Going Hunting with ThreatLabZ

Deepen Desai, VP Security Research, Zscaler
Agenda

- Hunting & Coverage by ThreatLabZ
- Recent Threat Trends from the Cloud
- Live Infection Demo
- Hunting with Hyatt Zscaler Logs
Hunting by ThreatLabZ
Tracking Phishing campaigns

- **Machine Learning based intelligence**
  - Model trained over images & page layout of top targeted brands
  - Newly registered domains and subset of uncategorized URLs are vetted

- **Phishing template based intelligence**
  - Content based signatures for confirmed phishing campaigns
  - Generic content based detection

- **Destination based intelligence**
  - Reputation feeds

---

Over 11,500 certificates with the string "paypal" were issued by Let's Encrypt!!
Tracking Exploit Kits

- Exploit Kit tracking
- Exploit Kit landing page fingerprinting
- Gate monitoring
- Exploit payload monitoring
- Automated sandbox detonation
- Quarterly Exploit Kit reports

**Research Datamining Framework**

- Automated sandbox detonation
- Hourly EK cycle reports for coverage
- Signatures and IOCs

**EK Tracking dashboards**

**EK Feeds**
Tracking malware families

Malware Family tracking

• Top prevalent malware families
• Clustering approach
  • Static features
    • Unpacked samples for hundreds of prevalent malware families
  • Assembly function checksums
• Dynamic features
  • System and Network activity
• VirusTotal and OSINT feeds
Recent Threat Trends
Out of sight but not invisible: Defeating fileless malware with behavior monitoring, AMSI, and next-gen AV

Consider this scenario: Two never-before-seen, heavily obfuscated scripts manage to slip past file-based detection and dynamically load an info-stealing payload into memory.

In this scenario, Antimalware Scan Interface (AMSI) facilitates detection. AMSI is an open interface that allows antivirus solutions to inspect.

AMSI is part of the range of dynamic next-gen features that enable antivirus capabilities in Windows Defender ATP to go beyond file scanning. These features, which also include behavior monitoring, memory scanning, and boot sector protection, catch a wide spectrum of threats, including new and unknown variants.
Encrypted traffic on the rise!

- 80% of Internet bound traffic is encrypted – Dec 2018
- Increase of 10% since Dec 2017
Phishing Attacks targeting Corporate Services

- 400% growth in phishing attacks over SSL since 2017
- Office 365 is mainly targeted

![Chart showing Newly Registered Domain blocks - HTTPS]

![Pie chart showing Top Phished Brands over HTTPS: 58% Microsoft, 12% Facebook, 10% Amazon, 10% Apple, 4% Adobe, 4% Dropbox, 2% DocuSign]
Abusing Microsoft Azure domains to host Phishing pages

- **ThreatLabZ discovered** phishing attacks hosted on Microsoft Azure domains.
- Attack starts with e-mails saying messages are quarantined or voice msg is waiting
- Links to *.web.core.windows.net, over HTTPS, cert signed by Microsoft
- Microsoft, Adobe, Blockchain, etc credentials phished
- ~3,000 phishing attempts blocked over 2 months
- Microsoft was notified, who quickly engaged to shut these sites down
SMiShing

SMiShing also known as SMS phishing is an attack method used to steal sensitive credentials from mobile users.

Attack starts with the end user receiving a SMS message containing a specially crafted link that points to a phishing site.

SMiShing campaigns targeting (2018):
- Social - Facebook, WhatsApp
- Financial - Natwest, HSBC, Paypal
- Productivity software and services
Recent SMiShing campaign targeting Canadian Banks

SMiShing also known as SMS phishing is an attack method used to steal sensitive credentials from mobile users.

Newly registered domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Creation Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>75-43-02-12.com</td>
<td>2019-03-28</td>
</tr>
<tr>
<td>65-75-34-23.com</td>
<td>2019-03-27</td>
</tr>
<tr>
<td>09-34-54-23.com</td>
<td>2019-03-28</td>
</tr>
<tr>
<td>182-32-12-43.com</td>
<td>2019-03-27</td>
</tr>
<tr>
<td>10-34-23-54.com</td>
<td>2019-03-28</td>
</tr>
<tr>
<td>172-32-23-43.com</td>
<td>2019-03-28</td>
</tr>
<tr>
<td>54-34-23-65.com</td>
<td>2019-03-27</td>
</tr>
<tr>
<td>65-34-23-12.com</td>
<td>2019-03-28</td>
</tr>
<tr>
<td>pp.online-kundenservice.info</td>
<td>2019-03-28</td>
</tr>
<tr>
<td>online-kundenservice.info</td>
<td>2019-03-28</td>
</tr>
<tr>
<td>onlinekundencenter.eu</td>
<td>2019-03-27</td>
</tr>
<tr>
<td>ppl.de-kunden.online</td>
<td>2019-03-27</td>
</tr>
<tr>
<td>de-kunden.online</td>
<td>2019-03-27</td>
</tr>
<tr>
<td>gruppo-biper-sicurezza.net</td>
<td>2019-03-26</td>
</tr>
<tr>
<td>poste-verifica-digitaile.net</td>
<td>2019-03-26</td>
</tr>
</tbody>
</table>

SMiSh text

ROYALBANK
Account status (Restricted)
Urgent action required.
http://rbc.com
54-34-23-65.com/

Canadian Bank Phishing pages – mobile supported!
JavaScript Skimmers – Magecart and Co.

Injected JS skims for User’s financial information from compromised e-commerce sites.

- E-commerce sites injected with malicious JS
- Dynamically adds a form to the payment page using DOM properties
- Captures site information, credit card, and user’s personal information
- Use of HTTPS
- Details on research.zscaler.com
Key Takeaways

• Defense in depth approach
  • URL filtering, Advanced Threat Protection, Cloud Sandbox, Cloud Firewall

• Zscaler Security Policy recommendations
  • SSL inspection
  • Newly Registered Domains block
  • Generic TLD blocks
  • URL caution on uncategorized traffic

• User awareness & training
  • End User Notification customization to help users
In an open forum with Zscaler employees, partners, and customers

Your knowledge and learn from experts in cloud security

The conversation at community.zscaler.com
Thank You