Misconfiguration Manager

Still Overlooked, Still Overprivileged

Duane Michael & Garrett Foster

SpecterOps

Scan to download this slide deck

Duane Michael

- Managing Consultant, Adversary Simulation at SpecterOps

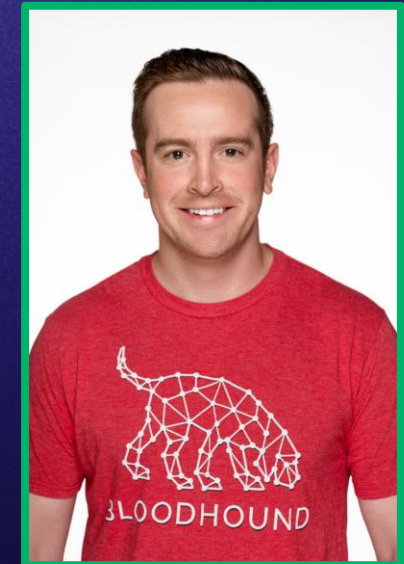- Contributor to SharpSCCM

- @subat0mik on all the things

Garrett Foster

- Senior Security Researcher at SpecterOps

- Primary author of SCCMHunter

- X: @unsigned_sh0rt

Chris Thompson

- Senior Security Researcher at SpecterOps

- Primary author of SharpSCCM and Maestro

- X: @_Mayyhem

TROOPERS

Agenda

What this talk is (and is not) about

This presentation covers:

- 2024 Summary
- 1 Year of MM
- New Technique Highlights
- Community Contributions
- Q&A

This presentation does NOT cover:

- Walkthroughs of *all* offensive techniques
- Defensive and remediation walkthroughs
- Comprehensive treatment of topics discussed

TROOPERS

Misconfiguration Manager

Where we started

- ## What is [Misconfiguration Manager](#)

  - ### Released at [SO-CON](#) & [TROOPERS 24](#)

  - ### Captures all known adversary tradecraft targeting SCCM

  - ### Provides detection and mitigation guidance

TROOPERS

Misconfiguration Manager

Where we started…

- ## The initial release contained:

  - 9 TAKEOVERs

  - 5 RECONs

  - 5 CREDs

  - 3 ELEVATEs

  - 2 EXECs

  - 22 PREVENTs

  - 5 DETECTs

  - 1 CANARY

TROOPERS

Misconfiguration Manager

Where we are now…

- Over the past year, with the help of the community, we've added:

  - 1 TAKEOVER

  - 2 RECONs

  - 3 CREDs

  - 2 ELEVATEs

  - 3 EXECs

  - New COERCE category

  - 3 COERCEs

  - 6 DETECTS

TROOPERS

What we (and the community) have been up to…

TAKEOVER-1 Recap

Our favorite, and most common, TAKEOVER primitive

- Site database is not hosted on the coercion target

- Primary site servers and SMS Providers are "db_owner" on site DB

- Coerce a system with one of these roles

- Relay it to site DB

- Grant SCCM "Full Administrator" by modifying "RBAC_Admins" table

TROOPERS

The Problem with TAKEOVER-1

There was one glaring issue…

- When found, TAKEOVER-1 allows a privilege escalation from *Domain Users* to site/hierarchy compromise

- But… we couldn't reliably enumerate standalone site DBs

- We relied on SPNs and hostnames

  - *MSSQL/SQLSCCM01.CORP.LOCAL:1433*

RECON-6

- Primary site servers and distribution points create reg keys

  - *HKLM\SOFTWARE\MICROSOFT\SMS**

- World-readable over WINREG, regardless of DACL

  - Key path set in local security policy on PSS and DP

- Keys contain site system information

- Weaponzied in pssrecon

- *Discovered, weaponized, and contributed by Dylan Bradley (@slygoo)*

TROOPERS

10

Time to Talk About Creds…

Again…

- There's more creds than we thought…

  - *Azure Application (Co-management), Discovery Accounts, Site-Installation Accounts, and more*

- All cred blobs retrievable via AdminService API and WMI (CRED-7 & 8)

  - CRED-7 weaponized by Garrett

CREDS

CREDS EVERYWHERE

TROOPERS

CRED-1 is More Practical

With the help of a little bit of PXE dust…

- CRED-1 can now be abused over SOCKS via C2

  - Previously required direct network access

  - Weaponized by [Adam Chester](#) in [cred1py](#)

Do You Want to Terrify Your Target?

CmRc will help you do that!
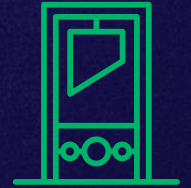
- ConfigMgr Remote Control

  - Allows admins to RDP to clients or shoulder surf users

  - Viable as a standalone tool, only requires admin on target

  - Settings controllable by local admin of target or SCCM Admin

  - Invisible to target users

  - Shared clipboard

Do You Want to Terrify Your Victim?

CmRc will help you do that!

- Viable as an execution technique a la VNC (EXEC-3)

- Requires local admin on target or SCCM admin

  - [Blogged](#) by [Chris Au](#)

- Also, a stealthy recon and credential access technique

  - Invisible to logged on users (shoulder surf)

  - Clipboard is shared

- *Allows taking over input and locking a user out while forcing them to watch you pillage!*

ELEVATE-4

Pre-Owned PXE Boot

- SCCM PKI configurations require client authentication certs for OSD

    - Found by @onSec-fr

- The cert is distributed to every PXE client during deployment

- It's a feature!*

    - "…only used during the OS deployment process."

    - "…use the same certificate for every OS deployment…"

- No PXE password = zero to hero

    - *Maybe even the site server…*

TROOPERS

```
┌─(sccmhunter)─(kali㉿sccm-kali)-[~/demo/PXEThief]
└─$ 
```

ELEVATE-5

Pre-Owned OSD Images

- Same PKI cert gets pushed into OSD images

- Images live on admin selected distribution points as packages

  - Found with CRED-6

- Just need an authenticated user to pull the images down

  - *But we've seen anonymous auth via HTTP…*

Community Contributions

Thank you to everyone who has contributed!

- Josh Prager – DETECT-5-8

- Diego Lomellini – RECON-4, COERCE-1

- Adam Chester – CRED-1 Update

- Alberto Rodriguez & Erik Hunstad – CRED-6

- Marshall Price – DETECT-4

- Dylan Bradley – RECON-6

- *And everyone that's furthering SCCM tradecraft research & discovery!*

TROOPERS

Future Work

Where we're going…

- Microsoft is collaborating and taking this seriously!

- There is SO much more work to be done:
  - Offensive research
  - Detection strategies
  - Configuration guidance

- We want to hear your stories and ideas!

- Pull requests welcome and encouraged

- Collaborate with us in #sccm on BloodHound Slack
  - Invite link: https://ghst.ly/BHSlack

https://misconfigurationmanager.com

Thank you!

Chris Thompson | @_Mayyhem

Duane Michael | @subat0mik

Garrett Foster | @garrfoster

Scan to download this slide deck