Ruler

Pivoting Through Exchange

TROOPERS

sensepost

whoami

@_staaldraad, @sensepost, #TR17

TROOPERS

sensepost

Outline

Recon

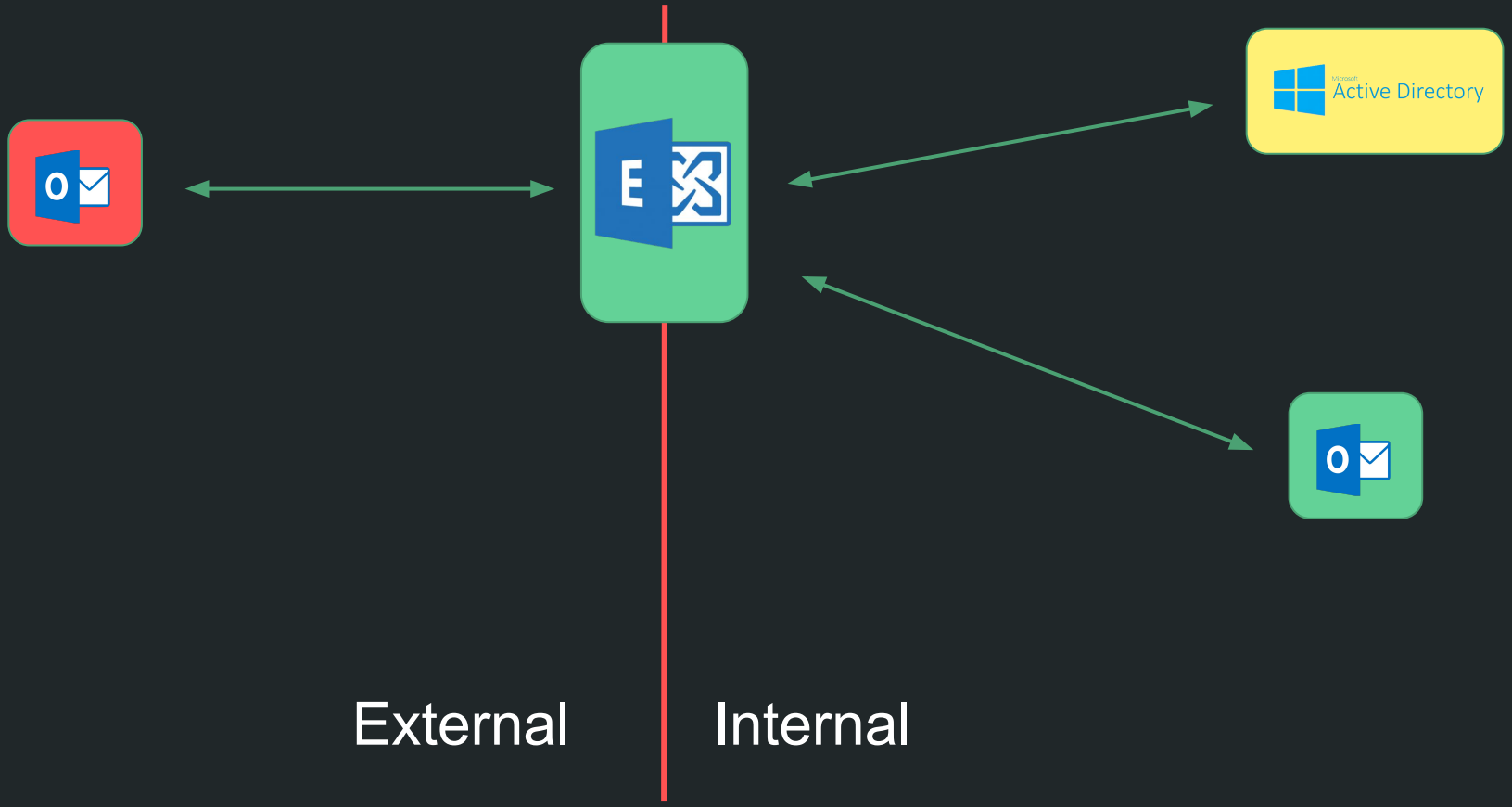
Exploit

Persist

Defend

Using Exchange to pop and persist shells

Exchange


Active Directory
External
Internal

Recon

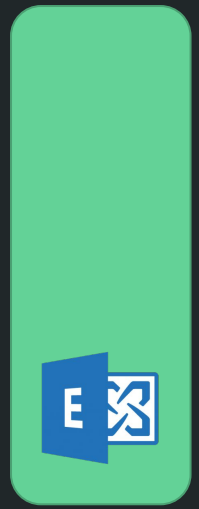
Autodiscover

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`

censys

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

TROOPERS

sensepost

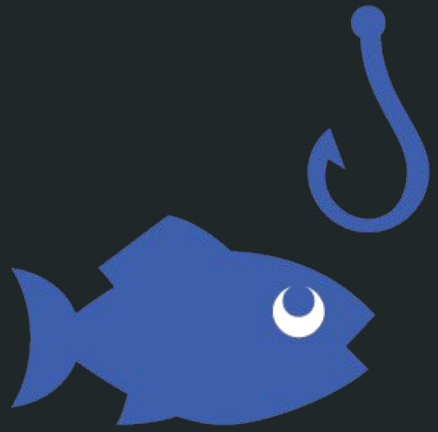
Gain Access

Brute-Force

WiFi

Phishing

Dumps



TROOPERS

sensepost

18,287 domains

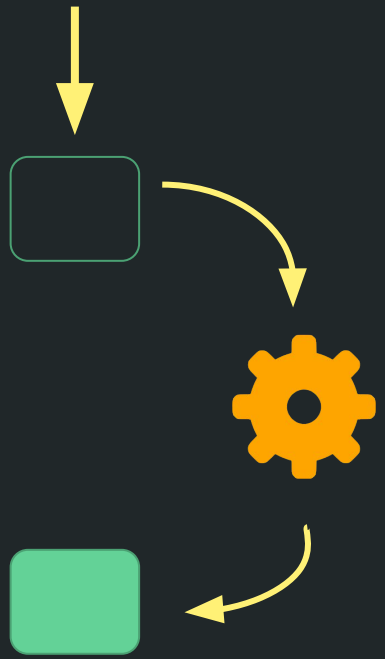
domain\username

email

password

Exploit

Automation



- [ ] print it
- [ ] play a sound
- [x] 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

TROOPERS

sensepost

Synchronisation

Client-Side
vs.
Server-Side

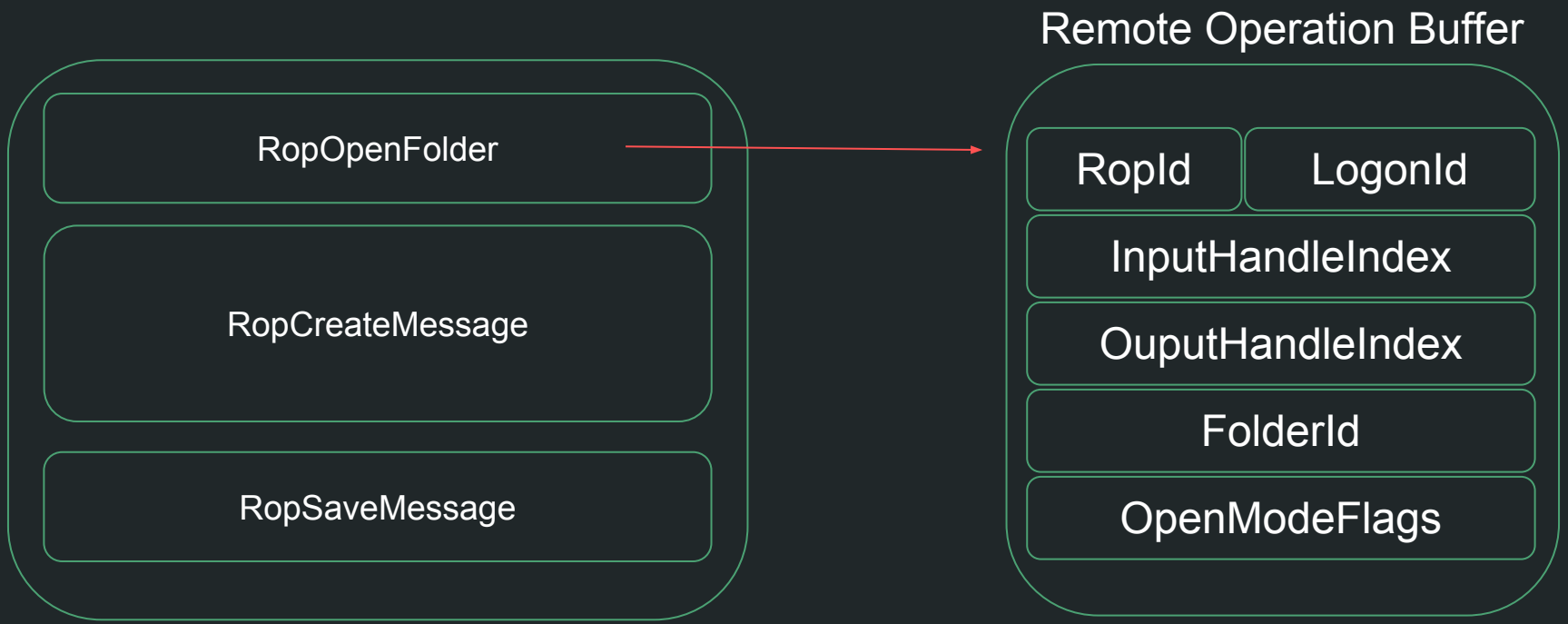
MAPI

Message Application Programming Interface

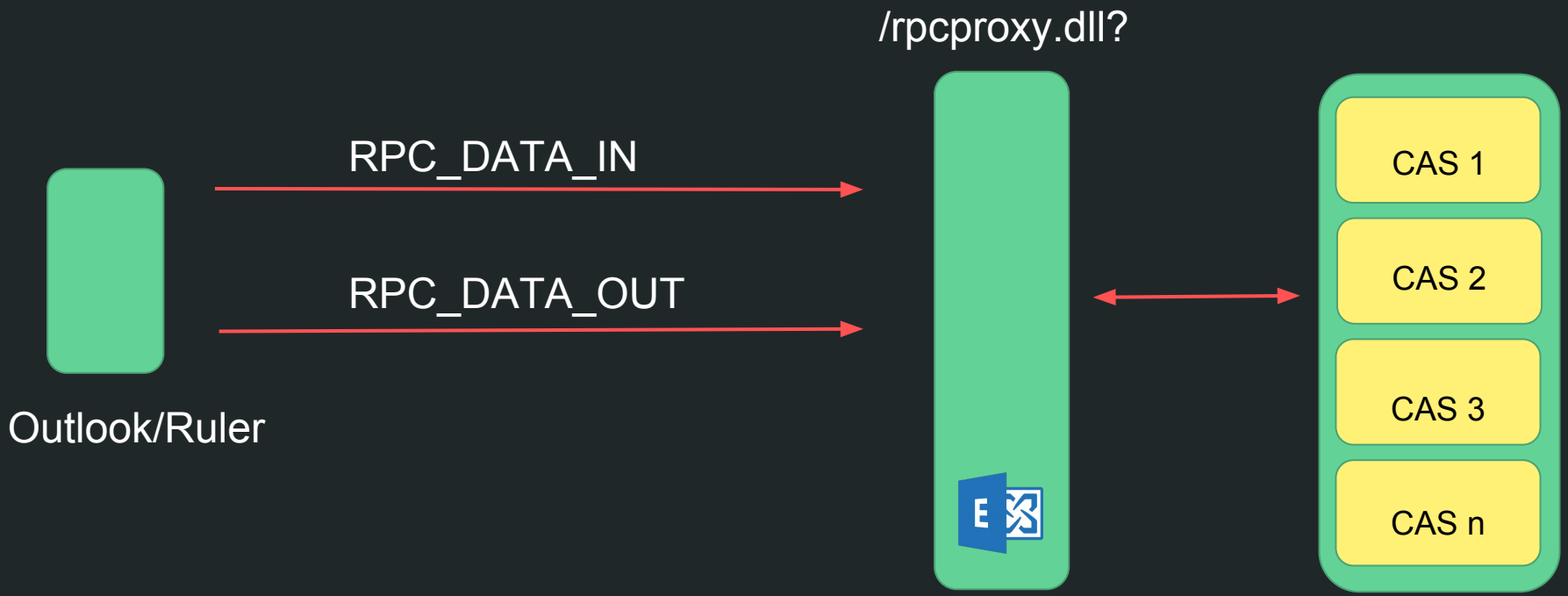
TROOPERS

sensepost

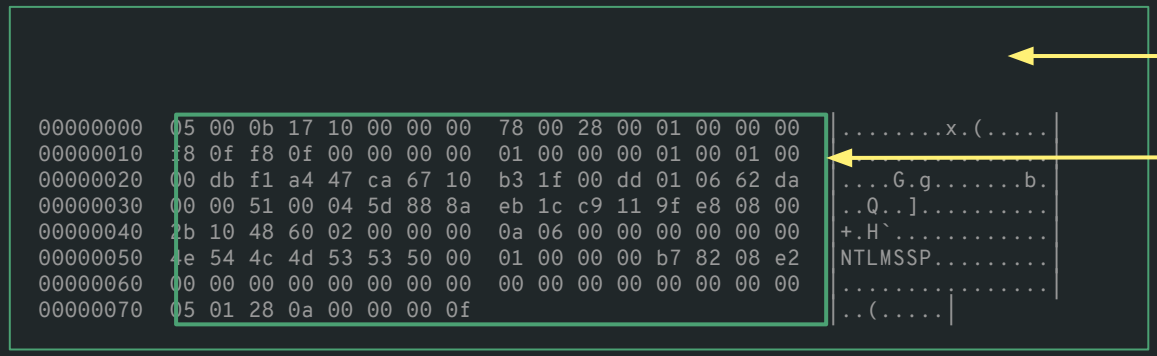
MAPI


RopOpenFolder
RopCreateMessage
RopSaveMessage
Remote Operation Buffer
RopId
LogonId
InputHandleIndex
OuputHandleIndex
FolderId
OpenModeFlags

RPC/HTTP


/rpcproxy.dll?
RPC_DATA_IN
RPC_DATA_OUT
Outlook/Ruler
CAS 1
CAS 2
CAS 3
CAS n

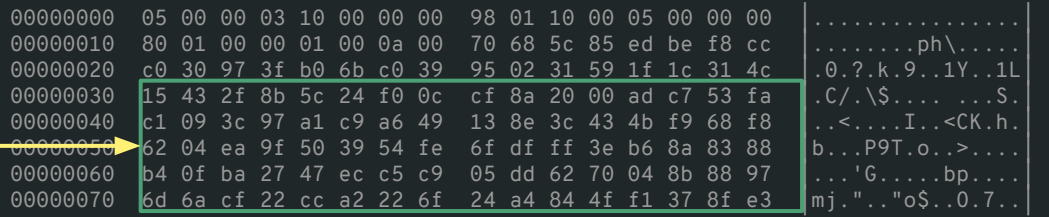
RPC/HTTP



HTTP

DCE/RPC

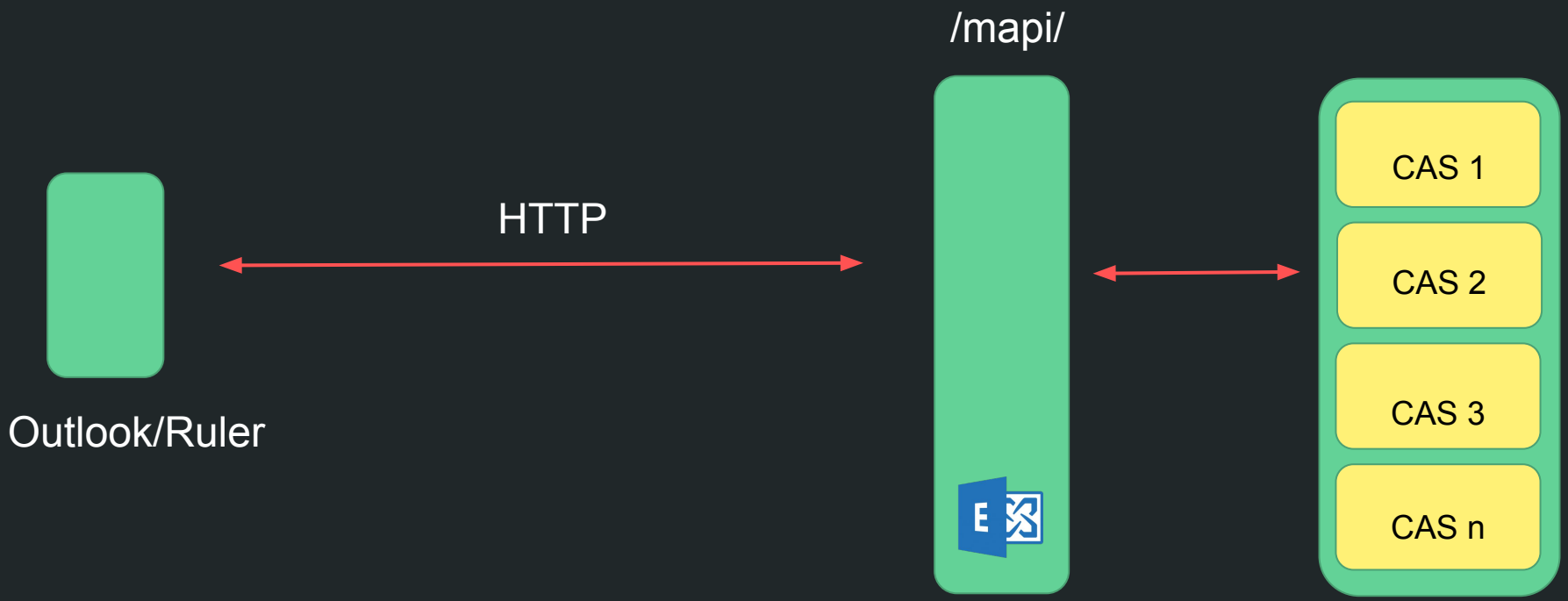
MAPI
[Encrypted]



TROOPERS

sensepost

MAPI/HTTP



Introducing Ruler

TROOPERS

sensepost

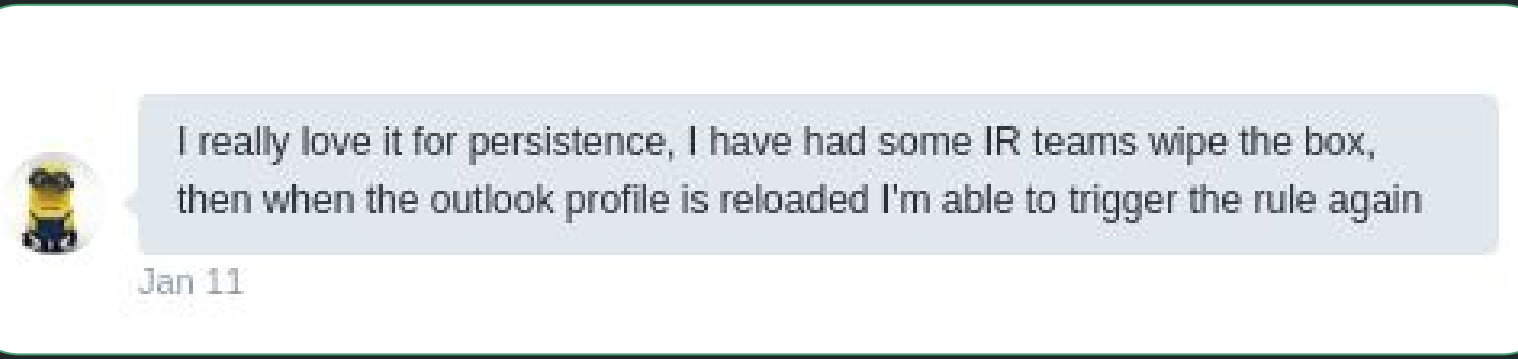
Ruler Demo

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

Persistence

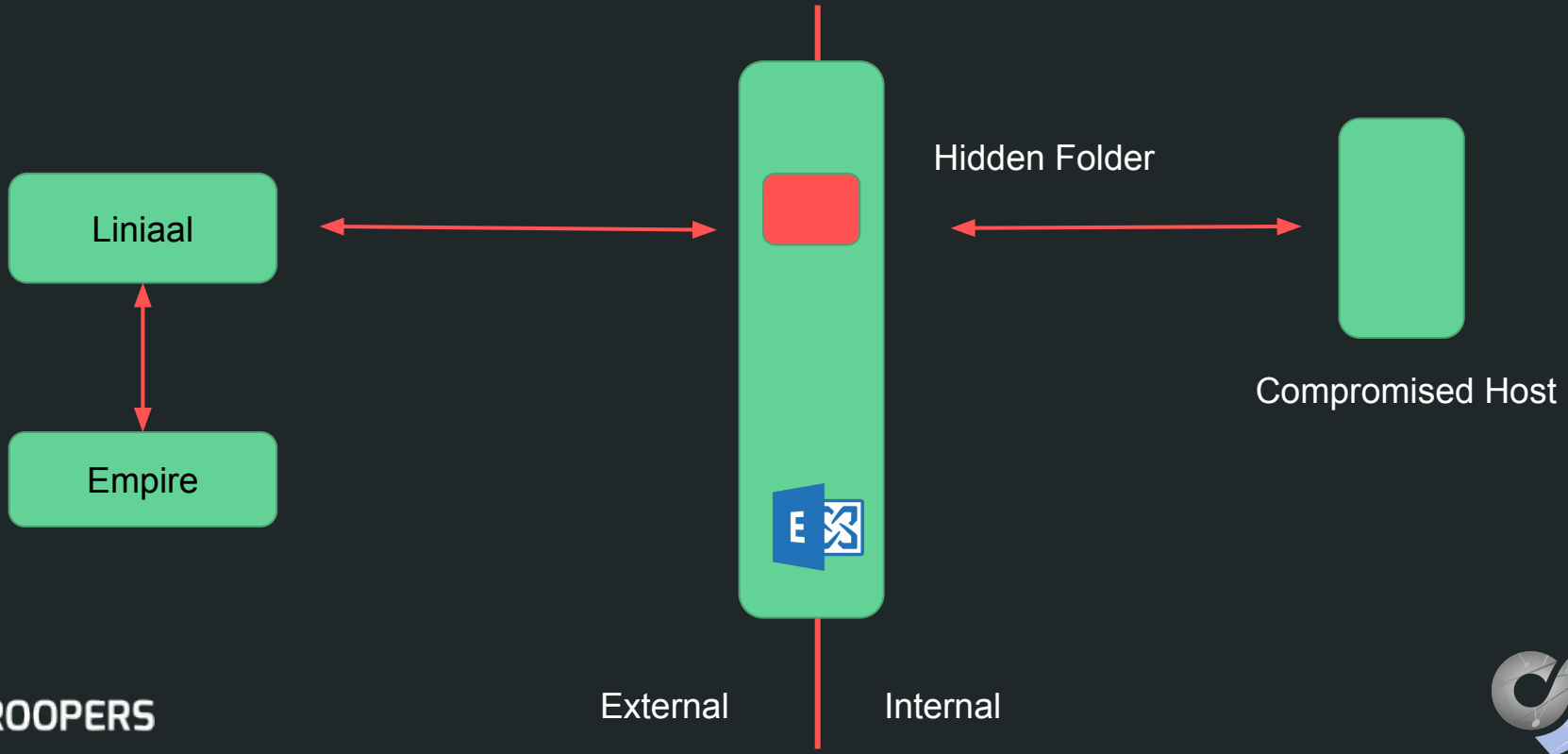
Never going to give you up

I'll never let you go



@slobtresix0 - Scot Berner

Hidden Comms

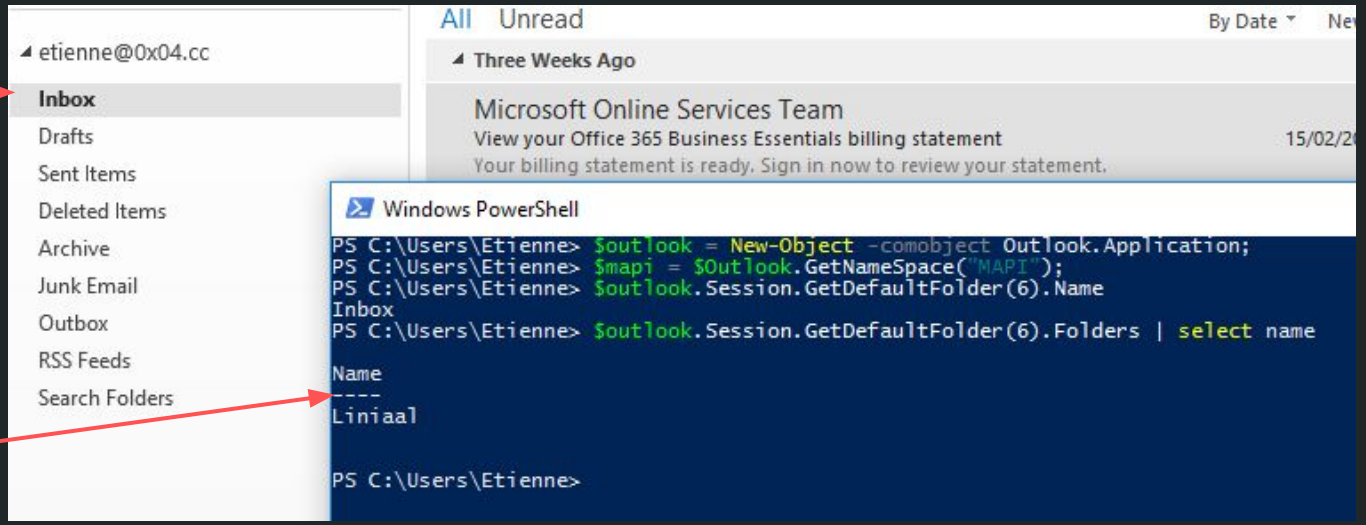


Hidden Comms

Don’t Traverse Traditional Network Boundary

Hidden

Unless you know where to look



TROOPERS

sensepost

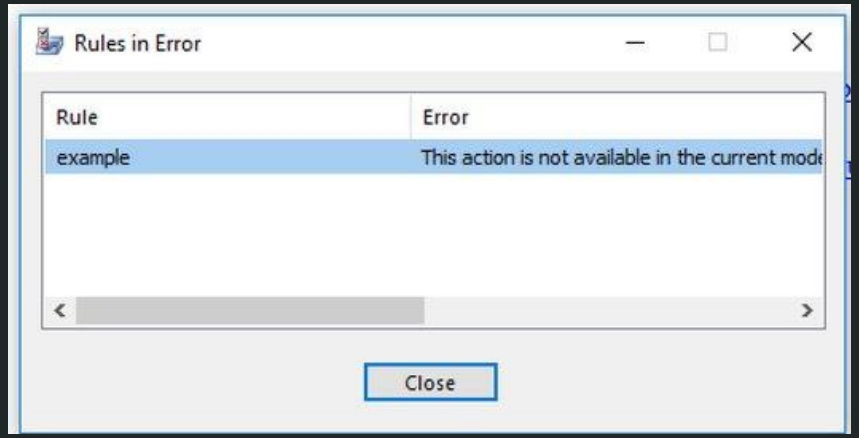
Liniaal Demo

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

TROOPERS

sensepost