A new approach to email security

Adrien GENDRE - Chief Solution Architect
Agenda

• Vade Secure brief presentation
• What are the phishing technics
• A Real-life phishing attack
• The answer
Vade Secure is the pioneer of predictive email defense.

- 76 countries
- 500M protected mailboxes
- More than 5000 customers
- 95% renewal rate
A wide dataset from Providers
A technology expertise
What are the phishing technics?
Existing solutions

Some of the major technologies are used to block email threats:

• Sender Blacklist (IP, Domain)
• Fingerprint
• Text Analysis
• URL Domain Filtering
Blacklists / Reputation

The Sending IPs, domains… lists
# Blacklists

<table>
<thead>
<tr>
<th>Defense</th>
<th>Attacker technics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sending IPs blacklist</td>
<td>Snowshoe attacks: Necurs (5-6M, Locky), Mirai (400K)...</td>
</tr>
<tr>
<td></td>
<td><strong>Abuse of good reputation IPs</strong>: hosters (Amazon), webmails (Yahoo!)...</td>
</tr>
<tr>
<td>Sending Domain names blacklist</td>
<td>Domain names created dynamically</td>
</tr>
<tr>
<td></td>
<td>Reuse of old domain names with good reputation</td>
</tr>
</tbody>
</table>
Fingerprints

Detect similar threats
Fingerprint of the email and webpage

<table>
<thead>
<tr>
<th>Defense</th>
<th>Attacker technic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic hash (MD5, SHA1, SHA256)</td>
<td>Make each attack unique: Code obfuscation, code encryption</td>
</tr>
<tr>
<td>Fuzzy hash (Nilsimsa, SSDEEP)</td>
<td>More code obfuscation Code encryption</td>
</tr>
</tbody>
</table>

Avalanche effect: the smallest difference changes completely the cryptographic hash:

\[
\text{MD5(‘helloworld’)} = \text{fc5e038d38a57032085441e7fe7010b0} \\
\text{MD5(‘hello world’)} = \text{5eb63bbe01eeced093cb22bb8f5acdc3}
\]

Fuzzy hash is resilient to a small change: the attacker will do more changes to bypass it.
Fingerprint Obfuscation technics

Making each attack unique

• Key idea: Change content, do not change behavior
  • Inserting random and invisible text
  • Encoding of characters selected randomly
  • Random values of certain HTML attributes (IDs, Class,...)
  • Insert whitespaces
  • Usage of similar colors
Fingerprint obfuscation technics

Confusing legit & malicious content

Embed Marketing content in the email (invisible, very small, or visible but further down)

<html>
[PHISHING CONTENT]
<br><br><br><br>
...
<small><small><small><small><small><small><small>
[MARKETING CONTENT]
</html>
Fingerprint bypass methods

Random Encoding of characters

Enter your email address.

VS

E;&#110;t;&#101;r;&#32;y;&#111;u;&#114; ;&#101;m;&#97;i;&#108; ;&#97;d;&#100;r;&#101;s;&#115;;

VS

&#69;&#110;&#116;&#101;&#114;&#32;&#121;&#111;&#117;&#114;&#32;&#101;&#109;&#97;&#105;&#108;&#32;&#97;&#100;&#114;& #101;&#115;&#115;&#46;

Random values of certain HTML attributes

<input name="fso" value="aWZYY5fkbTMexPe_qMIyD5vvVAGxMU2C_yTFO4Uus9AxyzvNPRzHDU_6rcIERcoEPbR6cW" type="hidden">

<style type="text/css"> ... random ... </style>

<button class=YqqH_76_vTBM type=submit>
Fingerprint bypass methods

Usage of similar colors

<a onmouseDown="alert('Try it a couple of times')"> <font color="#218D7"> </font> </a>

<a onmouseDown="alert('Try it a couple of times')"> <font color="#1F8D8"> </font> </a>
Text Analysis

Detect “lead to action” texts
Text Analysis bypass methods

Bypass text analysis by making the matching impossible

• Phishing email with Image only
• Phishing email with light or no content
• Phishing email with “legit” content leading to a Phishing webpage
• Usage of Homoglyphs
Text Analysis bypass methods

Drag & drop = One image
The global image is the link.
Text Analysis bypass methods

<title>Log in to your PayPal account</title> VS <title>iTunes - Update Card</title>

<title>Log in to your PayPal account</title> VS <title>iTunes - Update Card</title>

<title>Log in to your PayPal account</title> VS <title>iTunes - Update Card</title>
URL Domain filtering

Detect phishing email by identifying malicious link
URL Domain Filtering bypass methods

Bypass Domain Lists by making sure the domain used can’t be blacklisted

• Usage of shorteners (bit.ly, goo.gl,...)
• Usage of sub domains from website domain providers (weebly, 000webhost.com,...)
• Abuse of redirect mechanisms (cf Newsmax, Walmart,)
URL Domain Filtering bypass methods

Shorteners are highly used
URL Domain Filtering bypass methods

Abuse of redirect mechanisms / subdomains

http://news.newsmex.com/?KKIDX2exP4xyTpGwxqFvyW2nfsyDtJIZK&http://%E2%93%96%E2%93%9E%E2%93%9E.%E2%93%96%E2%93%9B/aaPajS

http://wmxemail.walmart.com/track?type=click&mailingid=94z_6-0-0-0-optcr_201707007&userid=-0225249577&extra=&amp;http://ec2-54-212-231-1.us-west-2.compute.amazonaws.com/?NzM1NTk4Nz9MnJc9NSy0OTQyMjc9MjUmMzQ9Y2xpY2smMWo3emYzPTEmbGlkPTI1MjQ=

http://exch.quantserve.com/r?a=p-qpUzqbsCMFypz;labels=_qc.clk,_click.adserver.rtb,_click.rand.21220;rtbdata2=EAgaGElFX0JyaWdodFRBTEtfVNVfQXBzMyAxNiCnxRkoo8wNMJSPNDo3aHR0cDovL3NpdGUtdW5rbm93bi5weVJsaXNoZXItOTQ0NC0xOTY3MjUvYW5vbmltb3VzLmFybFoobUE4WVNwMEpTUjZBRDNCRGZfOVdRTGMpW2guYTJoMyAgBjI3TAroBI3VDRjU1RjhGNTFFNzgwMDYzQzgwNjdDRkYzN0FDRTVGwAGA-S31AeLhh7fBKtoBEjU5MDk3MDC0NjEZnJmMzQ1MOUBJW1PegBZJgc_8wNgAIGqAIpASIugIEwLhAVMACAsqCANAC4Ojb04yY0-22AeACAQ;redirecturl2=lc.cx/NxFx

https://ddeabt.weebly.com/

https://u2inbox.weebly.com/

...
A real-life phishing attack
Real-Life phishing attack - The sample
Real-Life malware attack - The web page
Real-Life malware attack - The sending pattern

2530 Samples

246 shared Microsoft Office 365 IPs
110 different From Emails
5 different useful links
5 different webpages
Real-Life phishing attack - The sample

Apple <notice.mailboxapplidshp@appleitunnesnotifid.onmicrosoft.com>
Real-Life phishing attack - The sample
Real-Life phishing attack - The sample
Real-Life phishing attack - The sample
Real-Life phishing attack - The sample
Real-Life phishing attack - The sample

Hidden marketing content
Real-Life phishing attack - The sample

Random HTML Banners
Real-Life phishing attack - The sample

And a few useless legit URLs ...

https://www.youtube.com/watch?v=3pDSxs3AGzA3EnDJ00w
Real-Life malware attack - The web page

ASCII Encoding

Homoglyphs

Randomization of the encoding
Real-Life phishing attack - The sample

Method used in this Phishing:

- Snow Shoe Technique of sending
  +
- Real Phishing Content
  +
- Usage of shared IPs (Microsoft)
  +
- Content Randomization
  +
- Disturbing Content / Noise

Hidden Content with Legit Text
  +
- Hidden Content with Real Marketing
  +
- Visible Content with Real Marketing
  +
- Homoglyphs
The answer
How does the army analyze threats in critical situations?

Origin of the threat

Context of the threat

Content of the threat
How do email security leaders fight threats today?

- Origin of the threat: IP/Domain reputation
- Content of the threat: Fingerprint & Sandboxing
- Context of the threat: ??
Combining a Global Analysis with a Local Analysis using predictive technologies

<table>
<thead>
<tr>
<th>Machine learning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral analysis</td>
</tr>
<tr>
<td>Artificial intelligence</td>
</tr>
<tr>
<td>Predictive Models</td>
</tr>
<tr>
<td>Real-time reputation</td>
</tr>
<tr>
<td>Counter-measure detection</td>
</tr>
<tr>
<td>Web page exploration</td>
</tr>
<tr>
<td>Domain name exploration</td>
</tr>
</tbody>
</table>
Security is at the Border Gateway + Front

Phishing/Spam/Malware.

Detected by Contextual Analysis.

Classification of Marketing & Transactional Emails

Safe Unsubscribe process to protect users against Fake Unsubscribe links and Address validation by Spammers

Time of Click AntiPhishing Analysis to protect against Time Bombing Phishing
Thank you

Adrien GENDRE
Chief Solution Architect
+1 (415) 509-2025
adrien.gendre@vadesecure.com