



Supercharge your vuln finding workflow with automated labs:

How Ludus made it rain 💧 creds from SCCM

Has this been you?

— □ ×



This is perfect!



JiaT75 / CVE-2024-1234

Q Type [f] to search

>

+ ▾

🕒

🔗

📧

<> Code

🕒 Issues 12

🔗 Pull requests 2

🕒 Actions

📁 Projects

🔒 Security

📈 Insights

CVE-2024-1234

Public

👁 Watch 4 ▾

🍴 Fork 7 ▾

☆ Star 11 ▾

🔗 master ▾

🔗 1 Branch

🏷 0 Tags

Q Go to file

t

Add file ▾

<> Code ▾

JiaT75 removed STEST macro and changed to use __func__ instead

b99690b · 2 days ago

🕒 38 Commits

📁 .github/workflows	Fix CI error	2 days ago
📁 src	removed STEST macro and changed to use __func__ inst...	2 days ago
📁 tests	removed STEST macro and changed to use __func__ inst...	2 days ago
📄 .clang-format	Added clang format based on LLVM styling	3 days ago
📄 .gitignore	Added gitignore to project	3 days ago
📄 CMakeLists.txt	Adding cmake support	3 days ago
📄 README.md	removed STEST macro and changed to use __func__ inst...	2 days ago
📄 license.txt	Adding copyright to license	3 days ago

📖 README

📄 License

✎

☰

CVE-2024-1234

About

An exploit that you need to further your objectives in a customer environment.

c

trust-me

cpp

xunit

legit

📖 Readme

📄 View license

🔗 Activity

☆ 11 stars

👁 4 watching

🍴 7 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

C 99.0%

CMake 1.0%

Did you just YOLO that binary?



THREAT ANALYSIS GROUP

New campaign targeting security researchers

Jan 25, 2021 · 4 min read



Adam Weidemann
Threat Analysis Group

Hackers Lure Cybersecurity Researchers With Fake LinkedIn Recruiter Profiles

Campaign demonstrates the DPRK-backed cyberattackers are gaining tools to avoid EDR tools.



Dark Reading Staff, Dark Reading
March 13, 2023

1 Min Read

Editor's Choice

Daryna Antoniuk

September 7th, 2023

North Korean hackers target security researchers with new zero-day

State-backed North Korean hackers are reportedly targeting security researchers using at least one zero-day vulnerability, Google warned in a [report](#) released Thursday.

For the past two-and-a-half years, the researchers have been tracking campaigns by the threat actors they believe are behind the recent attacks.

Nation-state

Cybercrime

News

Did YOU just YOLO that binary?



Network Outage - Call Me External Inbox x



Angry Joe joe@angryclient.com

to me ▾

Hello,

We are experiencing a large network outage and our <insert EDR Vendor> is generating a lot of alerts. We believe it is due to your testing.

Our users are calling IT.

The CEO/CISO would like get on a call with you and your team immediately.

Thanks

- Angry Joe



- Erik Hunstad (@badsectorlabs)
 - Founder @ Bad Sector Labs
 - Previously
 - CTO @ Sixgen
 - DoD



- Alberto Rodriguez (@__ar0d__)
 - MSC @ GuidePoint Security (TAS)
 - Previously
 - Fortune 500
 - DoD

AGENDA



Intros

Automated Lab/Range Landscape

Our Solution - Ludus!

Use Case: Complex environments (Ahem.. SCCM)

Questions


Lab/Range Automation Tools

- Commercial
 - Immersive Labs (formerly Snap Labs)
 - SimSpace (mostly DoD)
 - Hack the Box
 - Try Hack Me
 - Pentester Lab
 - Various paid courses offer labs
- Open-Source
 - Detection Lab (archived 2023-01-01)
 - AutomatedLab (Powershell/HyperV only)
 - Game of Active Directory aka GOAD
 - ADLab (vagrant/ansible)
 - AD-Lab (Powershell)



Lab/Range Automation Tools - Disadvantages



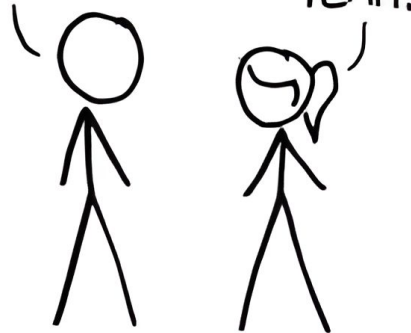
- Cloud based
 - 
 - No access to underlying infrastructure
 - Telemetry?
- Rigid
 - Fixed domain names
 - Fixed IPs
 - Fixed user accounts, vulnerabilities, etc
- Single user
 - No easy way to share with teammates
- Single EDR/logging solution - if any
- No concept of OPSEC
- Hard to extend

Introducing...

HOW STANDARDS PROLIFERATE: (SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)

SITUATION:
THERE ARE
14 COMPETING
STANDARDS.

14?! RIDICULOUS!
WE NEED TO DEVELOP
ONE UNIVERSAL STANDARD
THAT COVERS EVERYONE'S
USE CASES.



SOON:

SITUATION:
THERE ARE
15 COMPETING
STANDARDS.

Ludus

Goal: Solve infrastructure management for cybersecurity

- **Easy**

- One static binary
- Install instructions: `./ludus-server`
- Static **client binaries** for Windows/Linux/macOS
- Open source, fully documented, API driven
- Cloud or On-prem

- **Flexible**

- Templates are base OS installs
- Labs build dynamically during deploy
- No “golden master” templates (unless you want them)
- Domains, IPs, users, software etc all configured by the user

- **Expandable**

- Use any ansible role available today
- Write your own roles and use/share them easily
- Chocolatey support



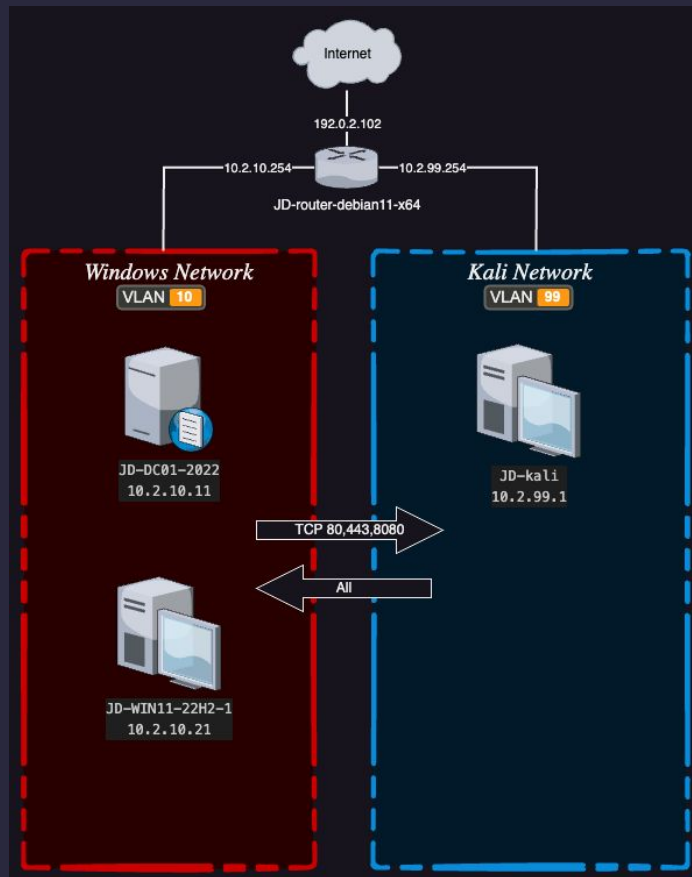
ANSIBLE



Ludus range config YAML

YAML

```
ludus:
- vm_name: ad-dc-win2022-server-x64
  hostname: JD-DC01-2022
  template: win2022-server-x64-template
  vlan: 10
  ip_last_octet: 11
  ram_gb: 8
  cpus: 4
  windows:
    sysprep: true
    domain:
      fqdn: ludus.domain
      role: primary-dc
- vm_name: ad-win11-22h2-enterprise-x64-1
  hostname: JD-WIN11-22H2-1
  template: win11-22h2-x64-enterprise
  vlan: 10
  ip_last_octet: 21
  ram_gb: 8
  cpus: 4
  windows:
    install_additional_tools: true
    office_version: 2019
    office_arch: 64bit
  domain:
    fqdn: ludus.domain
    role: member
```



Ludus - Roles


- Roles created by BSL
 - ADCS
 - Veloricator
 - Apache Guacamole
 - MSSQL
 - Bloodhound CE
 - Elastic Container
 - Elastic Agent
 - XZ Backdoor
 - Vulhub
 - EMUX
 - Commando VM
 - Flare VM
 - REMNUX
- Community Roles
 - SCCM 💰🌂
 - Wazuh Server
 - Wazuh Agent
 - MS Exchange
 - Child Domain
 - Child Domain Join
 - Local Users
 - Gitlab CE
 - AD Content (OUs, Groups, Users)
 - More coming soon!

Remember - Any existing Ansible role works with Ludus!

Configuration Manager (SCCM) - What is it?



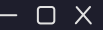
Microsoft: Configuration Manager is part of the Microsoft Intune family of products. The Microsoft Intune family of products is an integrated solution for **managing all of your devices**. Microsoft brings together Configuration Manager and Intune, without a complex migration, and with simplified licensing.

Red teams: A living-off-the-land C2 framework 

TLDR

Deploy software updates, OS deployments, endpoint protection, asset inventory, and more!

SCCM - Deploy Range Demo



Synzack / ludus_sccm

Public

SCCM - Range Complete!

→ /tmp ludus range status

USER ID	RANGE NETWORK	LAST DEPLOYMENT	NUMBER OF VMS	DEPLOYMENT STATUS	TESTING ENABLED
AR	10.2.0.0/16	2024-08-04 11:50	9	SUCCESS	FALSE

PROXMOX ID	VM NAME	POWER	IP
110	AR-router-debian11-x64	On	10.2.10.254
111	AR-DC01	On	10.2.10.10
112	AR-elastic-server	On	10.2.10.9
113	AR-Workstation	On	10.2.10.11
114	AR-sccm-distro	On	10.2.10.12
115	AR-sccm-sql	On	10.2.10.13
116	AR-sccm-mgmt	On	10.2.10.14
117	AR-sccm-sitesrv	On	10.2.10.15
118	AR-kali	On	10.2.99.1

SCCM - Distribution Points

SCCM distribution points (DPs) are the servers used by Microsoft SCCM to **host all the files** used in software installs, patches, script deployments, etc.

By default, these servers allow access via SMB (TCP/445) and HTTP/S (TCP/80 and/or TCP/443) and require some type of Windows authentication (i.e. NTLM).

1. Are defenders monitoring SMB for this SMB looting?
2. Can we get these files from the SCCM DP via HTTP/S? 🤔

— □ ×

They can then locate the actual file at **FileLib/<hash[0:4]>/<hash>**. This works because with access to the share, you can enumerate all files in the DataLib folder.

[illegible]

SCCM - SMB Looting Workflow (Datalib)

SCCMContentLib\$

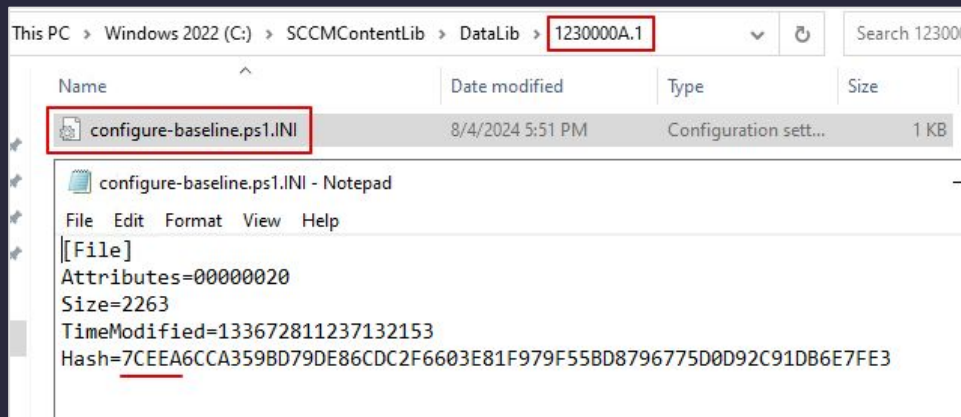
Datalib

Filelib

Pkglib

7CEE

1. Enumerate **every folder** in Datalib
2. Read existing any <filename>.ini in those folders
3. Extract **first 4 chars** & the **full hash** for later use



SCCM - SMB Looting Workflow (Filelib)



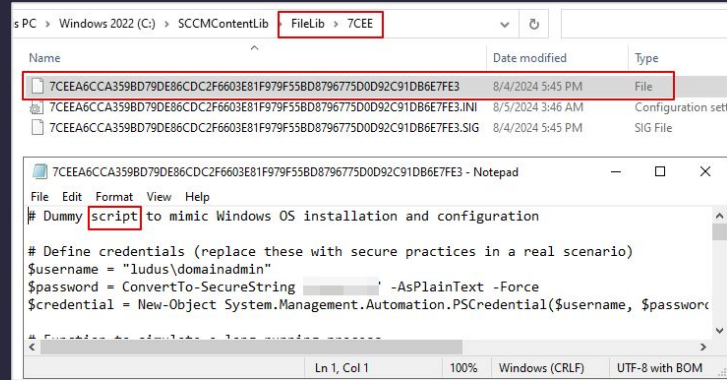
SCCMContentLib\$

Datalib

Filelib

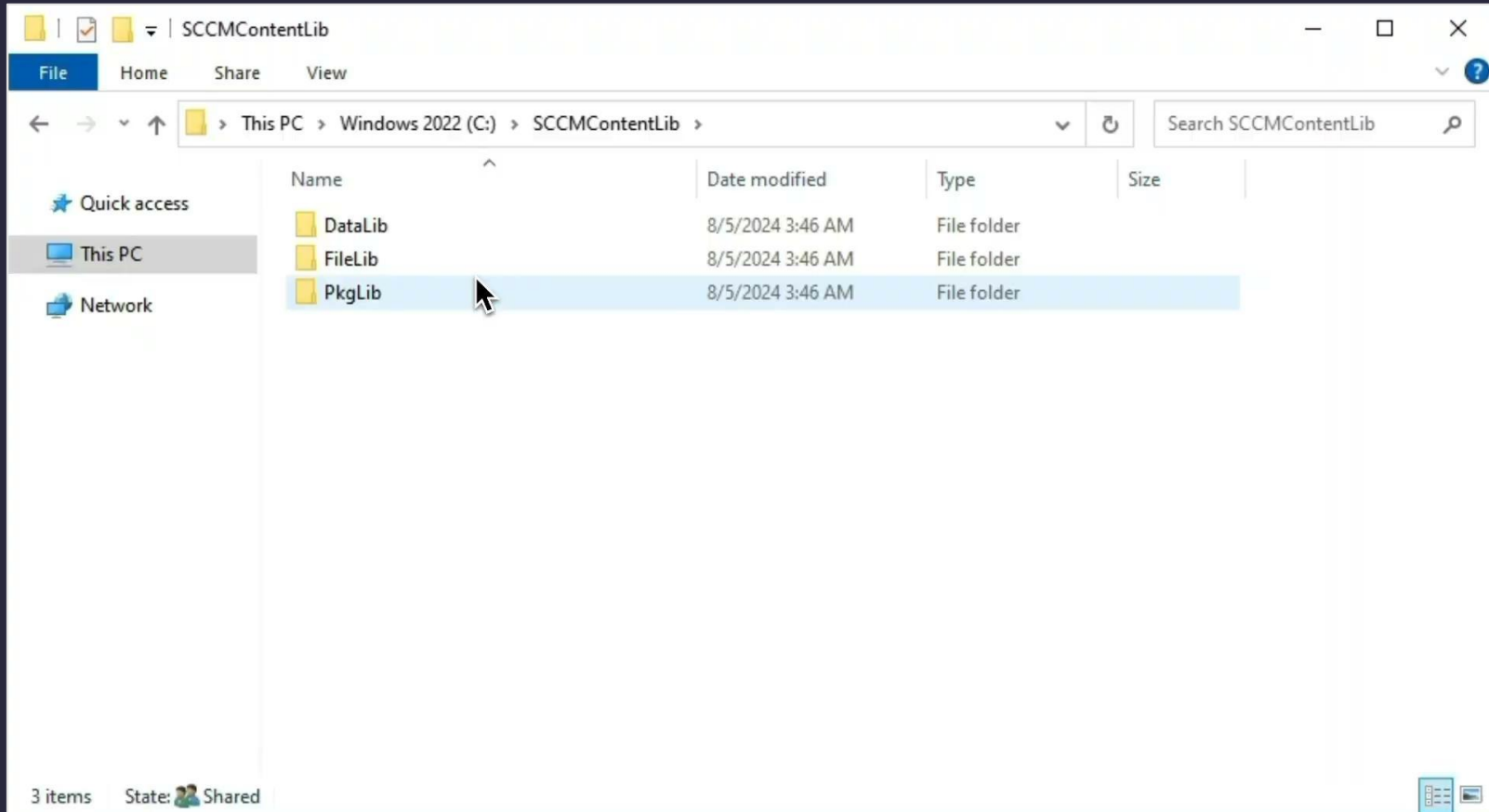
Pkglib

7CEE



1. Open FileLib/<hash[0:4]/><hash>
2. Download the file that is named with the full hash
3. Rename with the proper file extension

SCCM - SMB Looting Workflow (Recap)



SCCM - SMB Looting (Tooling)

1. <https://github.com/1njected/CMLoot> - Powershell (S/O Tomas Rzepka 🤖)
2. <https://github.com/jfjallid/go-cmloot> - Golang
3. <https://github.com/shelltrail/cmloot> - Python

```
(.env)-(root@AR-kali)-[/opt/cmloot]
# python3 cmloot.py ludus.domain/domainuser@10.2.10.12 -cmlootdownload sccmfiles.txt
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[+] sccmfiles.txt exists. Remove it if you want to recreate the inventory.
[+] Extensions to download ['XML', 'INI', 'CONFIG', 'PS1', 'VBS']
[+] Creating CMLootOut
[+] Downloaded F906-ep_defaultpolicy.xml
[+] Downloaded 7CEE-configure-baseline.ps1

(.env)-(root@AR-kali)-[/opt/cmloot]
# head -n 5 CMLootOut/7CEE-configure-baseline.ps1
# Dummy script to mimic Windows OS installation and configuration

# Define credentials (replace these with secure practices in a real scenario)
$Username = "ludus\domainadmin"
$password = ConvertTo-SecureString "password" -AsPlainText -Force
```

SCCM - DP HTTP Looting 🧐



SCCM-DISTRO ► Sites ► Default Web Site ► SMS_DP_SMSPKGS ►

File View Help

Connections

- Start Page
- SCCM-DISTRO (ludus\domainadmin)
 - Application Pools
 - CCMTOKENAUTH_SMS_DP_SMSPKGS
 - CCMTOKENAUTH_SMS_DP_SMSSIGS
 - SMS_DP_SMSPKGS**
 - DataLib
 - FileLib
 - PkgLib
 - SMS_DP_SMSSIGS

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Windows Authentication	Enabled	HTTP 401 Challenge

Advanced Settings

(General)

Application Pool: SMS Distribution Points Pool

Physical Path: C:\SCCMContentLib

Physical Path Credentials

Physical Path Credentials Logon: ClearText

Preload Enabled: False

Virtual Path: /SMS_DP_SMSPKGS

Behavior

Enabled Protocols: http

Virtual Path [path] URL path for the applic

Configuration: 'Default Web Site/SMS_DP_SMSPKGS' web.config

10.2.10.12/SMS_DP_SMSPKGS/DataLib

10.2.10.12

This site is asking you to sign in.

Username

Password

Cancel Sign in

ized: Access is denied due to invalid
ission to view this directory or page using the cre

SCCMContentLib

File Home Share View

This PC ► Windows 2022 (C:) ► SCCMContentLib ►

Name	Date modified	Type	Size
DataLib	8/4/2024 4:35 PM	File folder	
FileLib	8/4/2024 1:55 PM	File folder	
PkgLib	8/4/2024 1:55 PM	File folder	

Quick access

- Desktop
- Downloads
- Documents

SCCM - Anonymous Authentication



```
8/ 4/2024 4:04 pm <dir> http://10.2.10.12/SMS_DP_SMSPKG$/datalib\12300003.1
8/ 4/2024 4:04 pm 100 http://10.2.10.12/SMS_DP_SMSPKG$/datalib\12300003.1.INI
8/ 4/2024 4:04 pm <dir> http://10.2.10.12/SMS_DP_SMSPKG$/datalib\12300004.1
8/ 4/2024 4:04 pm 100 http://10.2.10.12/SMS_DP_SMSPKG$/datalib\12300004.1.INI
8/ 4/2024 4:55 pm <dir> http://10.2.10.12/SMS_DP_SMSPKG$/datalib\12300005.2
8/ 4/2024 4:55 pm 100 http://10.2.10.12/SMS_DP_SMSPKG$/datalib\12300005.2.INI
8/ 4/2024 4:14 pm <dir> http://
8/ 4/2024 4:15 pm 100 http://
8/ 4/2024 8:45 pm <dir> http://
8/ 4/2024 8:45 pm 100 http://
8/ 4/2024 8:51 pm <dir> http://
8/ 4/2024 8:51 pm 100 http://
```

Internet Information Services (IIS) Manager

SCCM-DISTRO > Sites > Default Web Site > SMS_DP_SMSPKG\$

File View Help

Connections

- Start Page
- SCCM-DISTRO (Iudus\domainadmin)
 - Application Pools
 - Sites
 - Default Web Site
 - CCMTOKENAUTH_SMS_DP_SMSPKG\$
 - CCMTOKENAUTH_SMS_DP_SMSSIG\$
 - SMS_DP_SMSPKG\$**
 - DataLib
 - FileLib
 - PkgLib
 - SMS_DP_SMSSIG\$

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Windows Authentication	Enabled	HTTP 401 Challenge

SCCM - "Zippidity Fast!"



how to speed up sccm distribution point

All

Videos

Images

Forums

News

Shopping

Web

More

Tools

AI Overview

Learn more

Here are some things you can try to speed up SCCM distribution points:

- Apply KB2905002: This can resolve slow distribution points
- Check IIS: Open IIS on your DP, go to Configuration Editor, uncheck Limit bandwidth usage, and click OK
- Improve disk configuration and memory management: This can make a big difference in SCCM server performance
- Defragment SQL SCCM database indexes: Do this regularly
- Run task sequences with the high-performance power plan: This configures Windows to use its built-in high-performance power plan, which delivers maximum performance at the expense of higher power consumption
- Use PullDPs and BranchCache: DataCache can help save on downloads, and HashCache can help if BranchCache enabled clients are downloading from the DP
- Manually copy content to the distribution point: Use this option when you have large packages, with content such as an operating system, and you never want to use the network to distribute the content to the distribution point

Soft Tech Community

Content Distribution Points and BranchCache

19 — DataCache 50% of the times better download...

System Center Dudes

SCCM 2012 Slow Distribution Point | System Center Dudes

Learn Microsoft

Manage network bandwidth content - Learn Microsoft

Oct 3, 2022 — However, content updates to this package might

Microsoft System Center Configuration Manager

Mr/SCCM

Welcome to Reddit,
the front page of the internet.

BECOME A REDDITOR

and join one of thousands of communities

SCCM 2012 - OSD Download faster with Anonymous Checked

self:SCCM

Submitted 7 years ago by deletejunkemail

Hi Reddit Folks!

After building a DP and testing OSD for some computers, i noticed package downloads were incredibly slow compared to my other DPs that had been in working use for a while.

I noticed on the new DP that i had not checked "Allow clients to connect anonymously" and once i did, downloads with **zippidity fast!** This is under Distribution point Properties > General Tab > HTTP(S) Section for those wondering where this is)

My question is, why does it make downloading packages so much faster than not? I'm guessing it has some sort of authentication process going on but what is the indepth explanation of when/why/how to use this feature.

I appreciate everyone's time in advance!

11 comments share save hide report

SCCM - Exhibit B!

Can't deploy a software package?

Just enable anonymous authentication



Parallels Products Support Partners My Account US / English Search...

Knowledge Base Overview Knowledge Base Forums Parallels Cares

I am not able to deploy a software package or application

4 users found this article helpful

Applies to:
Parallels Device Management
Last Review: Mar 6, 2020

Related Articles:
[Parallels Desktop for Mac mass deployment](#)

Available Translations:

Get updates **Download**

Symptoms

- I am not able to deploy a software package.
- The Distribution Point is configured in HTTP mode.

Logs

In the `/Library/Logs/pma_agent.log` I see the following:

```
01-09 06:51:00.514 W /PolicyTools:704:a13/ Download operation for 'http://win2012r2-001.pmm12.dom/SMS_DP_KGs/T1200007' finished with 204 (Host requires authentication)

01-09 06:51:00.514 D /ContentManager:704:a13/ Url list retrieval status for 'http://win2012r2-001.pmm12.dom/SMS_DP_KGs/T1200007' is 204

01-09 06:51:00.515 I /SoftDistAgent:704:a13/ Software deployment 'T1220006-T1200007-EFAF5F75' completed with 4
```

Cause

Anonymous connections to Distribution Point are not allowed.

Resolution

- Open Configuration Manager Console.
- Navigate to **Administration** → **Overview** → **Distribution Points**.
- In the right pane right-click required **Distribution Point** and click **Properties**.
- In the **General** tab tick **Allow clients to connect anonymously** checkbox:

WIN2012R2-001.PMM12.DOM Properties

SCCM - Accidental Fix?



This was disabled once upon a time? Likely broke some stuff. Sysadmins re-enabled it!? 🧐

Learn / Troubleshoot / Microsoft Intune / Configuration Manager /



IIS application folder SMS_DP_SMSPKG\$ anonymous authentication settings periodically reset to Disabled

Article • 12/05/2023 • 2 contributors



In this article

Symptoms
Cause
Resolution

Como que?

This article **fixes** an issue in which IIS application folder SMS_DP_SMSPKG\$ Anonymous Authentication settings are disabled.

Original product version: System Center Configuration Manager 2007

Original KB number: 2682514

Resolution



In the Configuration Manager console, check the distribution point configuration:

1. Go to **Site Database > Site Management > Site name > Site Settings > Site Systems > Site server**.
2. Right-click the distribution point, and then select **Properties**.
3. Verify whether the checkbox **Allow Clients to connect Anonymously** is selected. If it's unchecked, check it.

SCCM - DP HTTP Loot 1 - Folder Name



If directory listing is ENABLED:

- Download Datalib → Parse Datalib → Extract Non-INI folder names
- <SCCM DP>/SMS_DP_SMSPKG\$/<Folder Name> to see full URL paths
- <SCCM DP>/SMS_DP_SMSPKG\$/<Folder Name>/<Filename.ext>
- GET request to the full path to file → Download file :)



SCCM - DP HTTP Loot 1 - Signature Files

If directory listing is DISABLED:

- Download Datalib → Parse Datalib → Gather Non-INI Folder name
- <SCCM DP>/**SMS_DP_SMSSIG\$**/**<Folder Name>**.tar
- Extract the **filename** from .tar file (not an actual tars)

```
# xxd 1230000A.1.tar | head -n 10
00000000: 636f 6e66 6967 7572 652d 6261 7365 6c69  configure-baseli
00000010: 6e65 2e70 7331 0000 0000 0000 0000 0000  ne.ps1.....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000030: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000040: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000050: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000070: 0000 0000 0000 0000 0000 0000 3532 0000  .....52..
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000090: 0000 0000 0000 0000 0000 0000 3000 0000  .....0...
```

SCCM - DP HTTP Loot 1 - Signature Files Cont.

- /<SCCM DP>/SMS_DP_SMSPKG\$/Datalib/<filename>/<extracted filename>.INI
- Extract the hash and hash[0:4] from INI file
- Download the file → <SCCM DP>/SMS_DP_SMSPKG\$/<hash[0:4]>/<hash>

```
→ /tmp curl http://10.2.10.12/SMS_DP_SMSPKG$/datalib/1230000A.1/configure-baseline.ps1.INI -O
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100   144   100   144    0    0  13118      0 --:--:-- --:--:-- --:--:-- 14400
→ /tmp head -n 5 configure-baseline.ps1.INI
[File]
Attributes=00000020
Size=2263
TimeModified=133672811237132153
Hash=7CEEA6CCA359BD79DE86CDC2F6603E81F979F55BD8796775D0D92C91DB6E7FE3
```

SCCM - Demo Time!



SCCM - Intro sccm-http-looter



```
(root@AR-kali)-[/opt/sccm-http-looter]  
#
```



SCCM - Unauth DPs are Everywhere

- If we found this in production environments... could we find it on the internet?
- 100's of instances of unauthenticated HTTP/S DPs
- Scripts, custom apps, certificates, oh my
- 💀 Creds in powershell and batch scripts 💀
- Reverse lookup'd emails, responsibly disclosed

SCCM - NTLM Relay to HTTP DP?

SCCM - Porque No?



1. NTLMRelayx (checkout out smbtakeover.py - new 🔥)
2. Coerce Auth || LLMNR/NBT-NS Poisoning || IPv6 || etc.
3. Relay to HTTP service
4. Loot the Distribution Point
5. Profit

<https://github.com/ar0dd/impacket>

PR is in their LONG queue :)

SCCM - NTLM Relay to HTTP Demo



```
(.env)-(root@AR-kali)-[/home/kali/Desktop/impacket]  
# python3 examples/ntlmrelayx.py -t http://10.2.10.12/SMS_DP_SMSPKG$/Datalib --sccm --sccm-dp-dump -smb2support
```

```
(kali@AR-kali)-[~/PetitPotam]  
$ sleep 3; python3 PetitPotam.py 10.2.99.1 10.2.10.13 -u domainuser -p 'password'
```

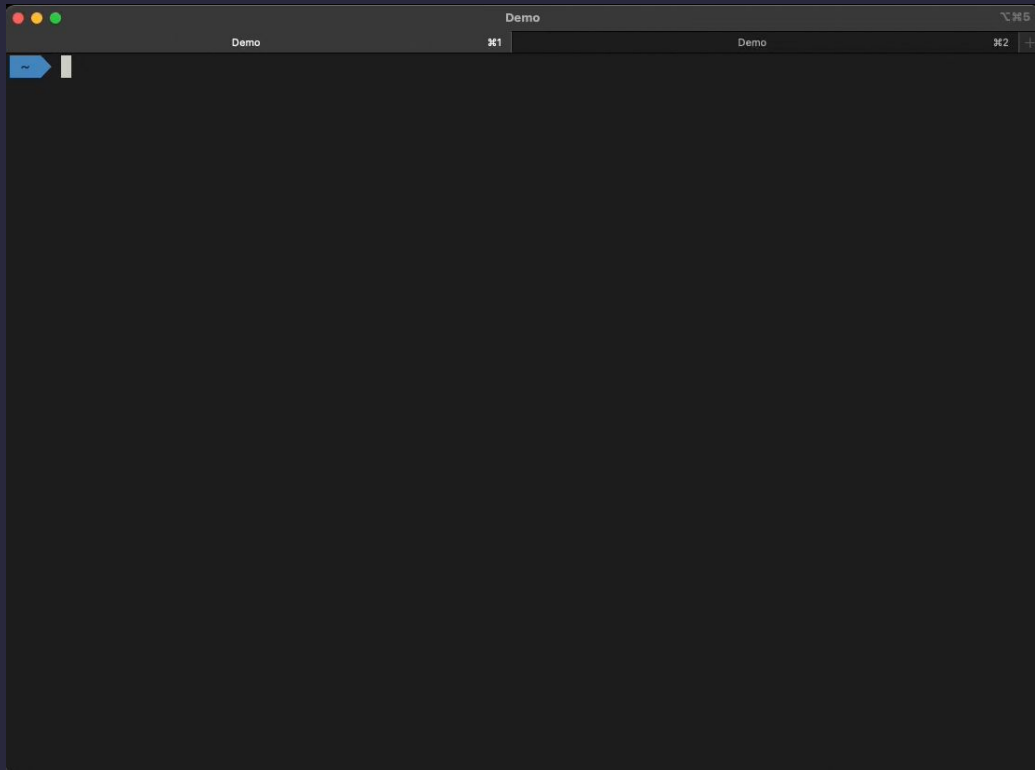
Ludus - Other features

- Automated template building from verified ISOs
- OPSEC safe testing mode
- Arbitrary networks
- Firewall rules
- Range sharing/collaboration
- Arbitrary DNS settings
- Arbitrary Ansible grouping
- Built-in Nexus Cache
- Fully documented REST API (OpenAPI 3.0)
- Detailed documentation (built into the server too!)
- More!

Ludus - Get Involved




- **./ludus-server**
- Join the Discord
- Write roles
- Share configurations
- Report bugs
- Add features



Contact/Questions



 @badsectorlabs || @__ar0d__

 badsectorlabs.com

ludus.cloud

github.com/badsectorlabs/sccm-http-looter

Thank You

- @1njected (Tomas Rzepka)
- Misconfiguration Manager (SpecterOps Team)
- @Synzack (Zach Stein)

