>12</td>
<td>80</td>
</tr>
<tr>
<td>France Uyghur Association</td>
<td>5</td>
<td>80</td>
</tr>
<tr>
<td>Eastern Turkestan Australian Association (ETAA)</td>
<td>6</td>
<td>77</td>
</tr>
<tr>
<td>Uyghur American Association (UAA)</td>
<td>10</td>
<td>72</td>
</tr>
</tbody>
</table>

... 

>100 targeted organizations

Dataset captures attacks against NGOs and few high-profile targets.
Example of targeted attack

From: ...
Date: Mon, Mar 4, 2013 at 8:58 AM
Subject: Invitation Letter of WUC International Conference
To: ...

Dear ..., 

I am writing to you from the World Uyghur Congress (WUC) and on behalf of the Unrepresented Nations and Peoples Organization (UNPO) and the Society for Threatened Peoples (STP) with financial support from the National Endowment for Democracy, cordially invites you to attend the WUC's upcoming Conference which will be held in Geneva between 11th and 13th March 2013.

Attached you can find the invitation letter. We hope you will give a positive consideration to this invitation, and look forward to meeting you in Geneva. During your stay in Geneva, travel, accommodation and food are covered by the WUC.

The WUC is a nonprofit organization granted by the National Endowment for Democracy in Washington, DC to peacefully promote human rights, democracy and freedom for the Uyghur people in East Turkestan.

If you have any questions or queries regarding your participation, please do not hesitate to contact me. Phone: ..., Fax: ..., e-mail: ...

sincerely,
Outline

Attacker(s)

Target(s)

Email services

Data

Malware

Social engineering

Attack vectors

Future work

- How specialized is command and control?
- How sophisticated is social engineering?
- What are the most common attack vectors?
How specialized is Command and Control (C2)?

- Cluster >500 samples
- >25% of malware linked to known groups
- One group (DTL) targeted wide range of industries

Same C2 used for diverse organizations / industries

Source: FireEye
Outline

Attacker(s)

Data

Malware

Social engineering

Attack vectors

Email services

Gmail

Hotmail

Yahoo!

Target(s)

WUC

• How specialized is command and control?
• How sophisticated is social engineering?
  – What is the timing of attacks?
  – Are topic and language tailored to targets?
  – Do emails impersonate contacts of targets?
• What are the most common attack vectors?
What is the timing of attacks?

Attacks occur often; over long time periods; sprayed over several targets.
Are topic and language tailored to targets?

Topics and languages are manually tailored to targets.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Fraction of Malicious Emails</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>1,116</td>
</tr>
<tr>
<td>WUC</td>
<td>51%</td>
</tr>
<tr>
<td>Uyghur</td>
<td>29%</td>
</tr>
<tr>
<td>Rights</td>
<td>12%</td>
</tr>
<tr>
<td>Others</td>
<td>2%</td>
</tr>
<tr>
<td>Unknown</td>
<td>4%</td>
</tr>
</tbody>
</table>
Do emails impersonate contacts of targets?

Attackers exploit legitimacy of targets’ real social contacts.
Outline

Attacker(s)

Email services

Target(s)

- How specialized is command and control?
- How sophisticated is social engineering?
- What are the most common attack vectors?

Data

Malware

Social engineering

Attack vectors

Future work
Timeline of exploited vulnerabilities

Attacks exploit recent but disclosed vulnerabilities (no 0-days)
(In)effectiveness of reactive security

Fails to detect even old exploits
Impact of application-level isolation

Significantly raises the bar
Future work

Attacker(s)

- Data
- Malware
- Social engineering
- Attack vectors

Defenses

- Generalize results
- Monitoring and attack attribution
- Defenses
  - Detection of contact impersonation
  - Dynamic analysis in controlled env.
  - Spatio-temporal, OS-based isolation

Target(s)
Detecting contact impersonation in spear-phishing attacks

Joint work with: Istemi Ekin Akkus, Cedric Gilbert, Peter Druschel
Do spam filters detect spoofed emails?

<table>
<thead>
<tr>
<th>Policy</th>
<th>AOL</th>
<th>GMail</th>
<th>Hotmail</th>
<th>Yahoo</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>Spam</td>
<td>Inbox (via)</td>
<td>Spam</td>
<td>Spam</td>
</tr>
</tbody>
</table>

Existing filters fail to detect spoofed contacts
Unilateral detection of contact impersonation in malicious emails

• A browser extension that leverages:
  – Typo emails/names
  – Authentication
  – Writing style

• Switches to crypto signatures if both users support it

• Optionally uploads attachments for dynamic analysis
Experimental setup

Incoming emails (testing set)

Authorship verification (Writeprints w/ training set)

Impersonated emails

Legit emails
Experimental setup cont.

• Enron dataset
  – Keep users with $\geq 4.5k$ words
  – Emulate impersonated emails
  – Verify authorship of emails $\geq 25$ words

• Accuracy metrics
  – Recall: Fraction of attacks detected
  – Precision: Fraction of warnings corresponding to attacks

What accuracy of authorship verification for email workload?
Can we verify that legitimate contact wrote email?

We can verify authorship with high accuracy.
Future work

Attacker(s)

Defenses

• Generalize results
• Monitoring and attack attribution
• Defenses
  – Detection of contact impersonation
  – Dynamic analysis in controlled env.
  – Spatio-temporal, OS-based isolation

Target(s)

Data

Malware

Social engineering

Attack vectors

Future work
Take home messages

- **Low-volume, socially engineered** communications which entice **specific targets** into installing malware

- **Malware:**
  - Same entities target corporations, political institutions, and NGOs
  - Download dataset at slingshot.mpi-sws.org

- **Social engineering:**
  - Topic, language, and senders manually tailored to targets
  - Stylometry accurately detects contact impersonation

- **Attack vectors:**
  - Recent but disclosed vulnerabilities that evade reactive defenses
  - Data indicates isolation is effective in the wild