



REAL  
INCIDENTS

REAL  
SOLUTIONS

# OUR PERSPECTIVES



@GELRATUMAE2

@JQEORDOANNA M E





DEFEND



# Building & Assessing Security Programs



---

Preparing for  
&  
Responding  
to Incidents



# OUR STORY FOR YOU

A REALISTIC ATTACK

MRP Database  
Accessed

7 PM: 💩

4:52PM

AS&A's IP stolen by  
competitor



Domain Admin

**1:52 PM**

Lateral Movement

**9:33 AM**

Local Admin

The Real Malware

**9:31 AM**

Malicious Email

9:30 AM

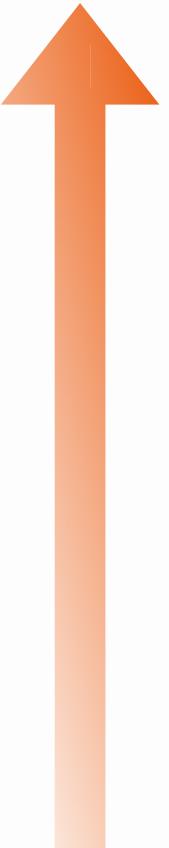
Dropper

9:06 AM



EVERYTHING IS FINE

ACME STEEL & ANVILS

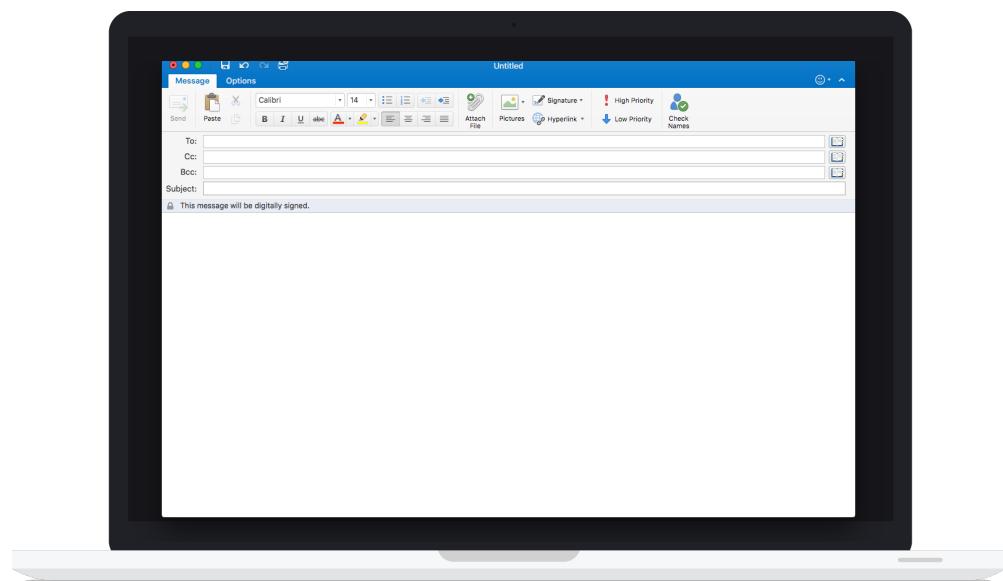


NEXT GEN  
&  
BOURBON



# 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...

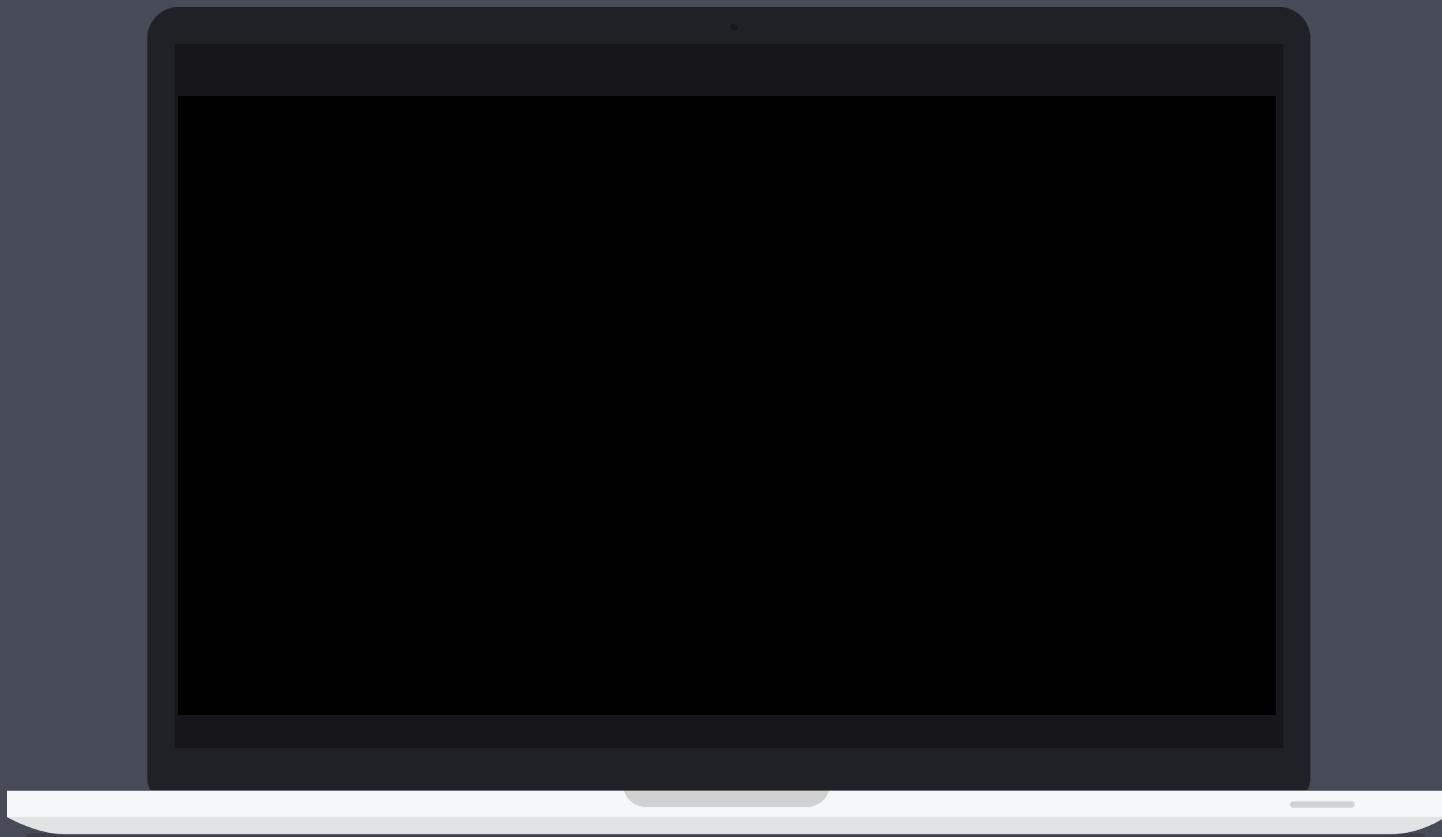
- CEO SCAM
- MALICIOUS LINK
- ATTACHMENT: WORD





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

FREE  
&  
EFFECTIVE





- CLICK-TO-PLAY
- WHITELIST SITES FOR PLUGINS
- DENY OLD PLUGINS
- GPO AVAILABLE A thumbs up emoji.
- 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



- **NGFW**
- **PROXY**
- **ENDPOINT AV**
- **SANDBOXING**
- **TECHNOLOGY**

Typical  
Defenses

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



Extra  
Config

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

# 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

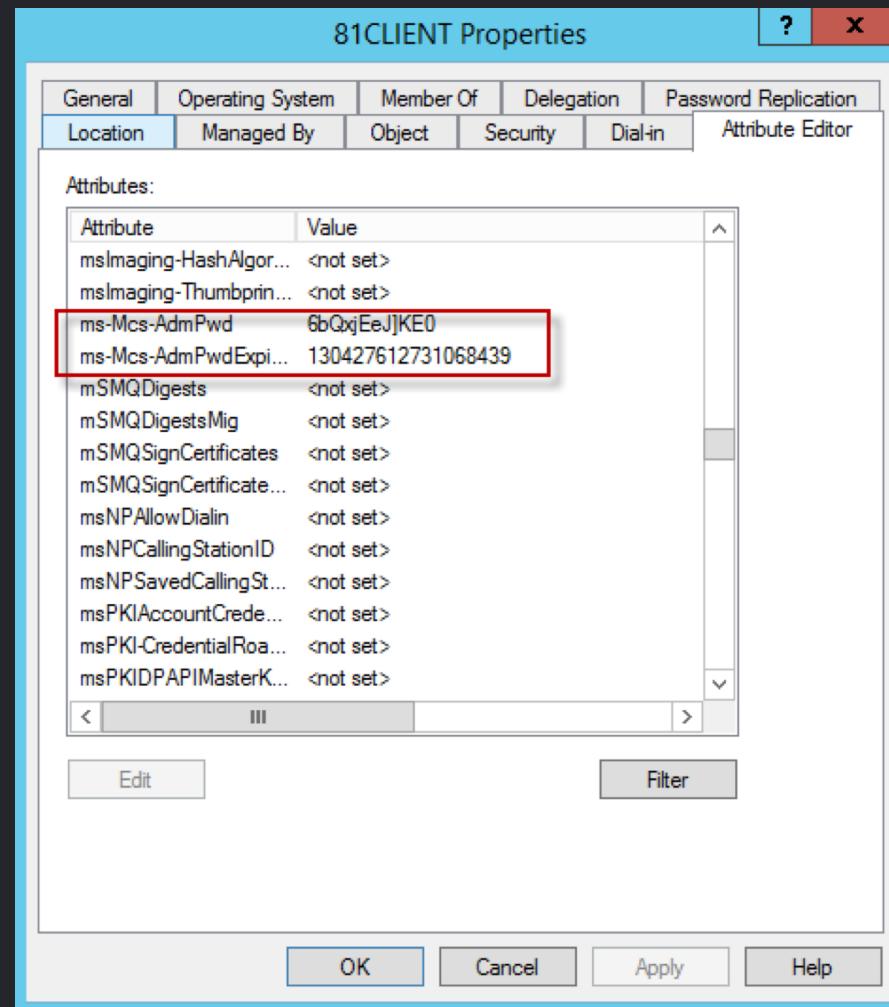
# LAPS

- RANDOMIZED
- AUTOMATED
- DELEGATED  
(MS-MCs-ADMPwd)
- FREE AS IN BEER  
(AS IN FREE BEER)



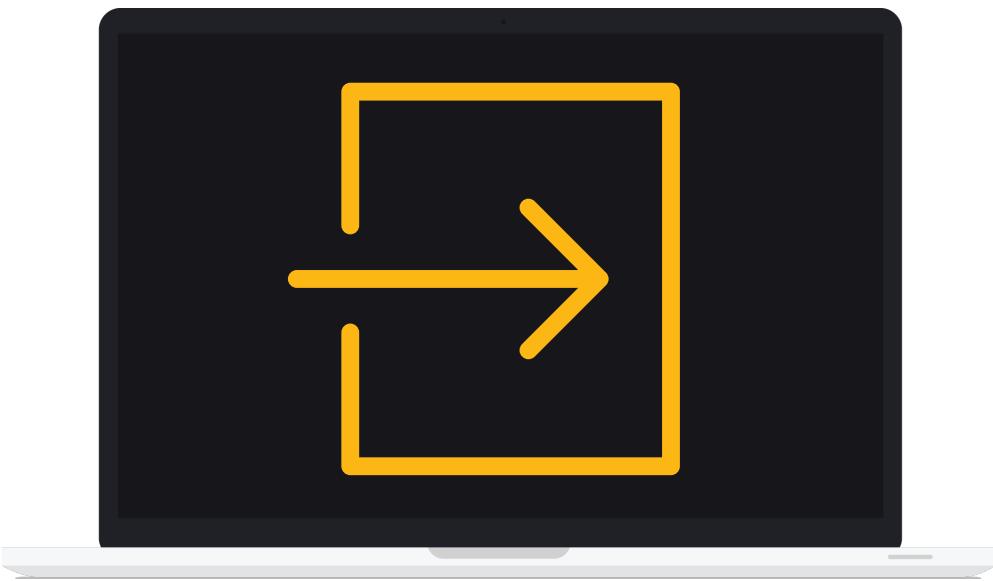
LOCAL ADMINISTRATOR PASSWORD  
SOLUTION

# 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

# 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.



- SERIOUSLY: SEPARATE  
YOUR SERVICE ACCOUNTS
- PATCH DOMAIN  
CONTROLLERS LIKE MAD  
MAX WOULD
- DELEGATE DELEGATE  
DELEGATE
- DEDICATED ADMIN BOXES

FREE  
DEFENSE



# PRIVILEGED ACCESS WORKSTATIONS

The screenshot shows the Windows Active Directory Users and Computers snap-in. On the left, the navigation pane displays the domain structure under 'contoso.com': Builtin, Computers, Domain Controllers, ForeignSecurityPrincipals, and Users. The 'Users' folder is selected. On the right, a list of built-in security groups and users is shown in a table format:

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_contoso	User	Built-in account for anonym...
IUSR_contos	User	Built-in account for anonym...
IWAM_contos	User	Built-in account for Intern...
IWAM_contoso	User	Built-in account for anonym...
PowerUser...	Security Group ...	Members in this group can...

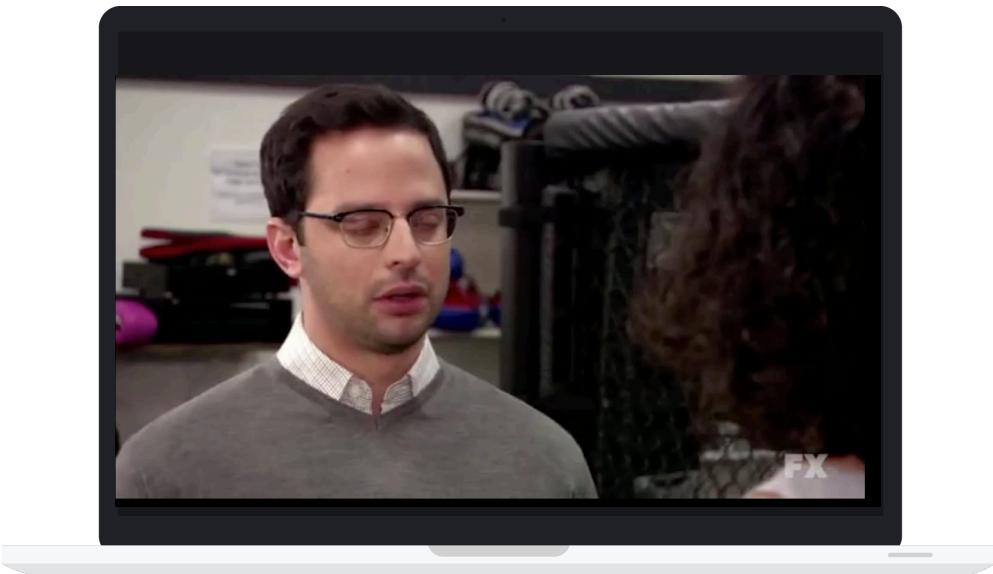


## MORE INFO

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

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

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



CHECK  
PRIVILEGES



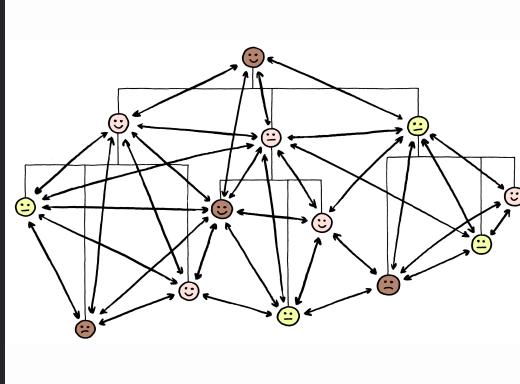
SEGMENT  
SYSTEMS



DELEGATE



RANDOMIZE  
PASSWORDS



EGRESS +  
WEB FILTER

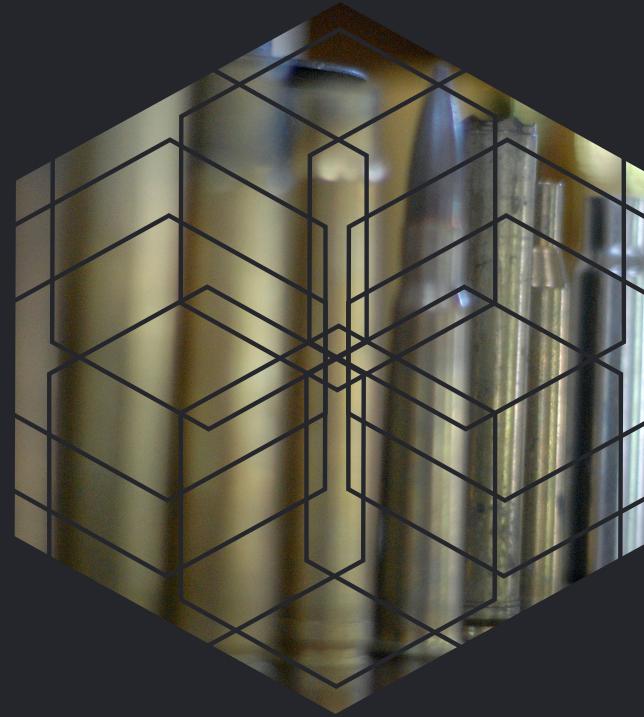


HARDEN  
SYSTEMS

CONCLUSION

# 2016–2017 CHALLENGE

LESS BULLETS  
MORE SHOVELS



THANK YOU

TROLL US

@GEPETO42

@JOEYNONAME

SLIDES AND LINKS: [HTTPS://EVILPLUMBING](https://evilplumbing.com)