CATCHING PHISHERS BY THEIR BAIT
INVESTIGATING THE DUTCH PHISHING
LANDSCAPE THROUGH PHISHING
KIT DETECTION

Hugo Bijmans, TNO
Tim Booij, TNO
Anneke Schwedersky, TNO
Arià Nedgabat, TU/e
Rolf van Wegberg, TU Delft
PHISHING IN 2021

NOT ALL PHISHERS SHARE SAME OBJECTIVES

Catching Phishers by Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection | 30th USENIX Security Symposium
LIFE CYCLE OF A PHISHING CAMPAIGN

5 STEPS TO A SUCCESSFUL EXPEDITION

1. Acquire phishing kit
2. Acquire domain name
   - Hijack insecure website
   - Buy a new domain name
3. Acquire hosting service
4. Acquire TLS certificate
   - 78% is served over HTTPS in 2020 (AWPG)
5. Send out phishing bait
PHISHING KITS 
AND WHERE TO FIND THEM

TELEGRAM

- We gathered 46 phishing kits from 50 public fraud-related Telegram channels
- Automatically downloaded 24 phishing kits from open server directories
- Manually examined the source code of all kits to create fingerprints

Files
rabobank/background.png
adminpanel/the_manual.txt
kTx4Jgh9H.php
phishpanel.html

Strings
That’s why you have to update your banking app and activate it again
### IDENTIFY POSSIBLE PHISHY DOMAINS

Real-time monitoring of a stream of TLS certificates, calculate a score based on a number of features:

<table>
<thead>
<tr>
<th>Domain feature</th>
<th>Example &amp; references</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious TLDs</td>
<td>.xyz,.icu,.top [16,41]</td>
<td>20</td>
</tr>
<tr>
<td>TLD as subdomain</td>
<td>x.com.domain.net [16,27]</td>
<td>20</td>
</tr>
<tr>
<td>Brand name</td>
<td>brand.domain.net [16,27]</td>
<td>40-150</td>
</tr>
<tr>
<td>Typosquatted brand</td>
<td>paypal.com [22,27]</td>
<td>0-110</td>
</tr>
<tr>
<td>Suspicious keyword</td>
<td>login.verify [27,31]</td>
<td>25-50</td>
</tr>
<tr>
<td>Hyphens count</td>
<td>brand-n--ame.net [18,27]</td>
<td>3x</td>
</tr>
<tr>
<td>Subdomain count</td>
<td>sub.x.domain.net [27,32]</td>
<td>3x</td>
</tr>
<tr>
<td>Free certificate</td>
<td>Let’s Encrypt [16,48]</td>
<td>20</td>
</tr>
<tr>
<td>Fake www</td>
<td>wwwbrand.com [22]</td>
<td>45</td>
</tr>
</tbody>
</table>
Catching Phishers by Their Bait: Investigating the Dutch Phishing Landscape through Phishing Kit Detection | 30th USENIX Security Symposium

Keep monitoring for 7 days

**DOMAIN CRAWLER**

**CAPTURE ATTRIBUTES AND DETECT KITS**

1. Crawl domain online?
2. Download all resources
   - Landing URL
   - HTML
   - Favicon
   - IP address
   - WHOIS
3. False positive check
   - Favicon check *(Cheng et al. 2013)*
   - Default/empty pages
4. Phishing kit detection
   - Loaded resources
   - wFuzzing analysis
   - String matching
1.363 phishing domains found
31 phishing domains online on average every day
.info is the most popular TLD
56% of domains did not refer to a Dutch bank
73% was registered through Namecheap
1. 1.363 phishing domains found
2. 31 phishing domains online on average every day
3. .info is the most popular TLD
4. 56% of domains did not refer to a Dutch bank
5. 73% was registered through Namecheap
6. Installation times line up nicely with Dutch circadian rhythm!
TTP IN DUTCH PHISHING LANDSCAPE
SEPTEMBER 2020 – JANUARY 2021

- 24 hours median uptime, 45 hours on average
- 3 hours until domains is online after domain registration
- 1 hour later, the phishing kit is installed successfully
- 40 hours after registration, the domain is offline
- Phishers must act fast!
TTP IN DUTCH PHISHING LANDSCAPE
SEPTEMBER 2020 – JANUARY 2021

PHISHING KIT DEPLOYMENTS

› uAdmin is the most popular phishing kit framework (64%)
› Only 7.6% of the phishing websites load external resources
› 69% of all domains returned a blank screen to hide themselves

› Phishers have increased their capabilities by using decoy pages

› Validation with APWG eCrime Exchange data
  › Only 77 domains overlapping
  › On average 11.3 hours earlier
**TAKE AWAYS**

**A CLEAR OVERVIEW**

**TTP IN DUTCH PHISHING LANDSCAPE**

- Methodology to derive in-depth insights into a phishing landscape
- New realm of domains previously not identified
- Discovered faster, enabling interventions before victim arrive

- Phishers have increased their capabilities by using decoy pages
- uAdmin is a very popular framework to build phishing pages upon
- The creator is arrested by Ukrainian police in February, 2021

- In-depth knowledge of used phishing kit and their popularity can assist LEA to prioritise their anti-phishing effort
CATCHING PHISHERS BY THEIR BAIT
INVESTIGATING THE DUTCH PHISHING LANDSCAPE THROUGH PHISHING KIT DETECTION

Hugo Bijnans, TNO
hugo.bijnans@tno.nl
Tim Booij, TNO
Anneke Schwedersky, TNO
Aria Nedgabat, TU/e
Rolf van Wegberg, TU Delft