Talk00: Phishing, Phishing kits, and Rudimentary Analysis of Phishing E-mails

Acknowledgment of Country

We acknowledge the Larrakia People as the traditional custodians of the lands on which we meet. We pay our respects to their Elders past, present, and emerging.

~$ whoami

Obligatory Disclaimer - Views and opinions expressed within the content are solely my own and do not reflect the opinions and beliefs of my employer, it's affiliates, nor CrocSec!

- I'm just another cyber security practitioner.
- I have a keen interest in all thing information security.
  - `https://www.linkedin.com/in/kushfj`
  - `https://github.com/kushfj/`
  - `https://keybase.io/kush`

Overview

- Introduction – What is Phishing
    - Taxonomy
    - Anatomy
- Phishing Kits
- Basic Analysis of Phishing Emails
- Challenges
- Summary

What is Phishing?

- Social Engineering
- Initial Access
- Digitally/electronically delivered
- “Trick” targets into revealing actionable information
    - Financial
    - Credential/Access
    - Identity
- “Verizon 2024 Data Breach Investigations Report” - https://www.verizon.com/business/resources/reports/dbir/
    - Median time for phish is 60-seconds after a user receives a phishing e-mail
    - 73% of breaches attributed to phishing and pretexting (40% pretext and 33% phishing)

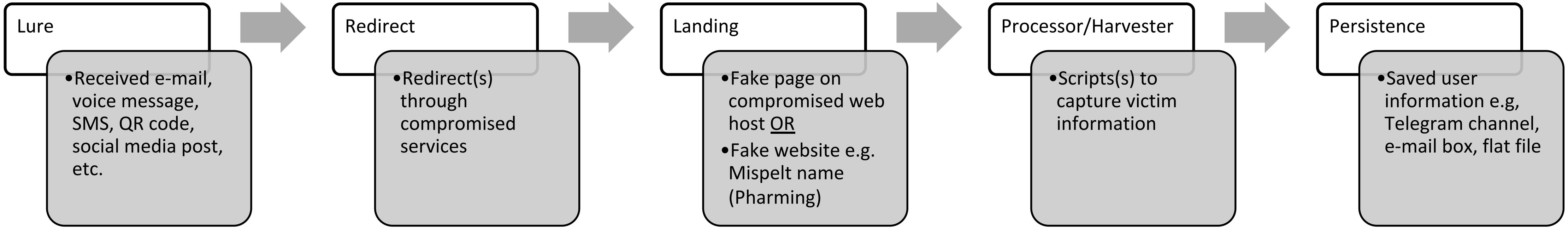
Phishing Taxonomy

- Intent – actionable information (*ishing), solicitation (SPAM/pretexting), malware (mal-SPAM)
- Targeting – mass/random (*ishing), specific (spear-phishing/whaling)
- Delivery – e-mail (phishing), SMS (smishing), voice (vishing), QR (quishing/QRishing), social media (angler phishing)
- Volume – none (pharming), low (angler phishing), medium (phishing), high (snow-shoeing/hail-storming)
- Pretext – none (pharming), low (angler phishing), medium (phishing), high (spear-phishing/whaling)
- Effort – manual (clone phishing/cloning), framework (kit)

Common Phishing Components

- Lure (except Pharming)
  - Enticement – subject, all to action, urgency, authority
  - Impersonation – spoofing, branding
  - Payload (except Quishing/QRishing sometimes)
    - Links
    - PDF Attachments
- Redirects (sometimes multiple) – HTTP, HTML, Javascript
- Landing – cloned site/pages
- Processing/Harvesting – “next.php”
- Persistence – local (file, database) vs. remote (database, file, e-mails, telegram, slack)

Common Phishing Components



Lure

- Received e-mail, voice message, SMS, QR code, social media post, etc.

Redirect

- Redirect(s) through compromised services

Landing

- Fake page on compromised web host OR
- Fake website e.g. Mispelt name (Pharming)

Processor/Harvester

- Scripts(s) to capture victim information

Persistence

- Saved user information e.g, Telegram channel, e-mail box, flat file

What are Phishing Kits?

- Software archive (.zip) of scripts (JS, PHP) and templates (HTML, CSS)
- Different types – low-code/no-code vs. PHaaS
- MVP kit = landing page + processor
- Frameworks = ability to generate lure templates, landing page, processor, and customize persistence (limited shelf-life for some)
- Anti-detection/evasion/Cloaking
  - HTTP headers (Referrer, User-agent, Accept-Language),
  - IP address/Geo-location permitting,
  - Blocking known bots and scanners,
  - Delayed activation (post-delivery weaponization) – content replacement, shortener destination update
- Anti-analysis
  - Code obfuscation
  - URL/link obfuscation

Isn’t Phishing a Solved Problem?

- Secure e-mail gateways
- E-mail spoofing – SPF, DKIM, DMARC
- MFA – but Evilginx Framework
  - Monkey-in-the-middle for credentials and session data

Basic Analysis of Phishing e-mails

- Read the ”raw” content of the e-mail
- Check the SPF and DKIM headers
- Check the sender IP address
- Manually inspect any links or attachment (do not open attachments) – what does it look like and what is it capturing
- Identify domain owner (`whois`)
- Identify network operation (`whois -h whois.cymru.com “-v` *`n.n.n.n`*”)

Basic Analysis of Phishing e-mails

- Hide your details (user agent, IP, etc.)
  - https://www.useragents.me/
  - VPN
  - Online scanners – see useful resources
- Follow redirect
- Examine landing page
- Attempt to identify processor/harvester
- Sometimes you can find the kit (.zip)
- Request take-down

Worked Example

- I haven’t had any recent phishing e-mails ☹
- Some kits leave the `.git` directory in there
  - `git show HEAD`

Useful Resources

- Lots of free tools
- Checkphish.ai - https://checkphish.bolster.ai/
- PhishTank - https://www.phishtank.com/index.php
- URLScan – https://urlscan.io
- URLVoid - https://www.urlvoid.com/
- etc. etc.

Common Controls

- Training and Awareness
- Access control and account management
- Secure e-mail gateways
- Information sharing
  - Phishtank
  - Phishhunt

Challenges

- Use of legitimate services e.g., URL shortening services, file hosting, website hosting, etc.
- Changing delivery methods i.e., increasing smishing and angler-phishing
- Increasing manual analysis effort due to cloaking and obfuscation – does not scale well
- Take-down requests can be delayed

Summary

- Phishing – taxonomy, anatomy, kits.
- Mitigation – user training, SEG (SPF, DKIM, DMARC), EDR, content blocking, IDAM.
- Detection – logs (application, proxy), network traffic (content).
- Challenges – scaling.

Thank you