Red Team Apocalypse

Beau Bullock (@dafthack)

Sobre la charla

- La perspectiva del Red Team:
  - La organizacion objetivo tiene los ultimos productos: EDR/BA/AV
  - La Ingenieria social standard no funciona

- La perspective del Blue Team:
  - El ultimo pentest salio bien
  - No se encontraron vulnerabilidades criticas
  - Sistemas parchados, controls de acceso de red, application whitelisting, etc…
  - Pero…
    - …La organizacion encuentra una base de datos critica siendo vendida en la dark web (o en Wilson) . Que paso ?

About

- Pentest/Red Team en Black Hills Information Security
- Con certificationes por SANS, OffSec, y otros…
- Organizador de CitySec Meetup
- Podcasts
  - Tradecraft Security | Weekly, Hacker Dialogues | CoinSe
- Entusiasta avido de OWA

Original Pentest Apocalypse

- Vulnerability Management Program
- Group Policy Preferences
- Widespread Local Administrator Account
- Weak Passwords (Password Spraying)
- Over Privileged Users

- Sensitive Data in File Shares
- Intranet Information Disclosure
- NetBios and LLMNR Poisoning
- Local Workstation Privilege Escalation

Red Team vs Pen Test

- Un Pentest tradicional busca encontrar la mayor cantidad de vulnerabilidades en el tiempo establecido
  - Usar herramientas COTS tools como scaners de vulnerabilidades
  - Generalmente no preocupa alertar al blue team
- Las pruebas Red Team simulan adversarios reales enfocados en lograr un objetivo.
  - Se tiende a usar backdoors y herramientas propias
  - Se intenta pasar desapercibido y no alertar al blue team

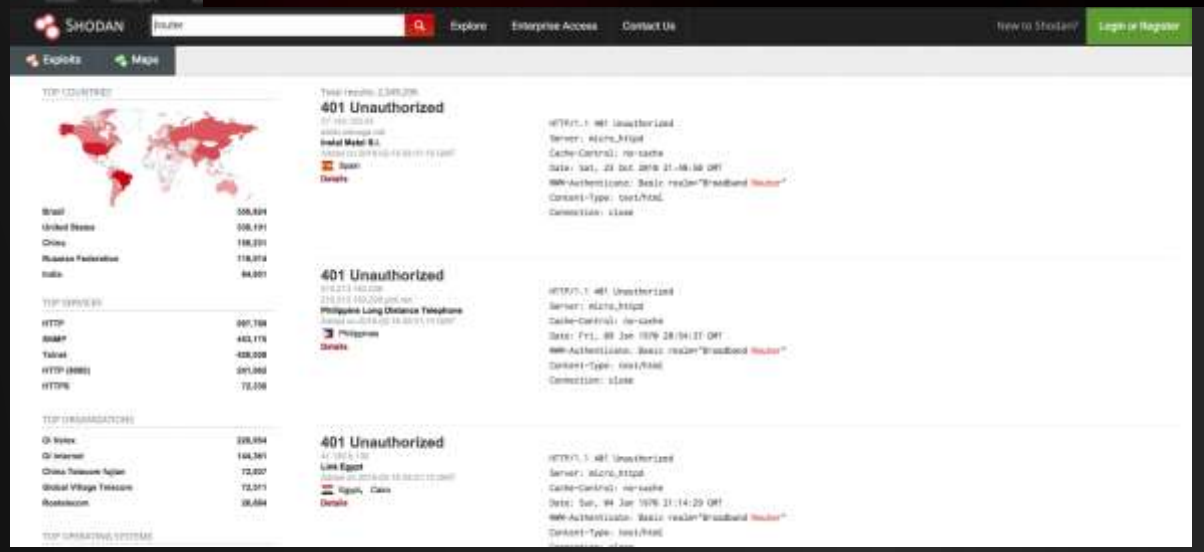
Red Team Methodology

- Reconnaissance
- Compromise
- Persistence
- Command and Control
- Asset Discovery
- Privilege Escalation
- Lateral Movement
- Actions on Objectives

Reconnaissance

External Recon

- Passively discover:
  - External hosts
  - Contacts at target organization
- Usan infrastructura en la nube ? O365, Amazon AWS, Google G-Suite, etc…
- Recon-NG
- Shodan
- LinkedIn



PowerMeta

- Descubriar archivos expuestos publicamente
- Extraer metadata
- Provee informacion de
  - La nomenclatura de usuarios (jperez vs perezj)
  - Nombres de equipos
  - Informacion del Domain (Active Diretory)
- https://github.com/dafthack/PowerMeta

```
PS C:\> Invoke-PowerMeta -TargetDomain "[redacted].com"

[*] Searching Google for 'site:[redacted].com filetype:pdf'
[*] Now Analyzing page 1 of Google search results (100 results per page)
[*] Searching Bing for 'site:[redacted].com filetype:pdf'
[*] Now Analyzing page 1 of Bing search results (30 results per page)
```

```
[*] Extracted 'Author' and 'Creator' metadata

"C:/Users/beau/Desktop/PowerMeta/2017-04-05-113740/Artifacts
"[redacted]"
%2[redacted]df"
%2[redacted]ion
Adobe InDesign CS3 (5.0.2)
AutoBVT
c[redacted]d
[redacted]
Dennis [redacted]
k[redacted]r
Microsoft┬« Word 2010 Subscription
Microsoft┬« Word 2013
[redacted]
```

Possible Usernames

Full Name

Compromise

Email Attacks

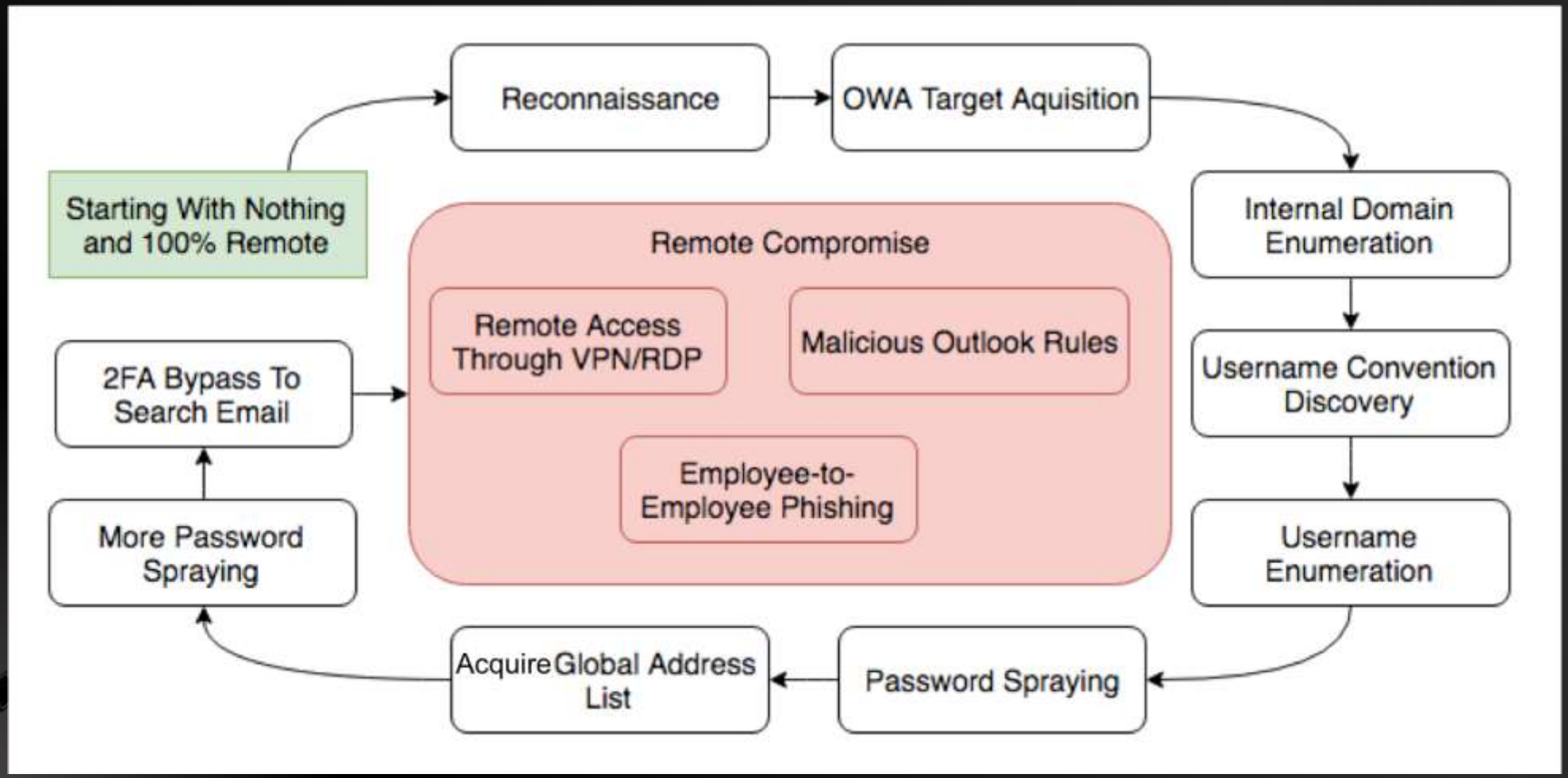
Business Email Compromise

- Los portals externos de correo (webmail)
  - Incluso si usan 2 factores de autenticacion
  - OWA I’m looking at you
  - Servicios en la nube tambien son objectivos(Gmail, O365, etc.)
- Pentesters pueden ignorar sistemas de correo como objectivo
  - Atacantes maliciosos (y Red Teamers) no
- Los servidores de correo son un gran fuente de informacion para un atacante para entender la red interna

Business Email Compromise

- MailSniper
  - https://github.com/dafthack/MailSniper
- Enumeracion de usuarios / dominio
- Password Spraying
- Descarga del GAL (Global Address List)
- Descubre Open Inbox delegation
- Permite buscar texto en correos como passwor
  2FA codes, etc…
- Salta algunos productios 2FA al conectarse directamente a EWS (Exchange Web Services) en vez de OWA

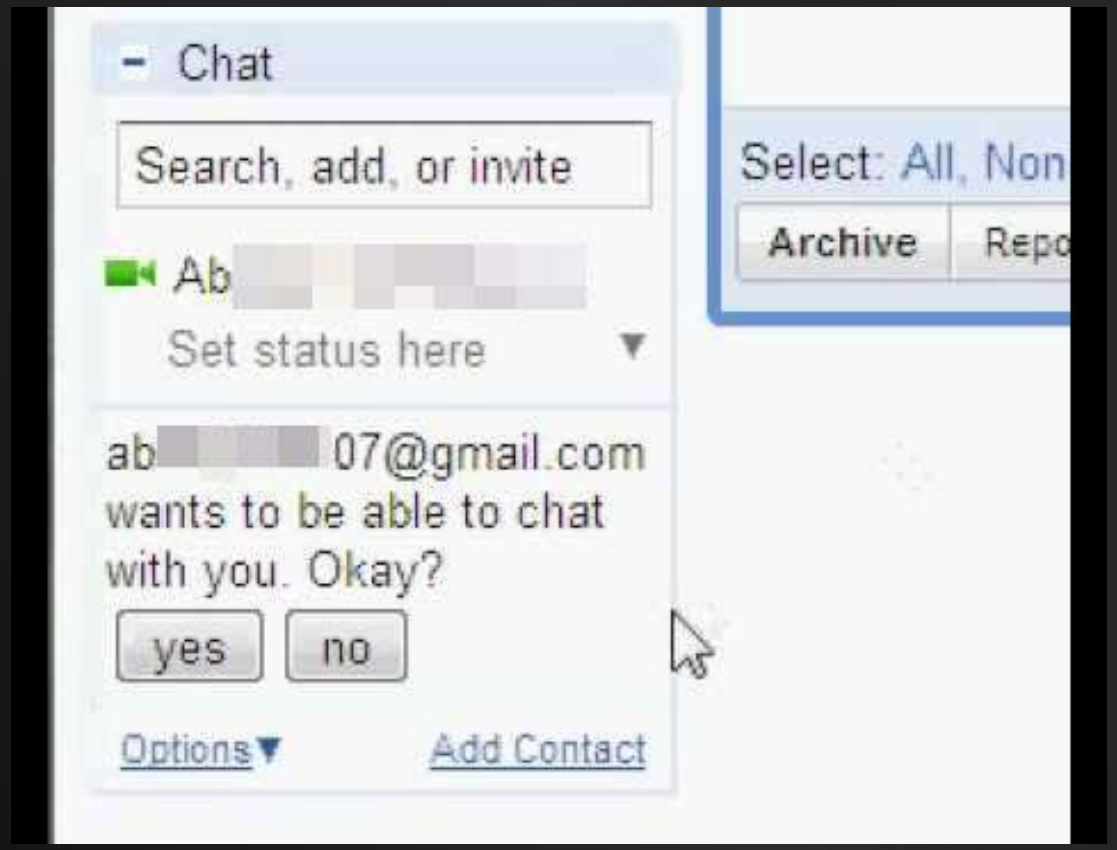
OWA Attack Flow



Red Teaming G-Suite

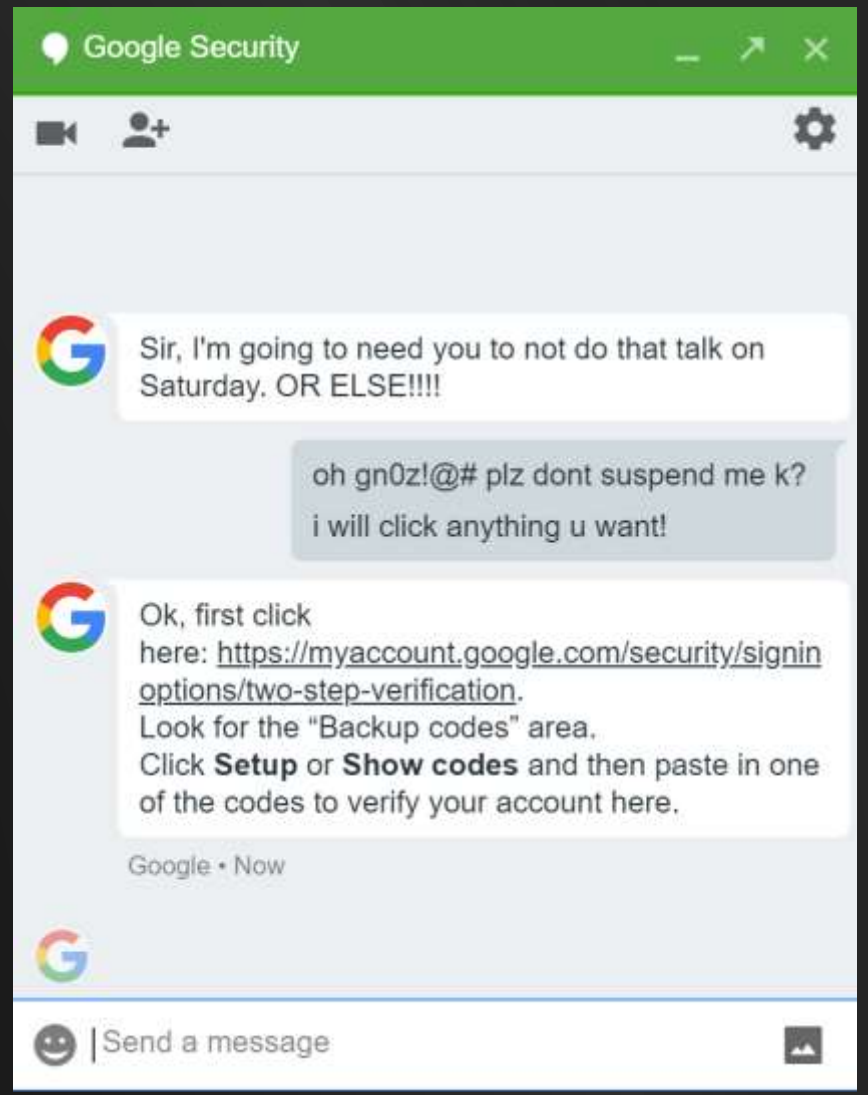
Google Hangouts Ruse

- Remember this? ---------->
- Una invitacion a chatear en Gmail
- Aparentemente esto era mucho trabajo para algunos usuarios



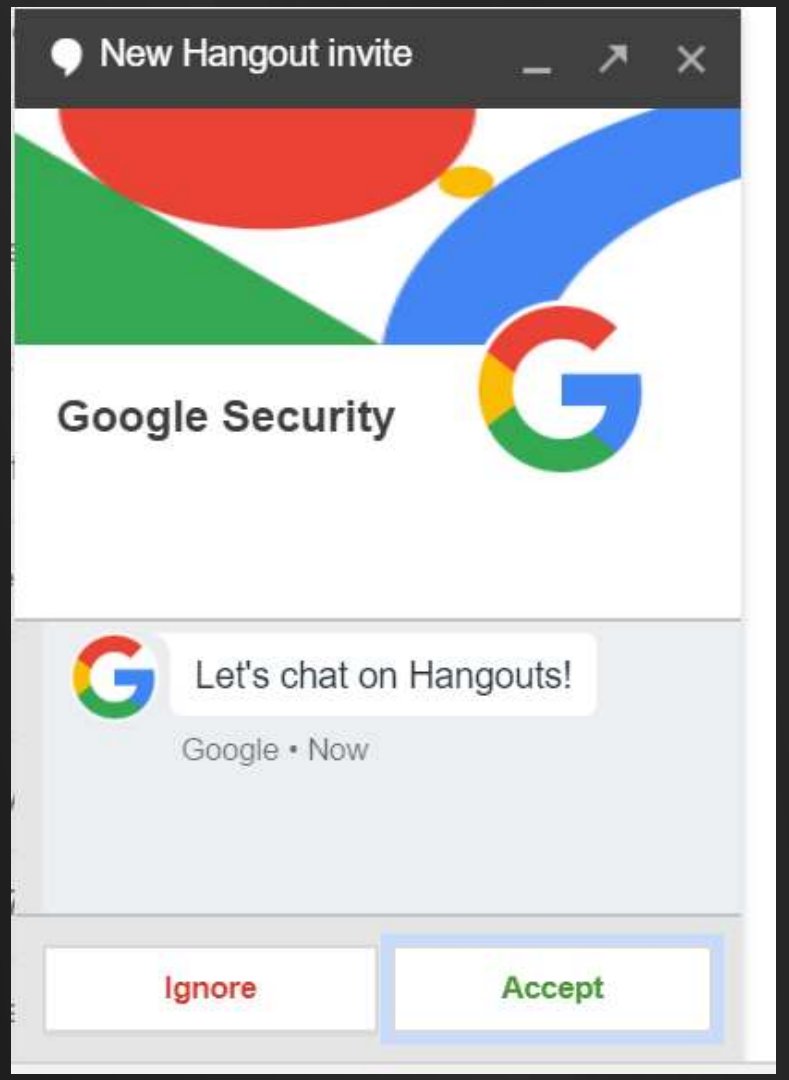
Google Hangouts Ruse

- Ahora, Google Hangouts permite chatear sin tener que aprobar
- Solo se necesita tener el correo
- Puedes enviar un mensaje aparentando ser alguien mas
- Di hola, envia un link, roba credenciales y/o obtienes una shell



Google Hangouts Ruse

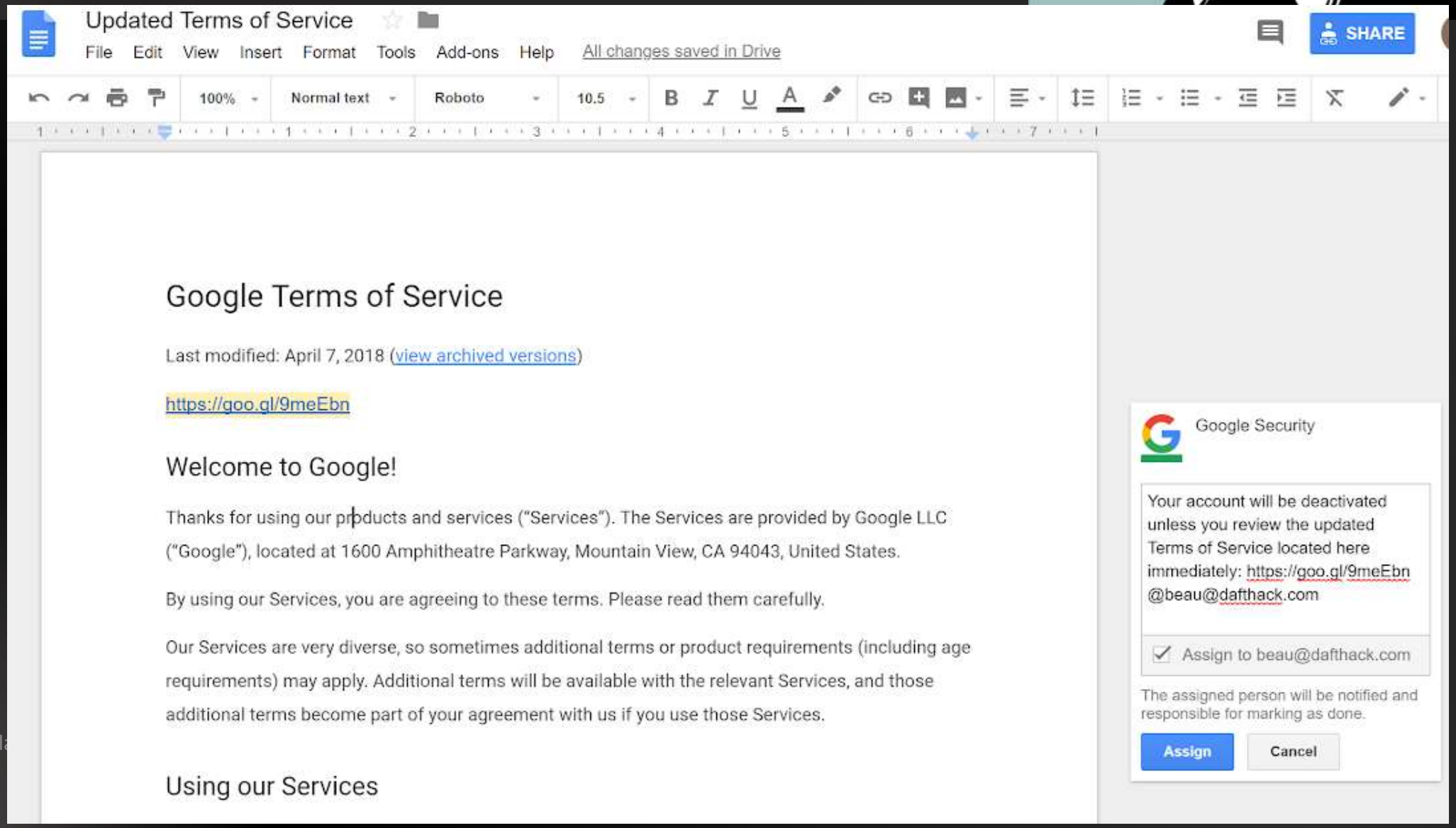
- Puedes cambiar los settings para requirir ver una invitacion
- Pero incluso con eso, impersonar a alguien es posible
- Para configurar invicationes:
  - Hangouts.google.com, click hamburger menu in top left, Settings, “Customize Invite Settings”, switch all to “Can send you an invitation”
- There doesn’t appear to be a global option for locking down accounts across an org



Google Doc Ruse

- Que tal si logramos que google envio un correo de phising por ti ?
- Google Docs es perfecto para esto
  - Crea un Google Doc con un nombre llamativo como “Critical Update Pending”
  - Anhade contenido y un comentario al doc con tu link phishing
  - En el comentario, escribe la direccion de la victima con el prefijo “+” *(i.e. +hacker@gmail.com)* then check ‘Assign’
  - Google enviara un correo a tu objectivo desde <random-string>@docs.google.com

Google Doc Ruse



Google Doc Ruse

Updated Terms of ... - Your account will be deactivated unle... Inbox x

Google Security (Google Docs) <d+MTA4NzU0OTQ5MzgwMzMxODExMjAz-MTAxNzU3NjU5OTAzMDExMDMwNTA1@docs.google.com>
to me

Google Security assigned you an action item in Updated Terms of Service

Google Security

https://goo.gl/9meEbn

Your account will be deactivated unless you review the updated Terms of Service located here immediately: https://goo.gl/9meEbn
+beau@dafthack.com

Assigned to you

Open

1 file with action items assigned to you View file

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

You have received this email because you are mentioned in this thread. Change what Google Docs sends you. You can reply to this email to reply to the discussion.

Google

Google Calendar Event Injection

- Silencioamente inyecta eventos en un calendario
- Crea urgencia a traves de recordatorios
- Incluye un link malicioso
- An email isn’t necessary, simply add a Google user to an event and select checkbox to not notify them
- Google will automatically add it to their calendar
- This presents a unique phishing situation

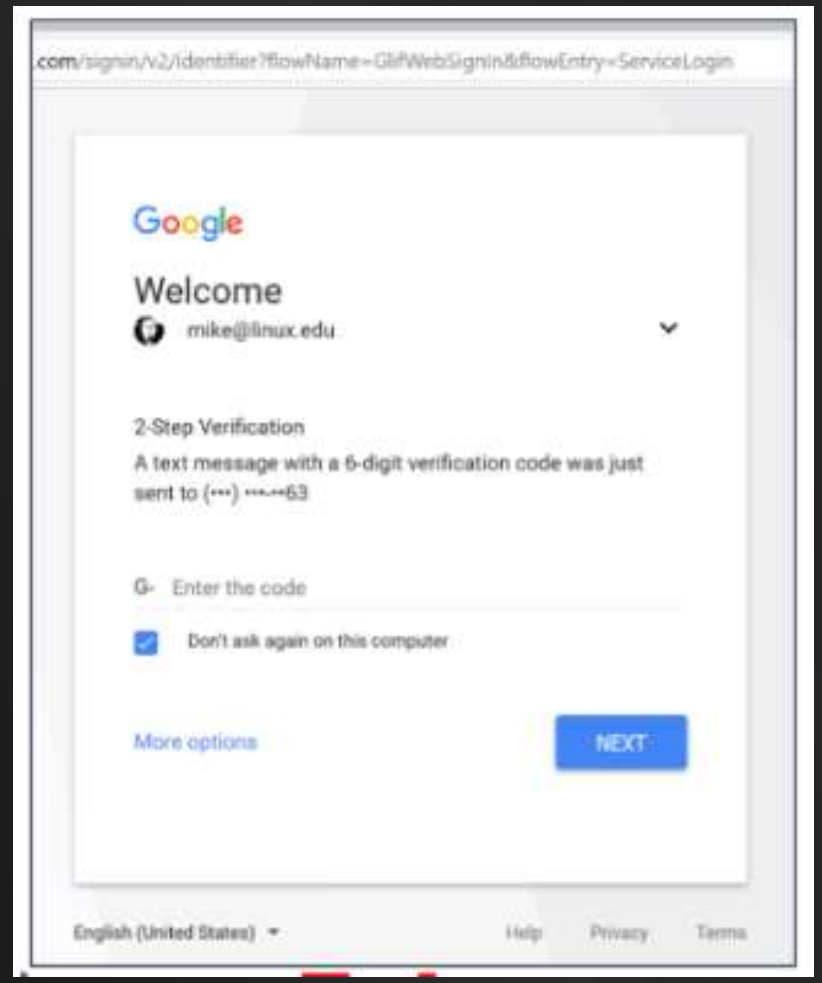
Google Calendar Event Injection

- A few ideas:
  - Include a link to a conference call site but have it pointing to a credential collection page (CredSniper!)
  - Include a malicious “agenda”
  - Have victims navigate to a fake Google Auth page and collect creds
- Gets more fun with Google API
  - **It’s possible to make it look like they already accepted the invite!**
  - **This completely bypasses the setting in G-calendar for not auto-adding events.**

Phishing 2FA Creds

Phishing 2FA Creds

- CredSniper by Mike Felch (@ustayready)
  - https://github.com/ustayready/CredSniper
- Framework para obtener credenciales
- Puede clonar un sitio web
- Intercepta tokens de 2FA
- Redirige a la victima a la web real y permite al atacante obtener acceso



Malicious Outlook Add-Ins

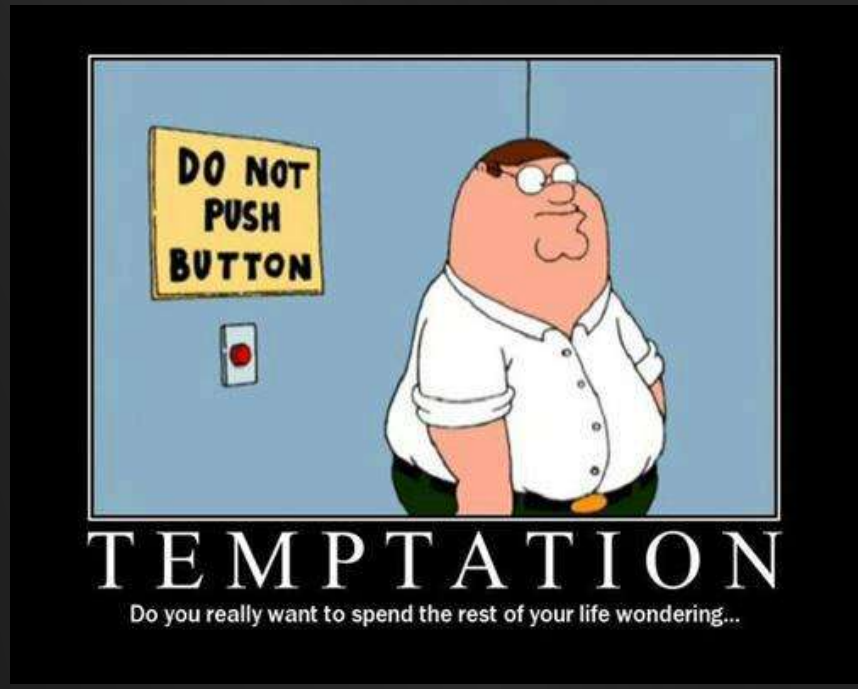
Outlook Web Add-Ins

- Microsoft permite add-ins para varios productos
- Outlook tiene “Web Addins” como tambien desktop add-ins
- **LOS WEB ADD-INS SON SYNCRONIZADOS A LOS CLIENTES DE BROWSER & ESCRITORIO**
- El ataque:
  - Consigue credentiales
  - Anhade un Add-in malcioso al Outlook web client
  - El add-in es replicado a las sesiones web y el cliente de escritorio Outlook

Outlook Add-in Potential

Que puede hacer un add-in ?

- Bueno… puede literalmente forzar al browser a visitar a un site malicioso.
- Cada vez que el add-in es ejecutado, usa el archivo “Manifest”
- Podemos hostear cualquier html/js
- Nota: El Outlook desktop client usa el browser Edge



Outlook Add-In Browser Hook

Podemos “infectar” el browser de la victima usando BeEF!

- Browser Exploitation Framework (BeEF)
- Inyectar hook.js al add-in
- Se puede utilizar plugins de BeEF
- Enumerate system/browser/LAN
- Inyectar otros frames
- Puedes lanzar un formulario para robar credenciales, descargar un, etc...
- Es necesario mas research en el potential para moviento lateral interno.

DEMO:
Outlook Add-In PoC

Onsite Attacks

Dropbox

- Un dispositivo de pentesting completamente funcional que puede ser dejado en las premisas del objectivo
- Utiliza tuneles SSH reversos persistentes
- Puedes ser controlado por Wifi
- Relativamente indistinguible
- ODROID-C2 instruciones aqui:
  - https://www.blackhillsinfosec.com/how-to-build-your-own-penetration-testing-drop-box/

NAC Bypass

- Impersonar a otro dispositivo
  - Encuentra una impresora o un telefono VOIP; Anota y replica la MAC and/or IP
  - Voiphopper to para saltar de VLAN's
  - Para NAC en Wi-Fi impersona la MAC y el User Agent de un dispositivo conectado
- Dispositivo Nat de Capa 2 y Capa 3
  - Helps avoid triggering port security rules on 802.1X
  - Device spoofs both sides of wire
  - Passively learns MAC addresses
- Check out SilentBridge - https://github.com/s0lst1c3/silentbridge

PXE Booting Attacks

- Obtain the “Golden” image from the network
- Set VM to “Boot from network”, boot VM, and get the image
- Mount image & profit
  - Steal Admin hashes
  - Set local admin pass pre-boot
  - Overwrite Sticky keys (sethc.exe)

Persistence

Backdoors for Persistence

- Microsoft O365/Azure:
  - Un Add-In de Outlook que reenvie todos los correos a un atacante
  - Una cuenta backdoor en Azure
    - Todos los usuarios del dominio O365 pueden ver informacion sobre otros usuarios incluyendo usuarios, correo, telefono, etc.
- Google G-Suite:
  - Application Password
  - Backup Codes
  - Email forward rule

Command and Control

Expired Categorized Domains

Expired Categorized Domains

- Tecnica usada para saltarse la categorizacion utilizado por los proxies web
- Utilizar sites que hayan sido previamente categorizados
- Trivial para encontrar
  - expireddomains.net
  - Domainhunter.py
- Simula utilizar un sitio web comprometido

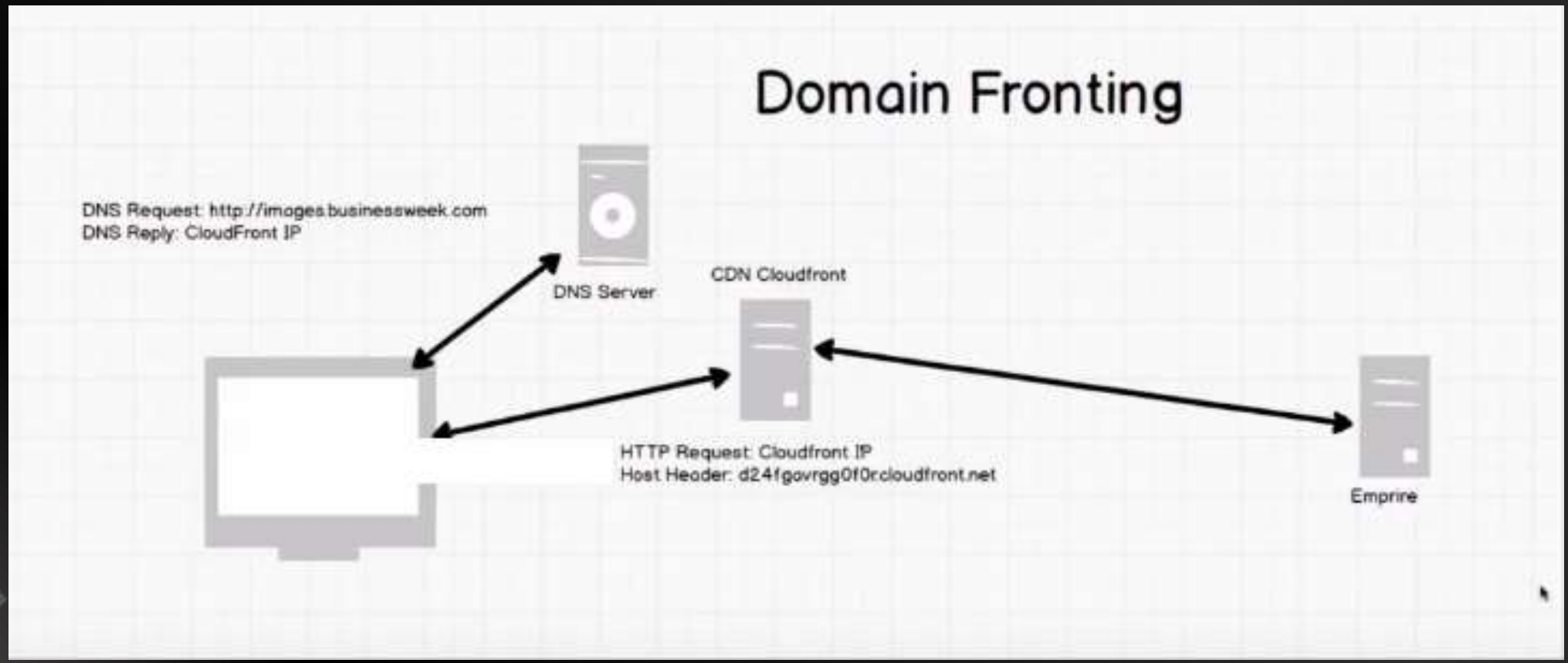
Domain Fronting

Domain Fronting

- Otra tecnica utilizada para saltar restriciones del web proxy
- Esconde el verdadero destino de una coneccion TTP

- Initial target domain for the traffic redirects to secondary host
- Can use a Content Delivery Network such as AWS Cloudfront
- Can be difficult to detect and block
- Wait your C2 channel is going to “opensource.carbonblack.com”?

Domain Fronting



Asset Discovery

PowerUp SQL

- Herramienta en PowerShell par atacar MSSQL
  - https://github.com/NetSPI/PowerUpSQL
- SQL Server discovery
- Detecta configuraciones debiles
- Escalamiento de privilegios
- Data sample searches
- OS command injection

Privilege Escalation

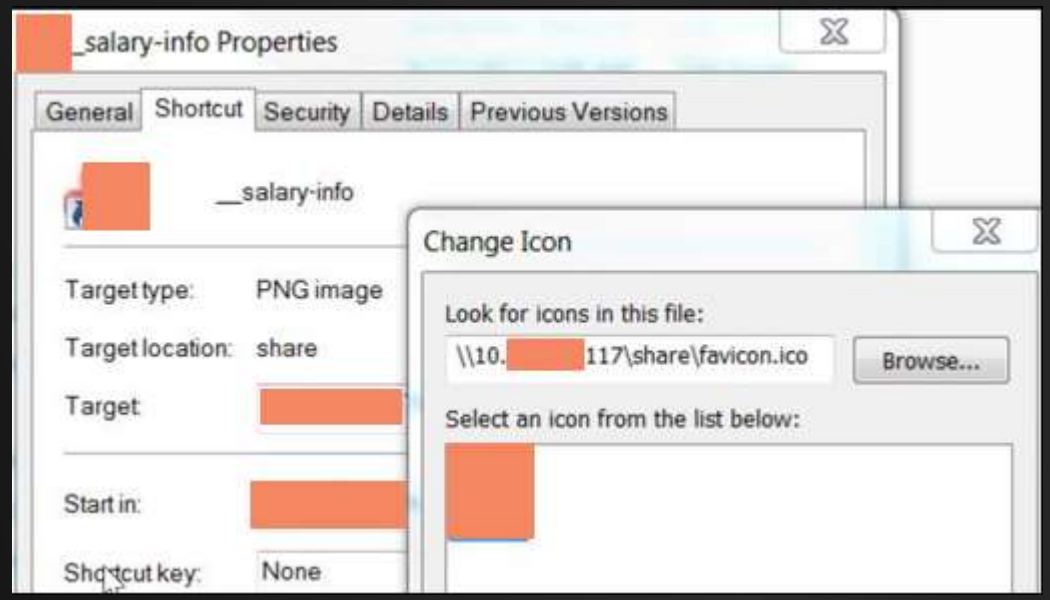
Kerberoasting

- Permite a un usuario preguntar al dominio por un Service Principal Name (SPN) de una cuenta asociada a un servicio
- Un peticion de autenticacion por Kerberos resulta en un Service Ticket que en parte es encriptado utilizando el password hash de la Service Account.
- Lo que esto significa es que un usuario del dominio puede obtener el hash de una cuenta e intentar crackearla para elevar privilegios.

Weaponized LNK File

- Deja un archivo shortcut (LNK) en un directorio compartido
- El icono apunta a una locacion UNC controlada por el atacante

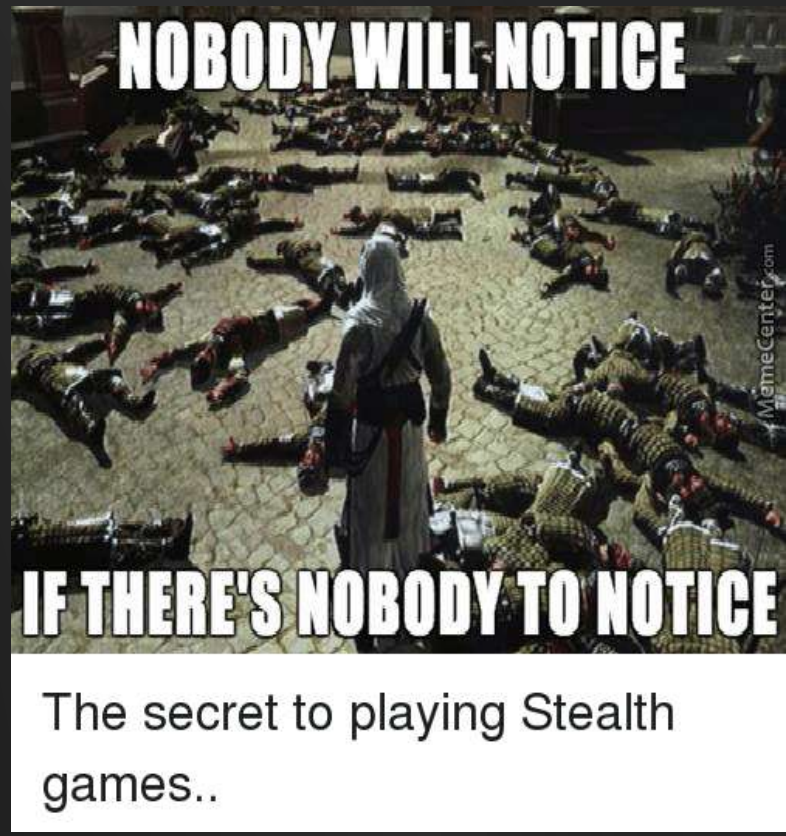
- El atacante levante un servicio SMB
- Se puede usar Inveigh
  - https://github.com/Kevin-Robertson/Inveigh
- Obteher hashes NetNTLMv2



Evading Failed Login Detection

Evading Failed Login Detection

- Standard password spraying alerted on?
- Looked to evade and tried RDP spraying
- Tested out xFreeRDP from Linux against a Windows Server RDP
- To our surprise the failed login event did not contain the source IP address…
- Hostname was in the log… but xFreeRDP has an option to set the client hostname (wat?)
- Set out to write a spraying tool for RDP



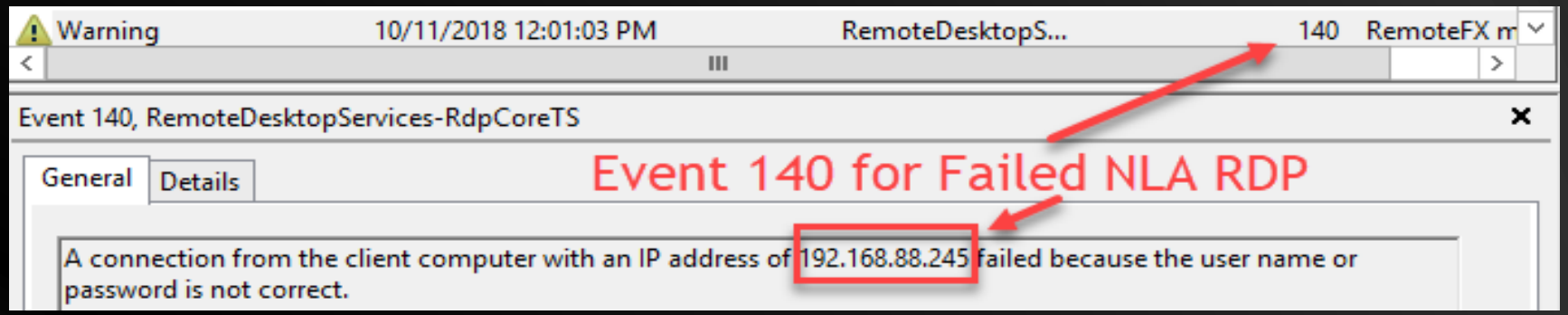
NLA FTW

- Why was there no IP in the log?
- It turns out RDP w/ NLA (Network Layer Authentication) doesn't log source IP in the security log
- NLA pre-authenticates prior to RDP access
- Causes Logon type 3 (Network) instead of 10 (RemoteInteractive)
- Allegedly there is supposed to be a log with the IP located here: Applications and Services Logs > Microsoft > Windows > RemoteDesktopServices-RdpCoreTS > Operational (Event ID 140)

What log?

Remember this is an "Applications and Services Log"... not "Security"

- This is what a failed RDP using NLA should look like:



- ...But authenticating via NLA doesn't <ALWAYS> generate this log... Because this alert is very, VERY misleading.
- It turns out this alert only fires when the **USER is invalid.**
- **Valid user + invalid password = No eventID 140 log**

DEMO:
RDPSpray PoC

Lateral Movement

Living off the Land

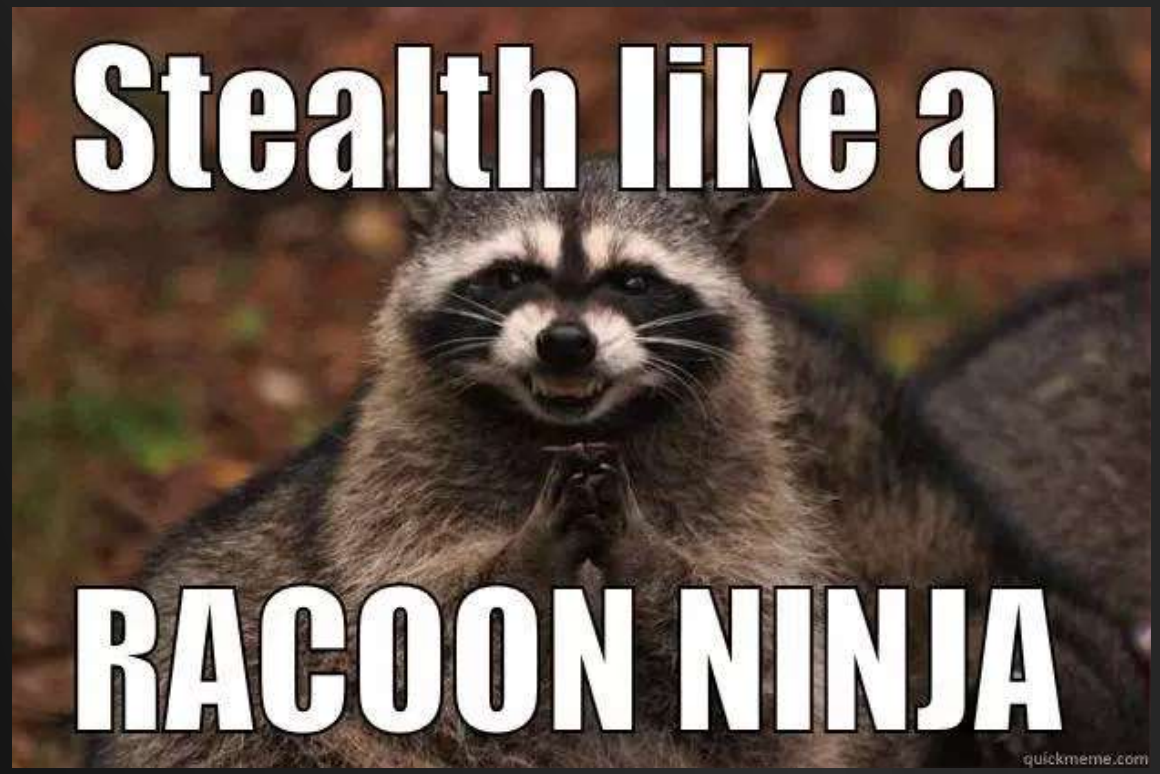
- Utilizar herramientas nativas para evitar descargar malware
- Reconocimiento de usuarios/grupos
- Listar directorios remotos, copiar.
- Ejectuar procesos remotamente
- Ataques de password
- Descubrimiento de red
- Windows tiene mucho para usar ofensivamente:
  - PowerShell, C#, WMI, etc…

Living off the Land

- Comandos net
  - net groups “DOMAIN ADMINS” /DOMAIN
  - net accounts /domain
  - net localgroup administrators hax /add
- Listar directorios remotoes
  - dir \\host\C$\files
  - get-WmiObject -class Win32_Share -computer
- Ejecutar comandos remotamente
  - Invoke-Command -ComputerName -ScriptBlock {Command Here}
  - wmic /node:”computer-name” process call create “cmd.exe /c C:\evil.bat”
- Crear tarejas programads
  - SCHTASKS /s remote_machine /U username /P password /create /tn “not evil" /tr "C:\evil.bat" /sc ONCE /sd 01/01/1910 /st 00:00
- WMI
  - WMI OPS from Chris Truncer - https://github.com/FortyNorthSecurity/WMIOps
- Encontrar passwords en GPP
  - findstr /S cpassword %logonserver%\sysvol*.xml
- CMD.exe Password Spray
  - @FOR /F %n in (users.txt) DO @FOR /F %p in (pass.txt) DO @net use \\DOMAINCONTROLLER\IPC$ /user:DOMAIN\%n %p 1>NUL 2>&1 && @echo [*] %n:%p && @net use /delete \\DOMAINCONTROLLER\IPC$ > NUL

Stealthy Host/Domain Enumeration

- Cada vez hay mas y mas antivirus, analisis de compartamiento, app whitelisting, etc. los productos ahora bloquean on alertan cuando se usando comandos nativos
- Ejem:net, ipconfig, whoami, netstat, etc.
- Puedes usar PowerShell en vez de las tools nativas
  - https://github.com/dafthack/HostRecon
- Utiliza tambien tecnicas para usar Powershell sin llamar a powershell.exe



BloodHound

- Enumera y obteiener:
  - Los administratores en todos los sistemas
  - Sesiones de usuario
  - Information de gruops
  - Informacion de confianza entre dominios
- Encuentra un camino a Domain Admin
- Author(s):
  - Andrew Robbins (@_wald0), Will Schroeder (@harmj0y), and Rohan Vazarkar (@CptJesus)
  - https://github.com/BloodHoundAD/BloodHound

Actions and Objectives

Finding Sensitive Data

- PowerView ShareFinder/FileFinder
  - Find shares on network then search them for files with certain terms in title: ‘*pass*’, ‘*sensitive*’, ‘*admin*’, ‘*secret*’, ‘*login*’, ‘*unattend*.xml’, ‘*.vmdk’, ‘*creds*’, or ‘*credential*’
- Locate RDP Jump Hosts
  - Get-NetComputers | Get-NetRDPSessions | Export-Csv –NoTypeInformation rdpsessions.csv
- Admin on Virtualization Hypervisors

Detection and Prevention

Solid Systems Administration

- Systems and software inventory (yes, CSC Top 20 are useful)
- Workstations should never talk to workstations - client to server communication only
  - Windows firewall or Private VLANS
- Baseline images with GPO enforcement
- All inbound and outbound network traffic go through an application proxy system
  - Any exceptions for direct outbound communication are by documented exception only

Enforce Good User Behavior

- Change every inbound email subject line with a tag such as (External):
- Inform your users that any email with that tag needs extra scrutiny
- Minimum of 15 characters for any domain account password
  - If you have to compromise to sell it to the business, no complexity requirements and 6 month change interval
- Consider additional credential defenses
  - Commercial offerings available
  - CredDefense Toolkit for Free
    - https://github.com/creddefense

Host Log Consolidation

- Consolida los logs mas importantes de las laptops/desktops, servidores a una locacion central
- Monitorea Powershell y ejecusion de procesos
- Sysmon es una poderosa y gratis options para monitorear actividad de los hosts
- Una vez con el monitoreo, configura alertas en “comandos anormales” como commandos net
- No tiene que ser caro:
  - https://www.blackhillsinfosec.com/end-point-log-consolidation-windows-event-forwarder/

Network Logging

- NetFlow, Bro, or Full Packet Capture?
  - Depende del presupuesto y capacidades
- Bro es un buen balance entre NetFlow 5-Tuple y los requerimientos de storage de Full Packet Capture.
- Captura los protocles mas comunes a archivos de texto
- Provee visibilidad a trafico SSL sin tener que romper SSL
  - Informacion anomala de un certificado
  - SSL fingerprinting - JA3 project - https://github.com/salesforce/ja3
- Detectar un backdoor con RITA (AIHunt)
  - https://www.blackhillsinfosec.com/projects/rita/

Red Team Prepper

- Don’t wait on the Red Team prepare on your own
- Use @vysecurity’s Red Team Tips to find techniques to try to detect
  - https://github.com/vysec/RedTips
- MITRE ATT&CK Framework for threat actor techniques
  - https://attack.mitre.org/wiki/Main_Page
- Red Canary’s Atomic Red Team - portable scripts to test ATT&CK framework
  - https://github.com/redcanaryco/atomic-red-team

Summary and Conclusions

- Black Hills Information Security
  - http://www.blackhillsinfosec.com
  - @BHInfoSecurity
- Beau Bullock @dafthack

- Questions?