

# Modern Realities of Securing Active Directory & the Need for AI



*Our Mission: Hacking Anything to Secure Everything*

7 Feb 2019

**Presenters:**

**Dustin Heywood (EvilMog), Senior Managing Consultant, X-Force Red**

# BIO

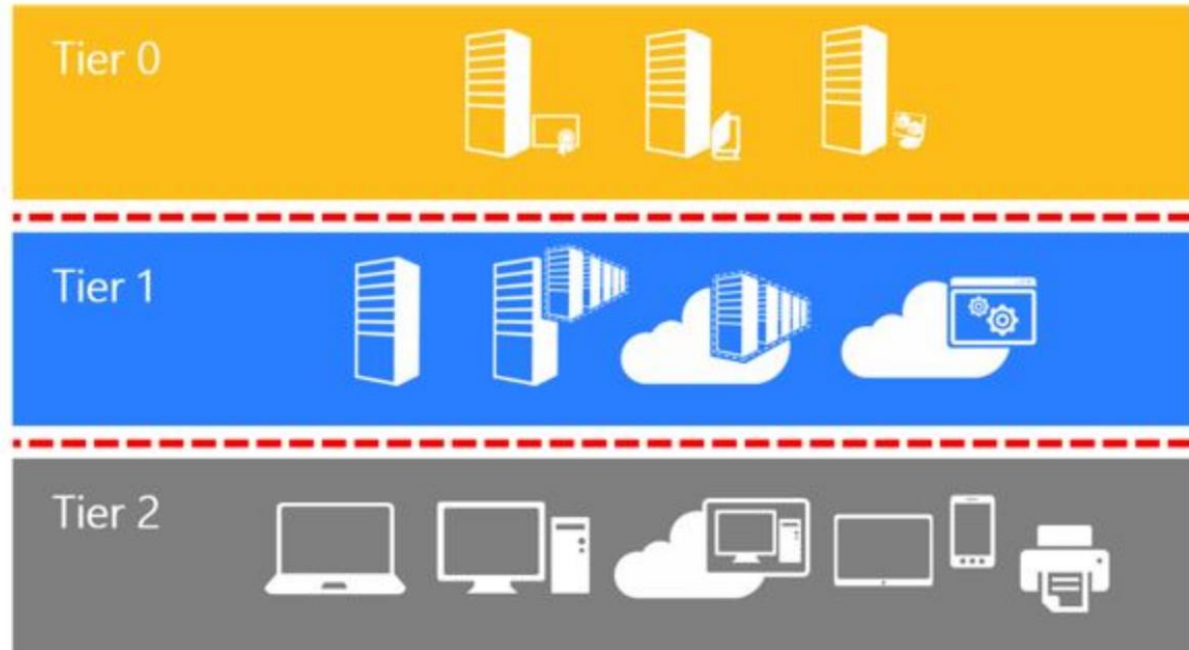
- Senior Managing Consultant, X-Force Red
- EvilMog from Team Hashcat
- Spoken at Multiple Conferences: BC Privacy & Security Conference, Derbycon, SkydogCon, IBM Think, Security BSidesLV
- Specialize in Password Cracking, Active Directory Security & Red Teaming
- Alberta Restricted Locksmith Tools License
- Senior Pyrotechnician (Proximate Fireworks)

# Active Directory Tiers

Tier 0 – Domain Controllers

Tier 1 – Servers

Tier 2 – Desktops



Source: <https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

# Stage 1 – Attacking Desktops

- Every endpoint can be penetrated for the most part
- Attack methods include:
  - Man in the middle via Layer 2 (ARP Poisoning, LLMNR/NBT-NS/WPAD)
  - Code Execution with AMSI Bypass (Powershell, vbscript, jscript, hta files, dde, C#, iron python)
  - Misconfigurations
  - Malware
  - PSEXEC, WMI, WinRM, SMBExec
  - Cold boot and steal SAM/SYSTEM registry hives if drive is not encrypted
- The point is desktops can be compromised in some way shape or form

# The problem with Windows

- Windows keeps credentials in memory on all remote interactive logins with some exceptions until reboot
- NTLM hashes are just a UTF-16LE Encoded String that is then run through MD4
- NTLM hashes are password equivalent in windows
- All authentication in windows such as Kerberos, NTLMv1, NTLMv2, Smart Cards all come down to knowledge of the NTLM Hash
- Most sysadmins leave the same common administrator password across workstations and even servers
- Knowledge of the hash will get you access to other systems, easy lateral movement

# Powershell

- Powershell is the go to post exploitation language of hackers
- Complete access to the Win32 API
- Zero logging of execution below Powershell 5
- Until windows 10 it didn't get scanned by anti-virus
- On by default on all systems As of Windows 2008/Vista

# New Techniques – AMSI & Powershell v5

- AMSI (Anti Malware Scan Interface) is in Windows 10 & Server 2016
  - Makes things substantially harder as it forces scanning of powershell, vbs, and jscript
- Powershell v5
  - Can enforce Script Block Logging, Transcription Logging, Module Logging centrally
- New evil
  - C#, Iron Python, LoLBins (Living off the Land Binaries/Built-in Admin Tools)
  - Entirely in memory, dynamically compiled, next to impossible to signature
  - Reflective Assembly Loading of C# direct through Common Command and Control, no forensic evidence without memory monitoring
- Most SIEMS will not catch this without highly tuned rules and things change all the time

# Malleable C2

- C2 is Command and Control
- Frameworks can now be modified to look like anything on the network from APT's to legitimate network protocols
- Encrypted with randomized keys
- Highly variable communications patterns ranging from a few ms to one callback per day and random intervals
- Communication can be over HTTP, HTTPS, DNS and has API hooks for connections over IRC, SLACK, or anything with an API
- In memory locations, compile times, permissions, process forking, code caves, everything is customizable
- Newer attackers are coding their own custom frameworks faster than you can keep up



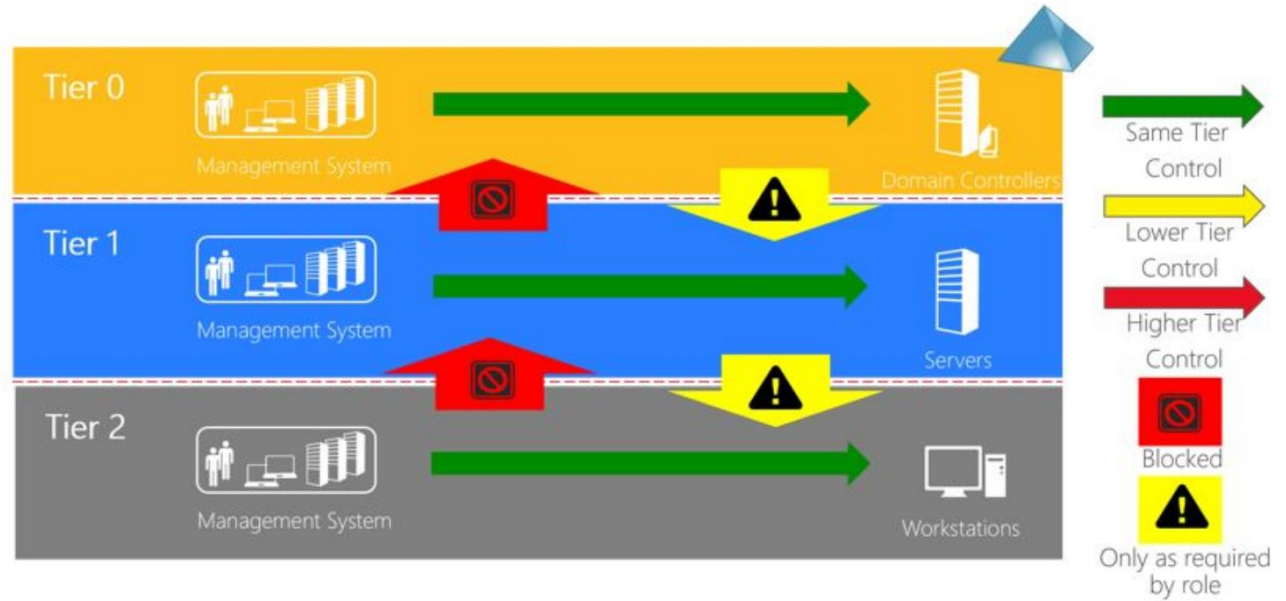
# Attacking Servers

- Servers can be attacked just like desktops
- Techniques such as Kerberoasting can attack AD Itself
- SQL Injections
- Actual Vulnerabilities (MS08-067, MS17-010 etc)
- Print Spooler Vulnerabilities to force hash disclosure
- Exchange Vulnerabilities
- Finally in house applications could have bugs
- Attack surface is endless

# Common Issues

- Server and Domain Administrators manage servers from their desktops
- Take over the Desktop Tier, if the desktop tier has access to server admins you now control servers
- Take over a Server Management Jumpbox and you now own the domain
- Credentials leak over the wire and there are multiple ways to get some kind of foothold

# Tier 0/1/2 Isolation



Tier 0 – Domain Controllers

Tier 1 – Servers

Tier 2 – Desktops

Source: <https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

# Misconceptions

- Active Directory Domains are security boundaries
- Vulnerability Scanners need Domain Admin
- Kerberos Ticket Hash never needs to be rotated
- Desktops/Servers need the same common local admin password for emergencies
- Secrets do not need to be rotated

# Reality

- Active Directory Forest is the Security Boundary
  - If you own a parent or child domain you can take over the entire forest
- Anybody who knows the ktbtgt hash owns your domain (Backup Admins, ESX Admins)
- Vulnerability scanners spray creds that can be captured
- Kerberos ticket hash needs to be rotated twice a year
- All local admin passwords should be randomized
- All privileged secrets must be frequently rotated
- Workstations should block all incoming connections except from management workstations
- Assume every system has been compromised

# Evil Mogs not Patented Active Directory Checklist

- Turn on Windows Firewall
  - Block 3389,445,139,137, 135, 5895/5896 at every network boundary
- Disable LLMNR/NBT-NT/WPAD & Block Arp Poisoning, secure Dynamic DNS Updates
- Get an Endpoint Detection & Response System
- Windows Defender ATP, Credential Guard, Device Guard and Exploit Guard
- Minimum of Windows 10/Server 2016
- Tier 0/1/2 Isolation with Privileged Access Workstations
  - Consider Red Forest + just in time permissions
- Deploy Application Whitelisting such as Applocker (or other commercial solution)
- Deploy a SIEM as well as Windows ATA or other solution (Such as QRADAR)
- Randomize all local admin passwords

# Most Important Line of Defense

- Application Security Testing
- Penetration Testing
- Red Team Engagements once you are confident you can detect attacks
- Vulnerability Management Services
- Phishing and Social Engineering Engagements
- Physical Security Assessments
  
- Repeat often, testing is a point in time view of security and security posture will change

# Contact Information

- Dustin Heywood
- Senior Managing Consultant, X-Force Red
- [evilmog@ibm.com](mailto:evilmog@ibm.com)
- @evil\_mog on Twitter





# THANK YOU

FOLLOW US ON:



[ibm.com/security](https://ibm.com/security)



[securityintelligence.com](https://securityintelligence.com)



[xforce.ibmcloud.com](https://xforce.ibmcloud.com)



[@ibmsecurity](https://twitter.com/ibmsecurity)



[youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2018. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

