Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits

Brian Kondracki, Babak Amin Azad, Oleksii Starov and Nick Nikiforakis
The Value of Stolen Data

Phishing vs. Malware

- Spotify Account: $2.75
- Hulu Account: $2.75
- Netflix Account: $1.00 - $3.00
- Driver's License: $20.00
- Credit Card: $8.00 - $22.00
- Email Address & Password: $0.70 - $2.30
- PayPal Credentials: $1.50
- Social Security Number: $1.00
- Medical Record from Large Scale Attack: $1.50 - $10.00
- Complete Medical Record: Up to $1000.00

Anatomy of a Traditional Phishing Attack

• Attackers manually copy/recreate web content from target website

• Phishing content served from attacker-owned web server
  • Or a compromised web server

• Links to phishing webpages dispatched to victims through email or SMS
Limitations of Traditional Phishing

• Implementation errors can lead to detection
• Webpages update at increasing speeds
• Detection by anti-phishing scanners leads to immediate blocklisting
Man-in-the-Middle (MITM) Phishing Toolkits

- Malicious reverse proxy servers
  - Victims see live content from target website
  - Credentials stolen in transit
- Popular MITM phishing toolkits today:
  - Evilginx
  - Muraena
  - Modlishka
MITM Phishing Toolkit Demo
MITM Phishing Toolkit Threat Model

- Attackers control *all* application layer content
- Cloaking restricts access to phishing content
- Detection cannot rely on integrity of application layer content
MITM Phishing Toolkit Threat Model

- Attackers control *all* application layer content

Fingerprint the server, not the content
Network-Level Phishing Detection

• Network architecture can be leveraged to discover presence of toolkits
  • Network timing analysis
  • TLS fingerprinting
• Fingerprinting possible from both ends of the communication channel
Network Timing Analysis

Figure Taken From: Daniel Alexander, "Inferring the Presence of Reverse Proxies Through Timing Analysis" (2015)
Network Timing Analysis

HTTP

HTTPS

GET/SYN RTT Ratio

GET Error/SYN RTT Ratio

GET/SYN RTT Ratio

GET Error/SYN RTT Ratio

Dataset

Evilginx
Modlishka
Muraena
Known Direct
TLS Fingerprinting

• MITM phishing toolkits utilize unusual TLS stacks
  • TLS versions supported
  • TLS libraries¹

¹ https://github.com/WestpointLtd/tls_prober
MITM Phishing Toolkit Groundtruth

• We are the first to conduct a comprehensive study on MITM phishing toolkits
  • No groundtruth dataset on MITM phishing toolkit behavior
• Collected network-level data from 30 globally-distributed nodes
  • Recorded all permutations of client → MITM phishing toolkit → webserver
  • 146,160 data points in total

• Random forest classifier
  • Achieved 99.9% accuracy and five-fold cross validation score of 99.9%
PHOCA: MITM Phishing Website Detector

- Framework to collect network-level data on, and detect MITM phishing websites
- Named after the Latin word for seal
  - Known to use vibrations in water to detect otherwise hidden prey
1. Candidate domains sourced from Certificate Transparency Logs and anti-phishing blocklists
2. Scheduler module dispatches worker nodes to retrieve classification from PHOCA, and screenshot/HTML code using Selenium.
Phishing Website Crawling Infrastructure

3. Collected data fed into analysis module for further processing
4. Recrawling module periodically revisits websites of interest
MITM Phishing Toolkits on the Web

- Data collection period from March 25th, 2020 to March 25th, 2021
- 841,711 web pages analyzed
- 1,220 MITM phishing toolkits identified
# MITM Phishing Website Targets

<table>
<thead>
<tr>
<th>Brand</th>
<th># Websites</th>
<th>Example Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instagram</td>
<td>298</td>
<td>m.logins-instagram.ga</td>
</tr>
<tr>
<td>Google</td>
<td>249</td>
<td>accounts.google-2fa.com</td>
</tr>
<tr>
<td>Facebook</td>
<td>198</td>
<td>sign-in.facebookes.com</td>
</tr>
<tr>
<td>Outlook</td>
<td>92</td>
<td>login.outlooks-mail.com</td>
</tr>
<tr>
<td>Paypal</td>
<td>84</td>
<td>paypalsecured.com</td>
</tr>
<tr>
<td>Apple</td>
<td>76</td>
<td>apple.icloud.com.ssl.host</td>
</tr>
<tr>
<td>Twitter</td>
<td>63</td>
<td>login.mobiletwitter.tk</td>
</tr>
<tr>
<td>Coinbase</td>
<td>56</td>
<td>googletag.coinbasel.com</td>
</tr>
<tr>
<td>Yahoo</td>
<td>50</td>
<td>yahoo.com.msg-inbox.ga</td>
</tr>
<tr>
<td>Linkedin</td>
<td>41</td>
<td>linkedin.com.securelogin.xyz</td>
</tr>
</tbody>
</table>
MITM Phishing Domain Types

Diagram showing the percentage of domains targeting different trademarks, categorized into three types: Comboquatting, Target Embedding, and Typosquatting.
MITM Phishing Website Lifecycle
MITM Phishing Website Lifecycle

MITM phishing use freshly registered domains
MITM phishing websites are weaponized immediately after TLS certificate creation
20% of MITM phishing websites remain active for longer than 10 days
MITM Phishing Website Lifecycle

43.7% of domains and 18.9% of IP addresses appear on blocklists
Case Study: Palo Alto Networks

• 56.7% of MITM phishing domains labeled as malicious by PAN in-line scanners
  • 15.1% received label at least one week after our initial discovery
• 6,403 customer requests directed towards 260 phishing websites over six months
  • Originating from 368 distinct firewall devices
Server-side TLS Fingerprinting

• MITM phishing toolkits do not utilize common web client TLS stacks
  • Forwarded HTTP User-Agent strings do not match TLS fingerprints
• JA3 TLS fingerprinting\(^1\) utilized to identify unique TLS implementations
• Purchased 13,000 advertising impressions from a popular advertising service
  • Collected 163 unique TLS fingerprints from 4,311 distinct HTTP User-Agents
• TLS fingerprints of MITM phishing toolkits unique in this dataset

\(^1\) https://github.com/salesforce/ja3
Countermeasures

• Users:
  • Analyze the primary domain of any suspicious URL encountered
  • Use U2F to secure online accounts

• Online Services/Anti-phishing Entities:
  • Look for discrepancies in client TLS fingerprints
  • Utilize network-level detection techniques when searching for phishing websites
Conclusion

- MITM phishing toolkits allow attackers to launch highly effective phishing attacks
- Unique architecture allows for fingerprinting at the network layer
- We found 1,220 MITM phishing toolkits operating in the wild, targeting real users
- Anti-phishing ecosystem does not effectively capture MITM phishing toolkits

Code and data: https://catching-transparent-phish.github.io

Thank you for your time! Any questions?
BACKUP SLIDES
MITM Phishing Toolkit Classifier

• Trained random forest classifier on data from real websites and MITM phishing toolkits

• Achieved 99.9% accuracy and five-fold cross validation score of 99.9%
Here, our classifier correctly identifies our deployment of Evilginx as a 2FA phishing website. Lastly, let’s classify a real-world deployment of Evilginx we found during this study.