ANALYZING PHISHING DOCUMENTS 101

Source Zero Con

// May 2021
id -un && id -Gn

David Forsythe – 0xdf

Training Architect at HackTheBox
● Develop Machine and Challenge Content
● Develop Automations to support the platform

Previous experience:
● SOC / CIRT / Hunt / Blue Team / Red Team / Threat Intel / Researcher
● Public and private sector

CTF addict

Author of 0xdf Hacks Stuff @ 0xdf.gitlab.io
i ❤ phishing docs

- Common real-world access vector
- Constantly evolving
- Entry-level skillset - not that high!
- Battle of creativity
phishing documents

- Files that don’t **typically** execute code
- Not executable / script files (.exe, .vbs, .js, .ps1, .src, .bat, .com)
- Not links to fake login pages
to what end?

• Block at firewall

• Tune defensive collection

• Tune defensive blocks
How is this document executing?
tools

- Native Viewer (Office, Adobe, etc)
- Zip
- Didier Stevens Suite
  - oledump
  - pdfparser
- olevba
Always handle potential malware with care. Use a VM. Disconnect it from the internet.
zip (microsoft office file formats)

2003 (and Before)
- Compound File Binary Format (CFBF)
- .doc, .xls, .ppt
- Still works in all version of office
- most common in phishing

2007+
- Office Open XML
- .docx, .xlsx, .pptx, .docm, .xlsm, .pptm
- Just a Zip archive with XML in it
  - (Almost) everything in plaintext
Demo:
Alien Phish
Didier Stevens **Suite**

- Treasure trove of tools / utilities
- Writeups / videos for SANS Internet Storm Center
- Start with:
  - oledump.py
  - pdfid.py / pdf-parser.py
olevba

- Part of oletools (on GitHub, `pip install python-oletools`)
- Detect / Extract VBA Macro source
- Highlights on known malicious patterns
- Highlights common obfuscation methods
- Command line or Python module
deobfuscation resources

- VBA editor / debugger in Office (alt+f11)
  - Remove unused variables
  - Remove commented lines
- JSNice – Javascript deobfuscator
- CyberChef – All around decoder / cyber utility knife
- `echo` commands in front of obfuscated DOS
- Replace `iex` with `echo` in PowerShell
practice resources

- VirusTotal (not free 😞)
  p:3+ p:10- type:doc

- malware-traffic-analysis.net

- SANS ISC Diaries

- CTF Challenges

Be careful with real malware!
CTF Challenges

Hack The Box has 3 phishing challenges in Forensics Category

<table>
<thead>
<tr>
<th>Challenge</th>
<th>User Rating</th>
<th>Points</th>
<th>User Solves</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>emo</td>
<td></td>
<td>40pts</td>
<td>689</td>
<td>190</td>
</tr>
<tr>
<td>oBfsC4t10n2</td>
<td></td>
<td>70pts</td>
<td>1082</td>
<td>292</td>
</tr>
<tr>
<td>oBfsC4t10n</td>
<td></td>
<td>60pts</td>
<td>1416</td>
<td>399</td>
</tr>
</tbody>
</table>
Demo: Phish in a Barrel
Hands on Training - Next Level

Dedicated Labs
**PRACTICAL TRAINING & READINESS**
Exclusive training environment. Countless labs, latest exploits.

Professional Labs
**ENTERPRISE ATTACK SIMULATION**

Academy For Business
**ONLINE CYBERSECURITY COURSES**
Guided training for any skill level. Offensive, Defensive, General

Business CTF
**UPSKILLING THROUGH GAMIFICATION**
Gamified hacking challenges. Learning and team-building at once.

Talent Search
**RECRUIT TOP TALENT**
Global cybersecurity talent pool. Post jobs and recruit talent.

Trainings & Workshops
**TAILORED LEARNING EXPERIENCE**
Off and on-premise. Diligently created to meet your team’s needs.
THANK YOU!

Contact:
sales@hackthebox.eu

twitter: 0xdf_
slack: 0xdf #7486