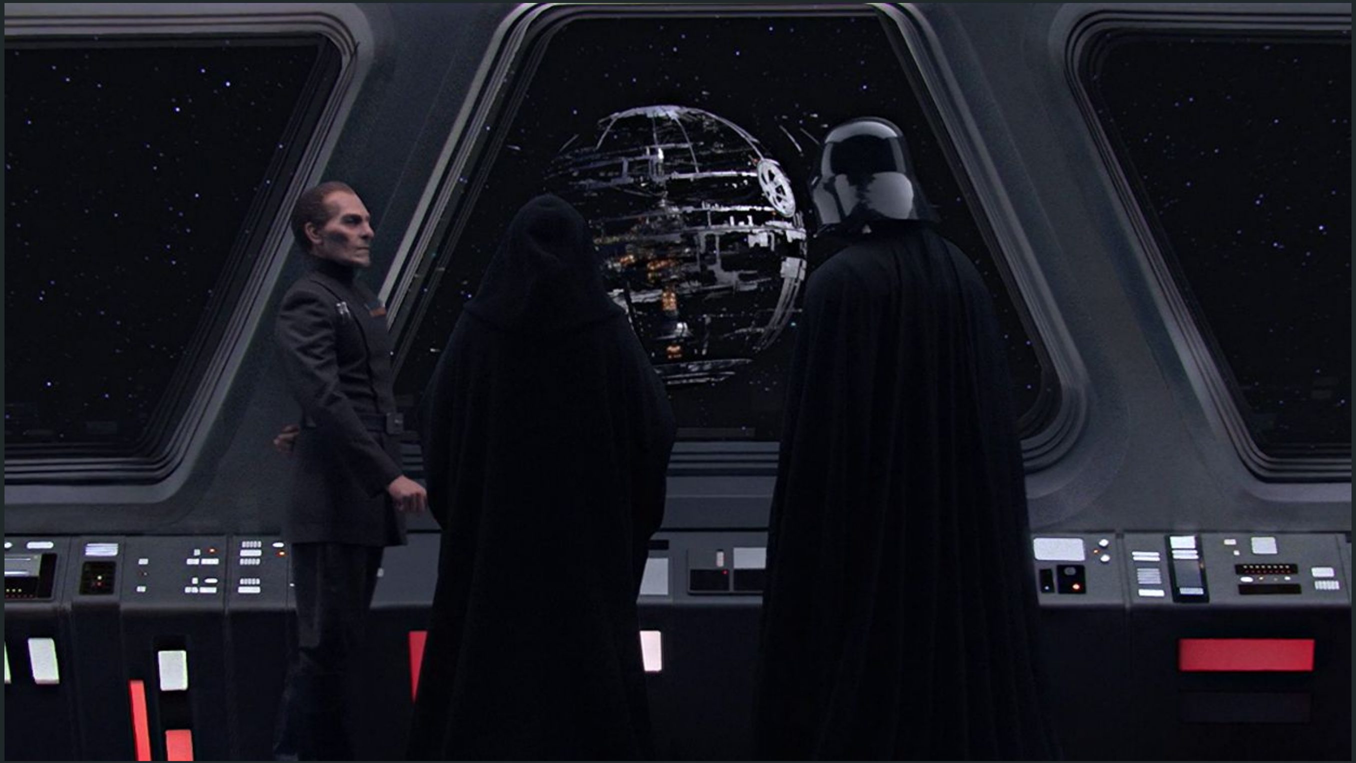
Building the DeathStar



Getting Domain Admin with a push of a button

whoami

COALFIRE℠

LABS

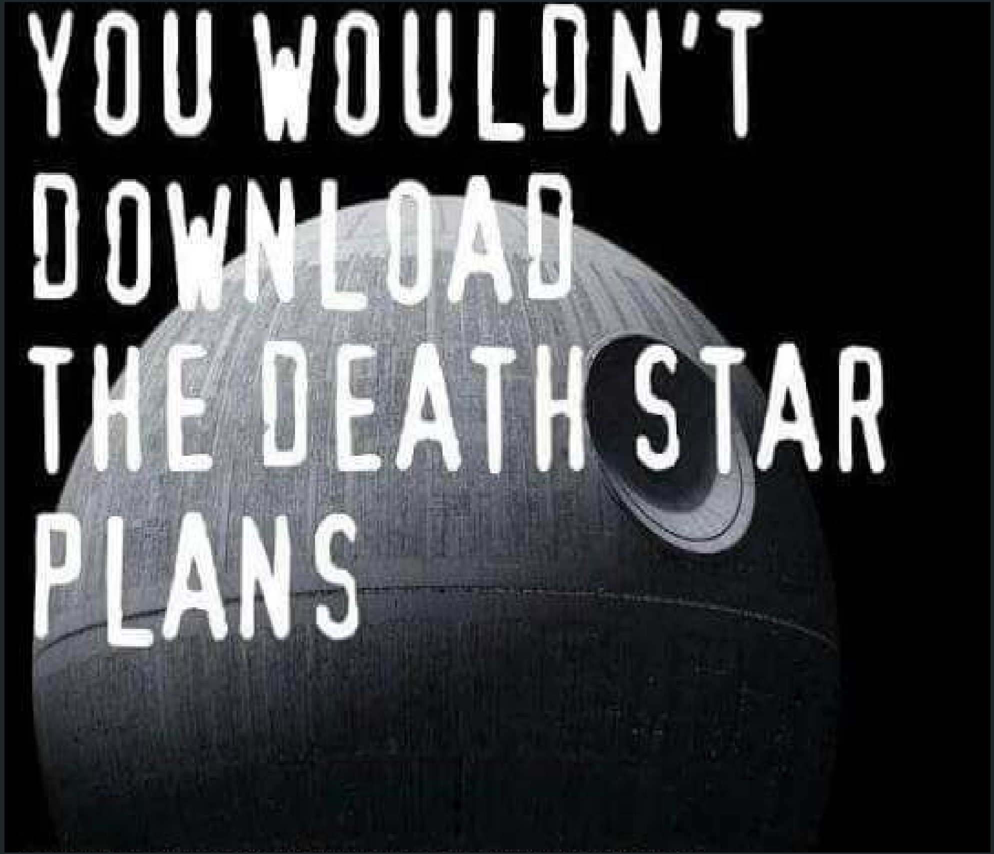
@byt3bl33d3r

https://github.com/byt3bl33d3r

https://byt3bl33d3r.github.io

Mini rant time …

Domain Admin != End of Pentest


YOU WOULDN'T
DOWNLOAD
THE DEATH STAR
PLANS

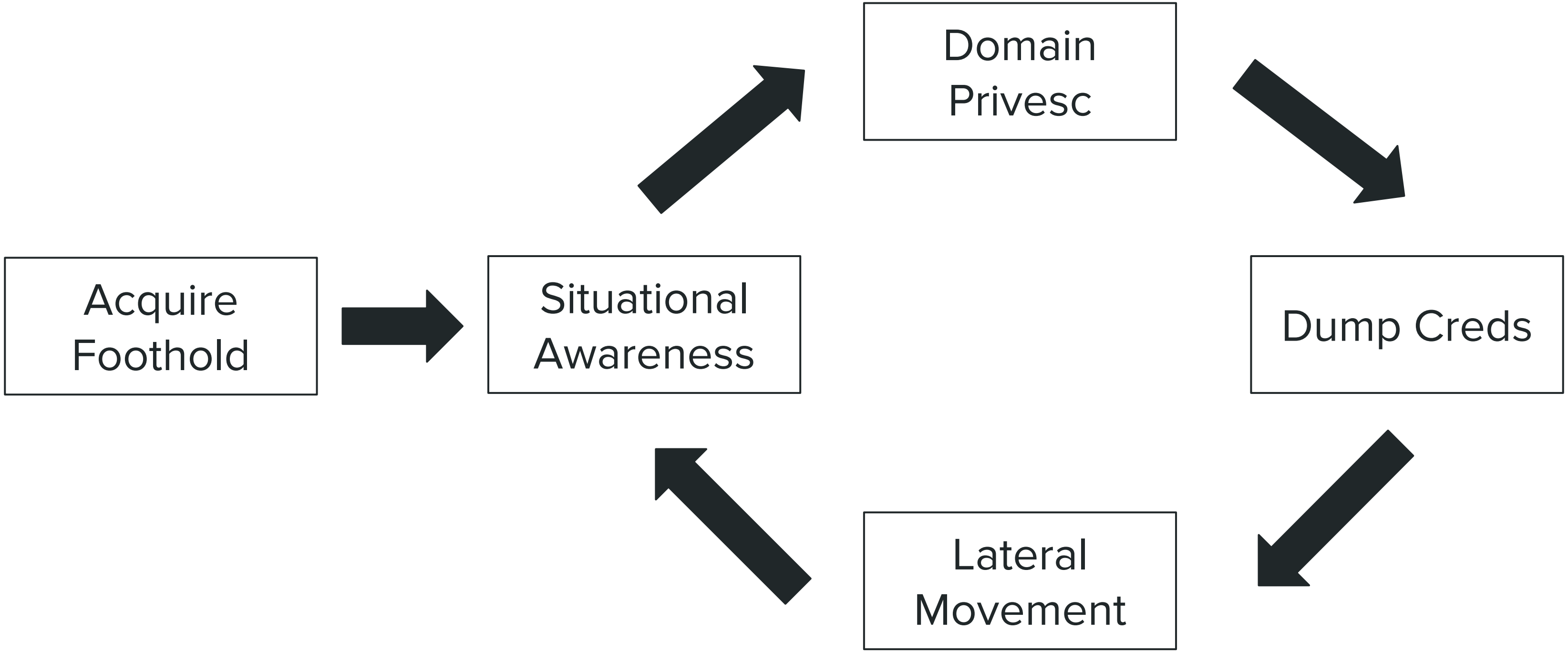
+

- Open-Source
- Written in Python 3
- Uses Empire’s RESTful API
- Takes you from Domain User to Domain Admin in 90% of all AD environments

Why do we even need this?

Let’s break down our daily Active Directory pentest routine…

Let’s step through each phase...



Acquire Foothold

Situational Awareness

Domain Privesc

Dump Creds

Lateral Movement

Getting a Foothold

(The only thing DeathStar won’t do for you)

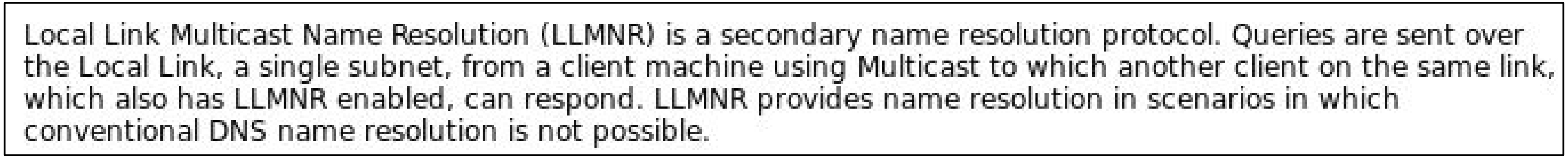
Externally:

- Ruler: https://github.com/sensepost/ruler
- LyncSniper: https://github.com/mdsecresearch/LyncSniper

Internally:

- Responder: https://github.com/lgandx/Responder
- Impacket: https://github.com/CoreSecurity/impacket
- CrackMapExec: https://github.com/byt3bl33d3r/CrackMapExec

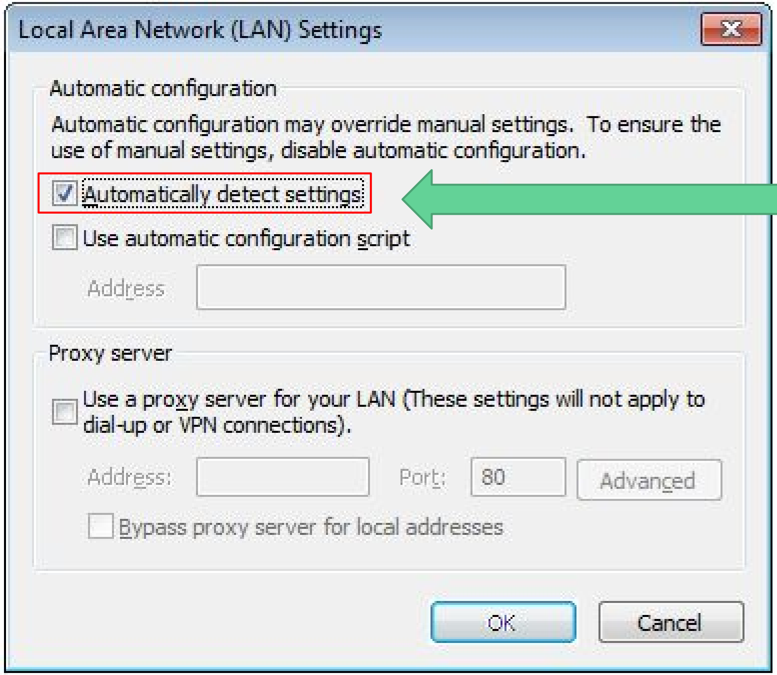
Multicast/Broadcast Name Resolution Poisoning



Local Link Multicast Name Resolution (LLMNR) is a secondary name resolution protocol. Queries are sent over the Local Link, a single subnet, from a client machine using Multicast to which another client on the same link, which also has LLMNR enabled, can respond. LLMNR provides name resolution in scenarios in which conventional DNS name resolution is not possible.

LLMNR, NBNS and WPAD are the major ones. There are others but I've personally never seen them used in a live environment yet.

http://www.computerstepbystep.com/turn-off-multicast-name-resolution.html



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

Mitigation

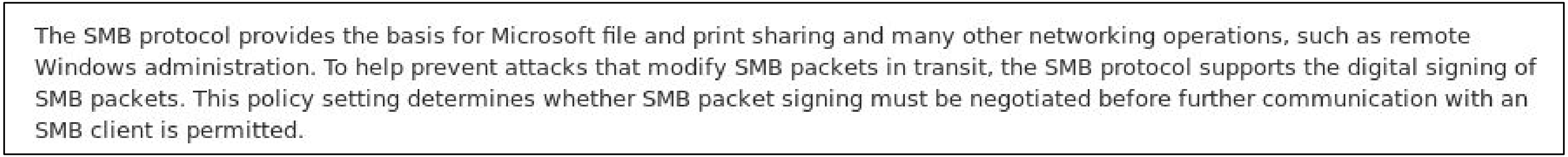
- Create a WPAD entry that points to the corporate proxy server, or disable proxy autodetection in Internet Explorer.
- Disable NBNS and LLMNR (test in a lab before deploying to all systems!).
- Set valid DNS entries for all internal and external resources.
- Monitor the network for broadcast poisoning attacks.

Difficulty: MODERATE

Breaks Stuff: MAYBE

SMB Signing

In my opinion, the most overlooked/underrated domain security setting.



The SMB protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To help prevent attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This policy setting determines whether SMB packet signing must be negotiated before further communication with an SMB client is permitted.

Enable this <u>EVERYWHERE</u>!

https://technet.microsoft.com/en-us/library/cc731957(v=ws.11).aspx

Mitigation

- Following key needs to be set EVERYWHERE:
    - HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature

- Test in lab before deploying to all systems!

Difficulty: EASY PEASY LEMON SQUEEZY

Breaks Stuff: MAYBE

NTLM Relaying FTW!

Responder + ntlmrelayx.py + Empire

Foothold in under 5 minutes!

Covered this in a blog post here:
https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html

Situational Awareness

Powerview

- https://github.com/PowerShellMafia/PowerSploit

Where my Admins at?

- Get-NetGroupMember
- Get-NetLocalGroup
- Invoke-UserHunter

Where my Domain Controllers at?
(so I know which boxes to stay away from)

- Get Net-DomainController

Mitigation

- Most of this functionality is considered a feature not a bug and is still there mainly for backwards compatibility reasons (a.k.a. Microsoft's Curse)

- There are some TechNet PS scripts which allow you to harden session enumeration and SAMR remote access (shoutout to @ItaiGrady <3):
  - https://gallery.technet.microsoft.com/SAMRi10-Hardening-Remote-48d94b5b
  - https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b

- If anyone has any pro-tips on how to mitigate AD information gathering on the cheap would love to hear it :)

Difficulty: HARD
Breaks Stuff: MAYBE

Domain Privesc

Passwords in SYSVOL & Group Policy Preferences

Here’s the TL;DR:

- When a new GPP is created, there’s an associated XML file created in the SYSVOL share with the relevant configuration data and if there is a password provided, it is AES-256 bit encrypted.

- At some point prior to 2012, Microsoft published the AES encryption key (shared secret) on MSDN which can be used to decrypt the password. Since authenticated users (any domain user or users in a trusted domain) have read access to SYSVOL, anyone in the domain can search the SYSVOL share for XML files containing “cpassword” which is the value that contains the AES encrypted password.

https://adsecurity.org/?p=2362

Mitigation

- Install KB2962486 on every computer used to manage GPOs which prevents new credentials from being placed in Group Policy Preferences.
  https://support.microsoft.com/en-us/kb/2962486

- Delete existing GPP xml files in SYSVOL containing passwords.

- Don't put passwords in files that are accessible by all authenticated users.

Difficulty: EASY\MODERATE

Breaks Stuff: NO

https://adsecurity.org/?p=2362

Dumping Credentials

Cleartext Passwords in Memory

Here’s the TL;DR:

- Windows stores domain credentials in memory (specifically the LSASS process)

- There are a lot of free tools that can dump these credentials (Mimikatz is the most popular)

- Powersploit’s Invoke-Mimikatz script can inject Mimikatz directly in memory without touching disk, making it fairly hard to detect.

Mitigation

- This attack can’t be performed on Windows 2012R2+ and Windows 8.1+.
- On older systems KB2871997 should be installed EVERYWHERE
  https://support.microsoft.com/en-us/kb/2871997
- The following registry should be set EVERYWHERE and monitored:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
  SecurityProviders\WDigest\UseLogonCredential: Value 0 (REG_DWORD)
- Your Administrators should have a separate workstation for their administrative activities!

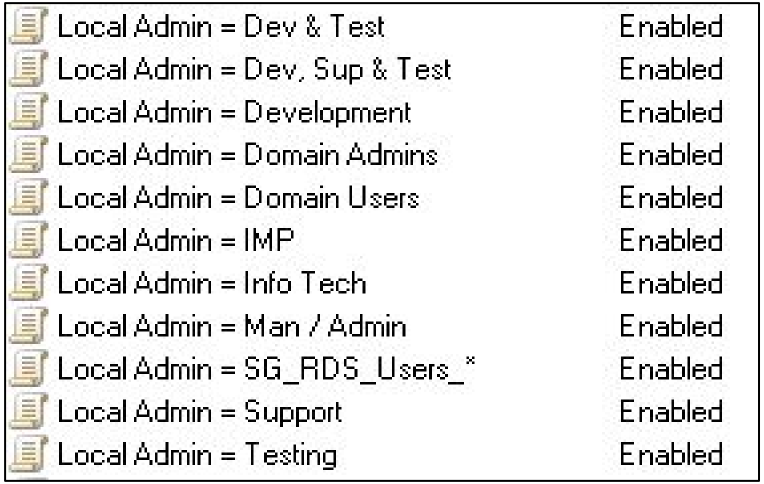
Difficulty: EASY

Breaks Stuff: NO/MAYBE

Lateral Movement

Local Administrator Accounts

Here’s a good example of what **not** to do:



Local Admin = Dev & Test	Enabled
Local Admin = Dev, Sup & Test	Enabled
Local Admin = Development	Enabled
Local Admin = Domain Admins	Enabled
Local Admin = Domain Users	Enabled
Local Admin = IMP	Enabled
Local Admin = Info Tech	Enabled
Local Admin = Man / Admin	Enabled
Local Admin = SG_RDS_Users_*	Enabled
Local Admin = Support	Enabled
Local Admin = Testing	Enabled

Mitigation

Microsoft LAPS:

- https://www.microsoft.com/en-us/download/details.aspx?id=46899
- https://adsecurity.org/?p=1790

Difficulty: MODERATE

Breaks Stuff: NO

Putting it all together

Empire is awesome

situational_awareness/network/powerview/get_group_member

situational_awareness/network/powerview/get_domain_controller

situational_awareness/network/powerview/user_hunter

situational_awareness/network/powerview/find_localadmin_access

situational_awareness/network/powerview/get_gpo_computer

situational_awareness/network/powerview/get_loggedon

Empire is awesome

privesc/gpp

privesc/bypassuac_eventvwr

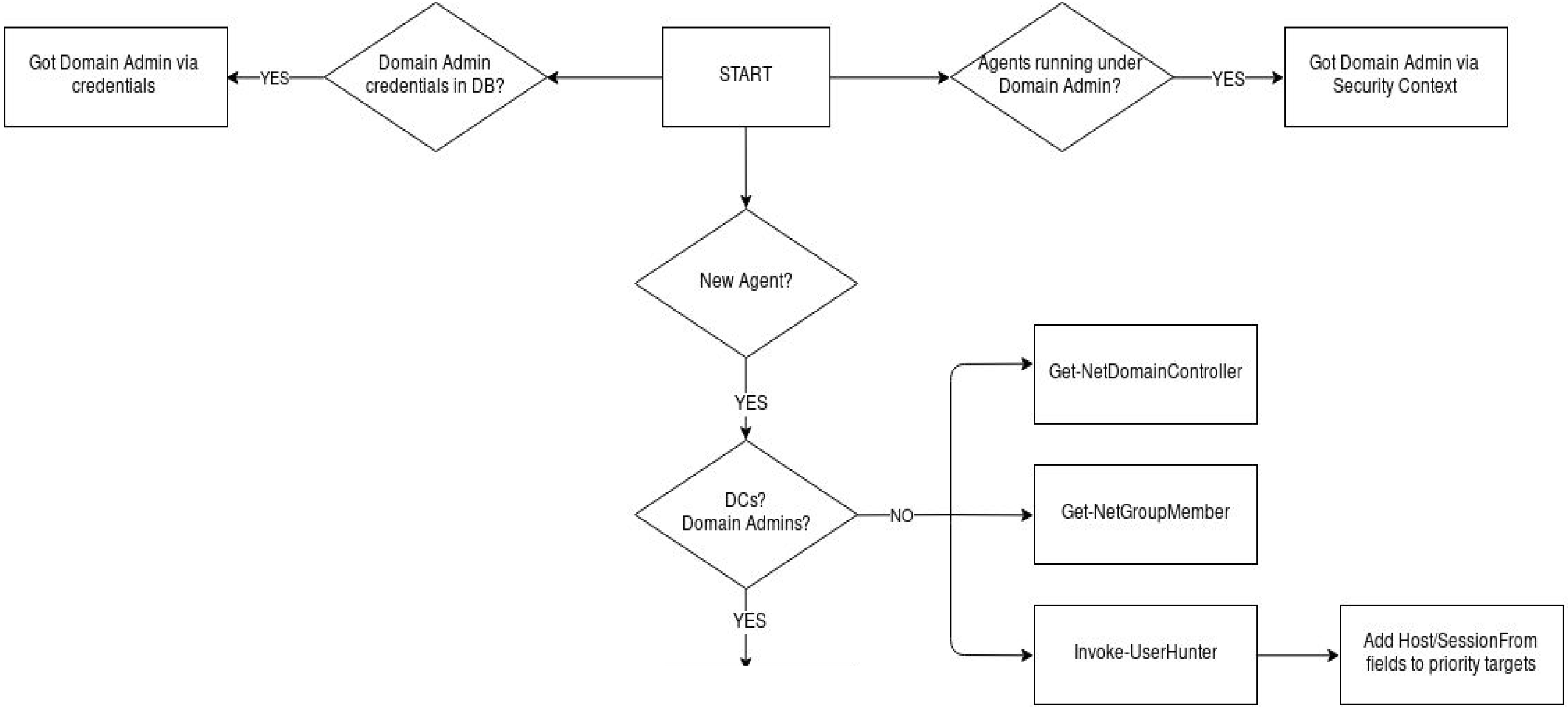
management/psinject

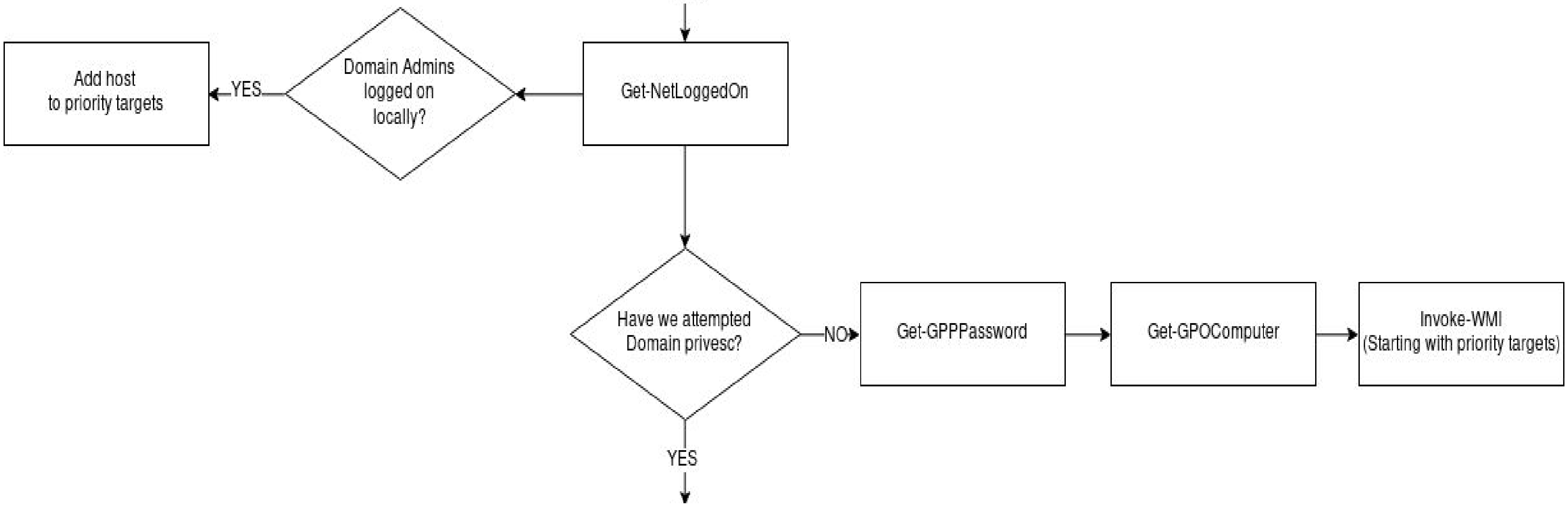
management/spawnas

management/get_domain_sid

lateral_movement/invoke_wmi

credentials/mimikatz/logonpasswords


Got Domain Admin via credentials
YES
Domain Admin credentials in DB?
START
Agents running under Domain Admin?
YES
Got Domain Admin via Security Context
New Agent?
YES
Get-NetDomainController
DCs?
Domain Admins?
NO
Get-NetGroupMember
YES
Invoke-UserHunter
Add Host/SessionFrom fields to priority targets



Get-NetLoggedOn

Domain Admins logged on locally?

YES

Add host to priority targets

Have we attempted Domain privesc?

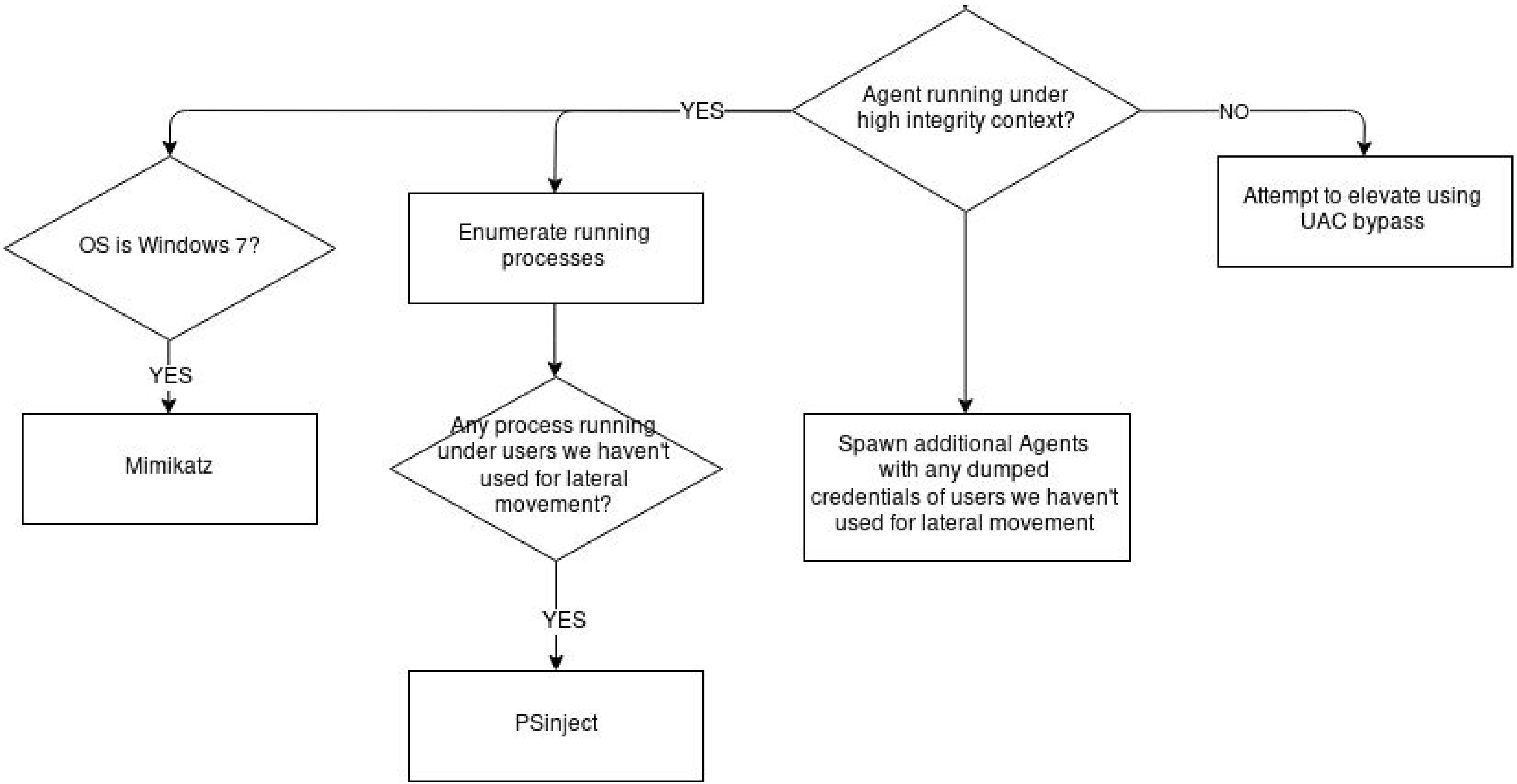
NO

Get-GPPPassword

Get-GPOComputer

Invoke-WMI (Starting with priority targets)

YES



Agent running under high integrity context?

YES

NO

Attempt to elevate using UAC bypass

OS is Windows 7?

YES

Mimikatz

Enumerate running processes

Any process running under users we haven't used for lateral movement?

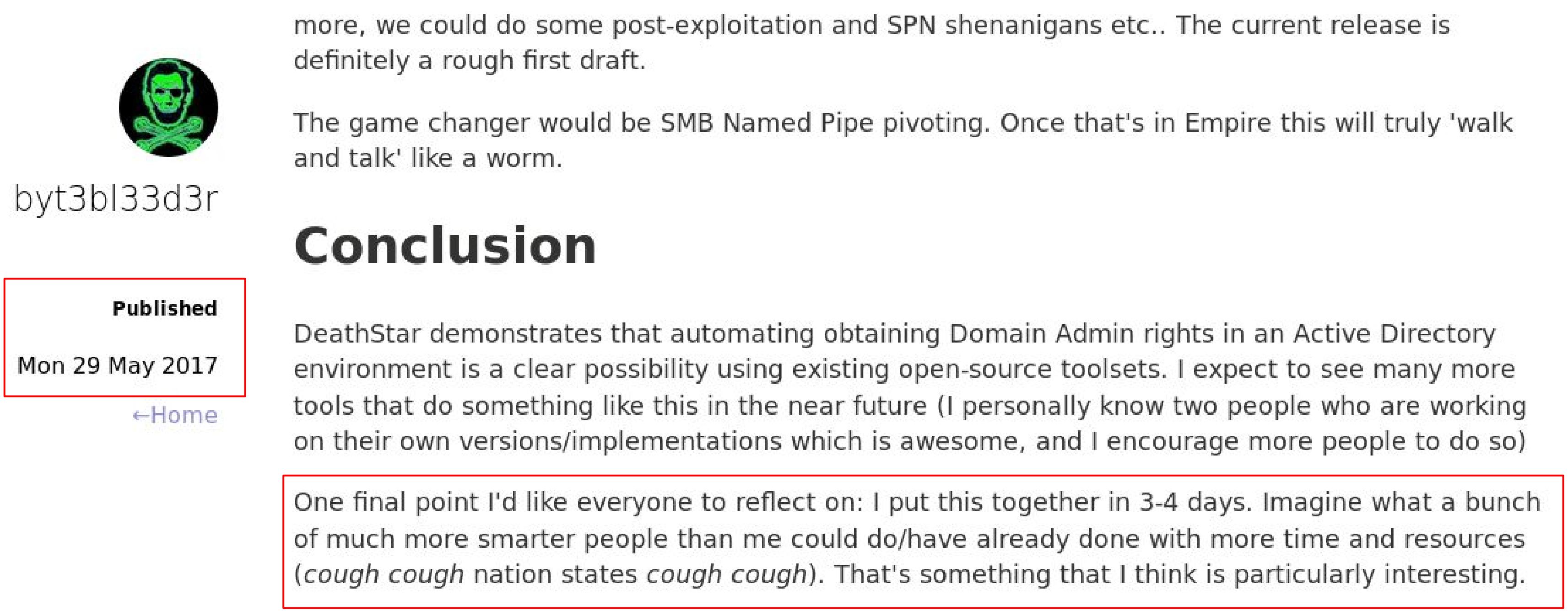
YES

PSinject

Spawn additional Agents with any dumped credentials of users we haven't used for lateral movement

Demo Time!

Wait a second… this sounds a little familiar…



byt3bl33d3r

Published

Mon 29 May 2017

←Home

more, we could do some post-exploitation and SPN shenanigans etc.. The current release is definitely a rough first draft.

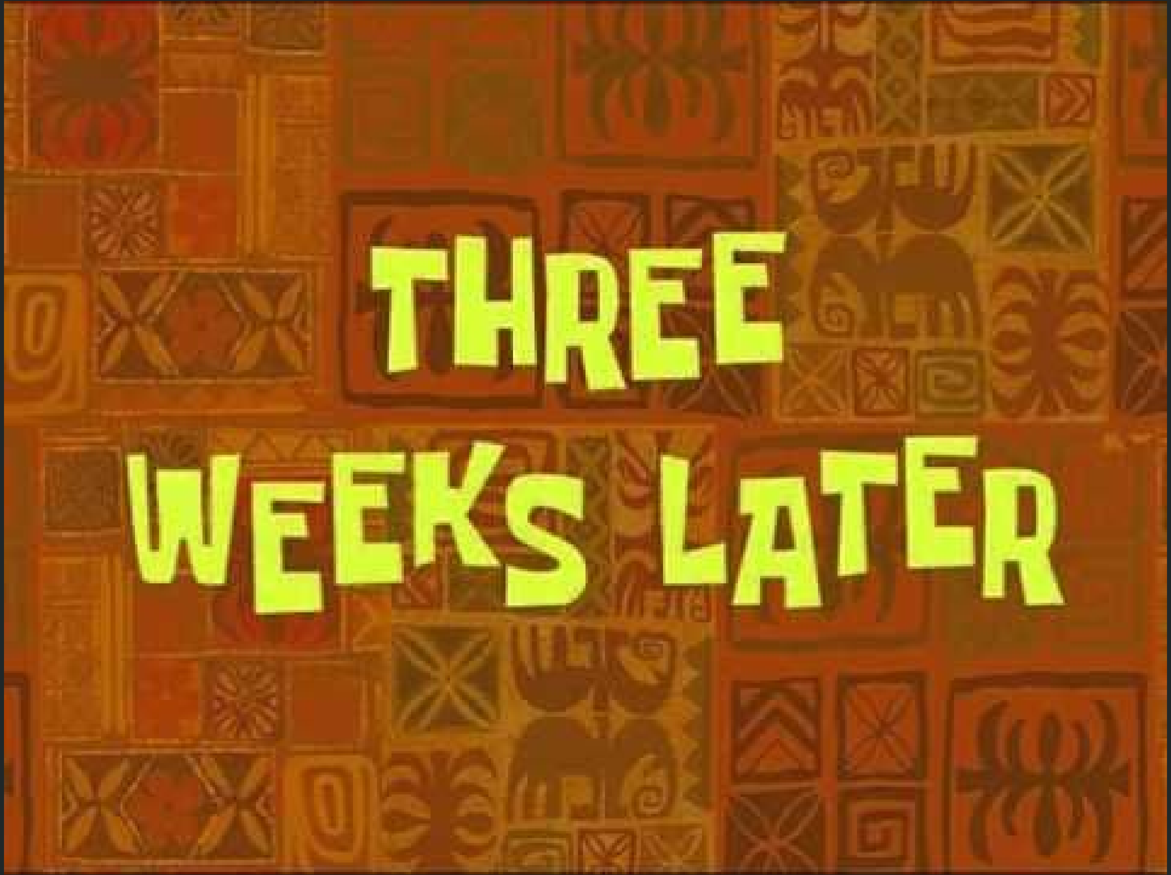
The game changer would be SMB Named Pipe pivoting. Once that's in Empire this will truly 'walk and talk' like a worm.

Conclusion

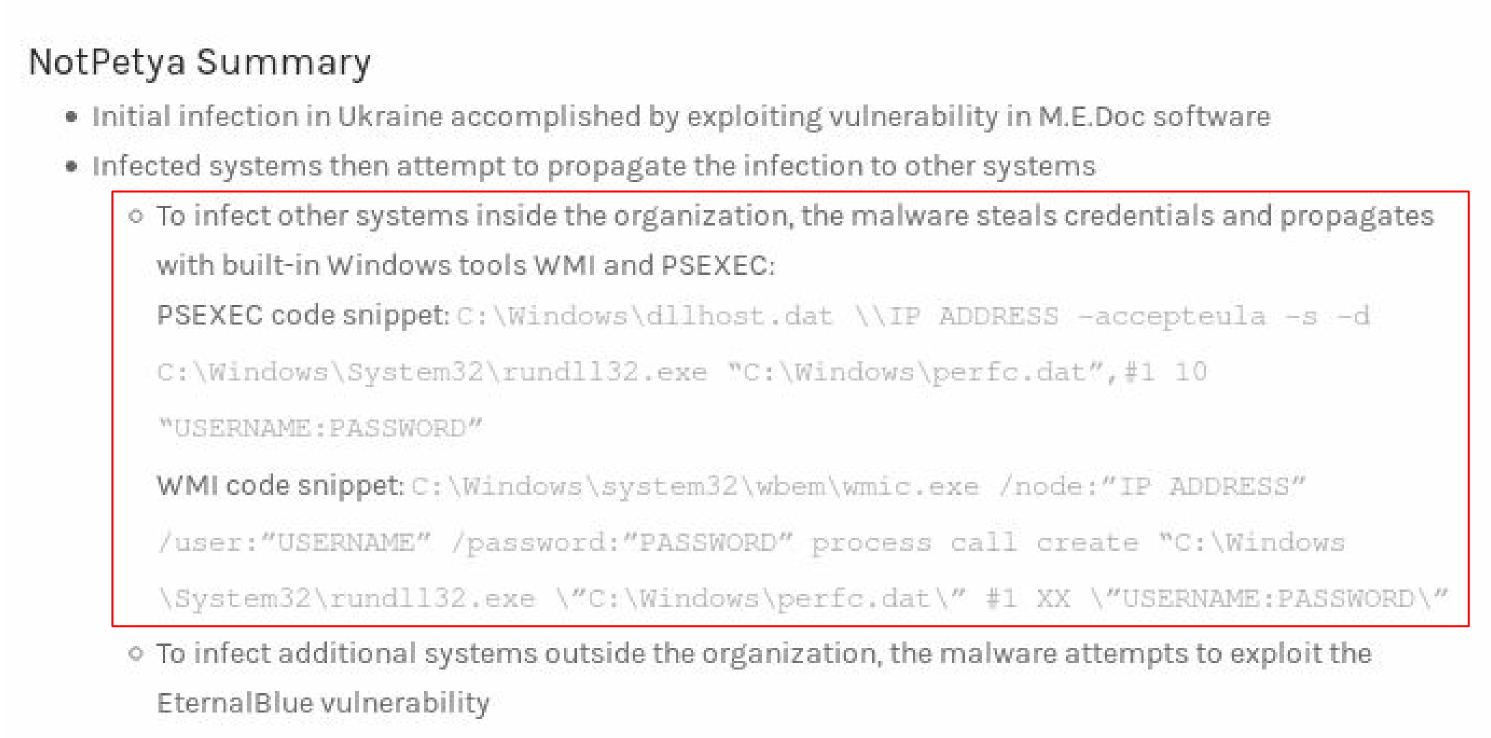
DeathStar demonstrates that automating obtaining Domain Admin rights in an Active Directory environment is a clear possibility using existing open-source toolsets. I expect to see many more tools that do something like this in the near future (I personally know two people who are working on their own versions/implementations which is awesome, and I encourage more people to do so)

One final point I'd like everyone to reflect on: I put this together in 3-4 days. Imagine what a bunch of much more smarter people than me could do/have already done with more time and resources (*cough cough* nation states *cough cough*). That's something that I think is particularly interesting.

https://byt3bl33d3r.github.io/automating-the-empire-with-the-death-star-getting-domain-admin-with-a-push-of-a-button.html


THREE
WEEKS LATER

Called it! Sorta.. Maybe.. Dunno...



NotPetya Summary

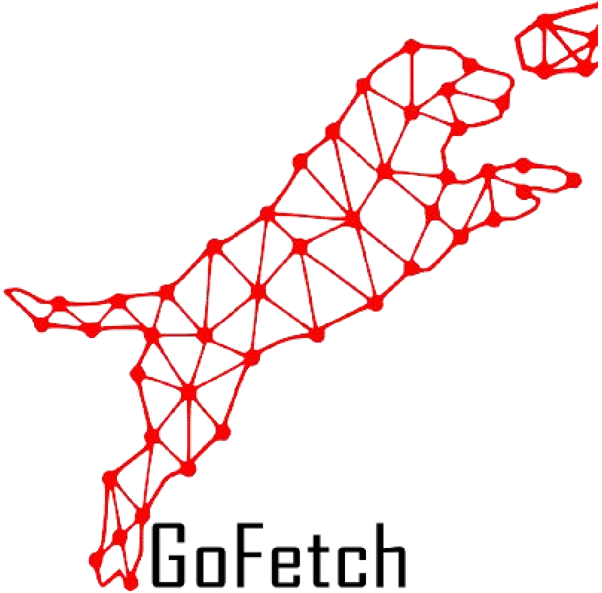
- Initial infection in Ukraine accomplished by exploiting vulnerability in M.E.Doc software
- Infected systems then attempt to propagate the infection to other systems
  - To infect other systems inside the organization, the malware steals credentials and propagates with built-in Windows tools WMI and PSEXEC:

    PSEXEC code snippet: `C:\Windows\dllhost.dat \\IP ADDRESS -accepteula -s -d C:\Windows\System32\rundll32.exe “C:\Windows\perfc.dat”,#1 10 “USERNAME:PASSWORD”`

    WMI code snippet: `C:\Windows\system32\wbem\wmic.exe /node:”IP ADDRESS” /user:”USERNAME” /password:”PASSWORD” process call create “C:\Windows \System32\rundll32.exe \”C:\Windows\perfc.dat\” #1 XX \”USERNAME:PASSWORD\”`
  - To infect additional systems outside the organization, the malware attempts to exploit the EternalBlue vulnerability

https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/

Same concept, different implementation



- https://github.com/GoFetchAD/GoFetch
- Developed by @talthemaor
- Uses BloodHound instead of Empire

People you should follow cause they are awesome

- @agsolino
- @gentilkiwi
- @subTee
- @PyroTek3
- @Carlos_Perez
- @talthemaor
- @xorrior
- @_wald0
- @harmj0y
- @mattifestation
- @enigma0x3
- @ItaiGradi
- @rvrsh3ll
- @CptJesus

Questions? Insults?

@byt3bl33d3r

https://github.com/byt3bl33d3r/DeathStar