slideshare a Scribd company
Search
Upload Download free for 30 days Login

Hunting for Credentials Dumping in Windows Environment

Nov 18, 2017 • 22 likes • 16962 views

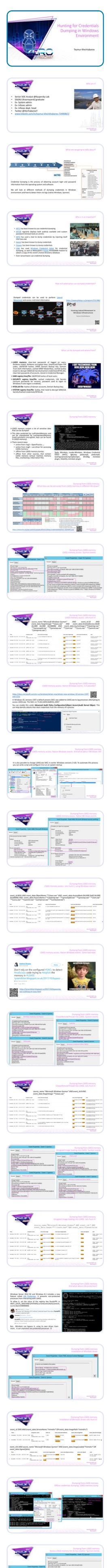
Teymur Kheirkhabarov Follow

My slides from Zero Nights 2017 talk - https://2017.zeronights.ru/report/hunting-for-credentials-dumping-in-windows-environment/

Read more

1 of 61

Download now
Download to read offline



Hunting for Credentials Dumping in Windows Environment

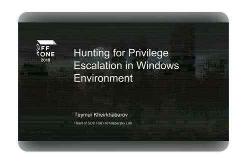
Teymur Kheirkhabarov

Who am I?

- Senior SOC Analyst @Kaspersky Lab
- SibSAU (Krasnoyarsk) graduate
- Ex- System admin
- Ex- Infosec admin
- Ex- Infosec dept. head
- Twitter @HeirhabarovT
- www.linkedin.com/in/teymur-kheirkhabarov-73490867/

www.zeronights.org
#zeronights

Recommended


Hunting for Privilege ...
Teymur Kheirkhabarov
12.6K views • 99 slides


Hunting Lateral Movement in ...
Sergey Soldatov
9.9K views • 52 slides

A Threat Hunter Himself
Sergey Soldatov
6.5K views • 31 slides

PHDays 2018 Threat Hunti...
Teymur Kheirkhabarov
8.2K views • 116 slides

Windows Forensic 101
Digit Oktavianto
745 views • 27 slides

Windows Threat Hunting
GIBIN JOHN
1.6K views • 17 slides

Pwning the Enterprise Wi...
Beau Bullock
6.4K views • 42 slides

Introduction to red team ...
Sunny Neo
1.6K views • 66 slides

Fantastic Red Team Attacks ...
Ross Wolf

Not a Security Boundary
Will Schroeder

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy
Third Parties

Storage Targeted Advertising Personalization Analytics

Manage Preferences
Accept All
Reject All

29
30
31
Most read
32
33
34

MITRE | Exfiltration
Command and Control

Tactic	Credential Access
Platform	Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10
Permissions Required	Administrator, SYSTEM
Data Sources	API monitoring, Process command-line parameters, Process monitoring, PowerShell logs
CAPEC ID	CAPEC-567

Credential dumping is the process of obtaining account login and password information from the operating system and software.

We will look at different methods of dumping credentials in Windows environment and how to detect them via logs (native Windows, Sysmon)

EPISODE 7 ZERO NIGHTS

Why is it so important?

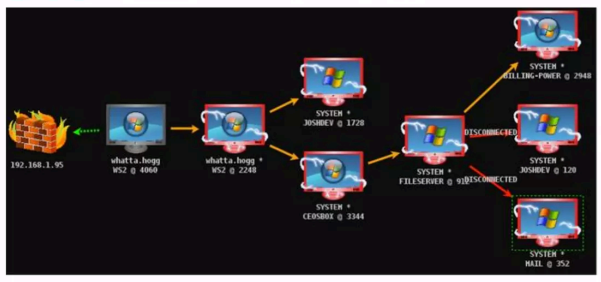
- APT1 has been known to use credential dumping
- APT28 regularly deploys both publicly available and custom password retrieval tools on victims
- APT3 has used a tool to dump credentials by injecting itself into lsass.exe
- Axiom has been known to dump credentials
- Cleaver has been known to dump credentials
- FIN6 has used Windows Credential Editor for credential dumping, as well as Metasploit's PsExec NTDSGRAB module to obtain a copy of the victim's Active Directory database
- Even ransomware use credential dumping

www.zeronights.org
#zeronights

EPISODE 7 ZERO NIGHTS

How will adversaries use dumped credentials?

Dumped credentials can be used to perform Lateral Movement and access restricted information



https://www.phdays.ru/program/231388/

www.zeronights.org
#zeronights

EPISODE 7 ZERO NIGHTS

What can be dumped and where from?

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy
Third Parties

Storage | Targeted Advertising | Personalization | Analytics

Teymur Kheirkhabarov

Catch Me If You Can: …
Will Schroeder

A Threat Hunter Himself
Teymur Kheirkhabarov

Windows

Secrets/Cached credentials/NTDS.dit.

www.zeronights.org
#zeronights

Dumping from LSASS memory

- LSASS memory contain a lot of sensitive data that can be dumped!
- This data protected by LsaProtectMemory and can be unprotected by LsaUnprotectMemory (used symmetric encryption, keys can be found in LSASS memory).
- There several ways:
  - online from ring3 – OpenProcess…;
  - online from ring0 – use driver for accessing LSASS memory;
  - offline from LSASS memory dumps;
  - offline from other sources, that contain LSASS memory (virtual machine memory files, crashdumps, hibernation file).

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 747368 (00000000:000b6768)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 07.11.2017 19:16:05
SID               : S-1-5-90-2
        msv :
         [00000003] Primary
         * Username : WIN-FJRMSLDJHD2$
         * Domain   : TEST
         * NTLM     : f9228579f8bdf37020d91b267f223d3e
         * SHA1     : c3a1b23634d3c0d51a1829980112977428261 4c1
        tspkg :
        wdigest :
         * Username : WIN-FJRMSLDJHD2$
         * Domain   : TEST
         * Password : 36 63 dc 18 c6 50 15 6d 84 25 6c c0 28 24 9c e7 f9 b5 52 6
8 79 0a ce 24 2b ba 36 e8 3b e3 e7 3a b1 97 63 f2 a7 27 b6 14 46 8e 6a f7 0d e7
f8 80 2d 3c e9 c1 06 97 fb 35 a3 0c 5d b4 8b 51 54 68 67 08 32 f7 79 00 82 24 40
 7a d6 1e 4a d4 dc 4e 30 48 5b 23 89 50 98 24 54 d5 04 a2 48 a9 b0 a9 b8 38 85 b
c 60 72 6d 90 83 42 45 d7 4a 93 50 97 5c aa 95 93 b6 8a 50 05 92 6c b6 c9 56 ef
17 78 14 c2 26 7b 54 e9 db 08 fc 4a e3 94 66 66 5f 4f a1 8b e1 df c1 f7 63 97 62
 23 f3 f0 b0 6e 43 40 21 59 e1 70 85 b0 ea fb 65 4c 67 5f b4 c4 15 50 a4 93 1d c
e c6 c6 78 42 01 1c 2f 40 8a 57 a3 f9 52 50 e2 ad 53 ec 48 45 fe 92 f3 2f dd 35
e5 0e 7d 8d 04 07 e0 91 fa df ec 68 03 f2 23 9f e6 90 2e 62 b5 36 34 c1 b1 01 0b
 43 ef 6e 62 6e cb ac
```

Tools: Mimikatz, Invoke-Mimikatz, Windows Credential Editor (WCE), fgdump, pwdump6, pwdumpX, taskmgr/procdump/sqldumper, WinDbg mimikatz plugin, Volatility mimikatz plugin

www.zeronights.org
#zeronights

Dumping from LSASS memory
What data can be extracted from LSASS memory in different Windows?

	Primary			CredentialKeys				tspkg		wdigest		kerberos				livessp	ssp	dpapi	credman 6
	LM	NTLM	SHA1	NTLM	SHA1	Root	DPAPI	off	on	off	on	pass 1	PIN 4	tickets	eKeys				
Windows XP/2003																			
Local Account								2											
Domain Account								2					5						
Windows Vista/2008 & 7/2008r2																			
Local Account																			
Domain Account																			
Windows 8/2012																			
Microsoft Account																			
Local Account																			
Domain Account																			
Windows 8.1/2012r2																			
Microsoft Account									3		3								
Local Account									3		3	7							
Domain Account									3		3								
Domain Protected Users									3		3								

	Windows 8.1 vault for user's authentication				
	PIN		Picture		Fingerprint
	code	pass	gestures	pass	pass
Microsoft Account					
Local Account					

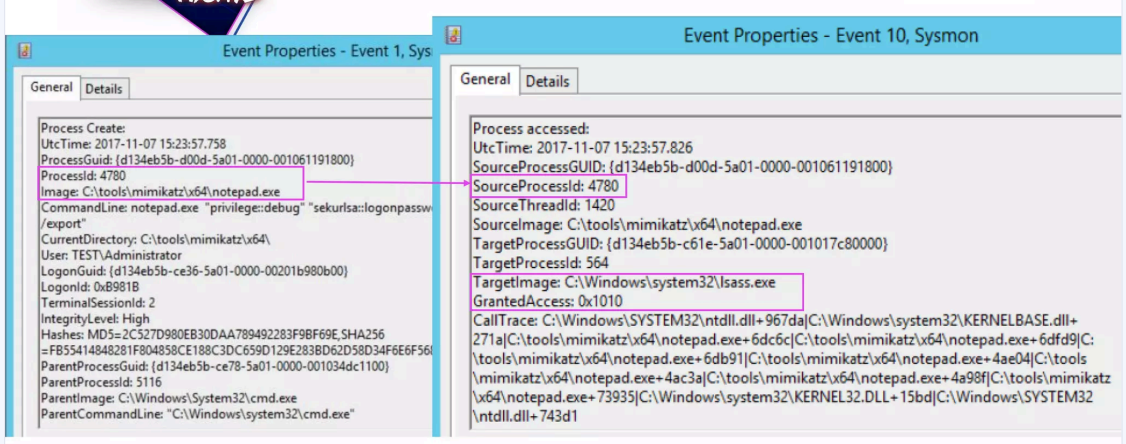
not applicable
data in memory
no data in memory

1. can need an unlock on NT5, not available with smartcard
2. tspkg is not installed by default on XP, not available on 2003
3. tspkg is off by default (but needed for SSO with remoteapps/ts), wdigest too
   http://technet.microsoft.com/library/dn303404.aspx
4. PIN code when SmartCard used for native Logon
5. PIN code is NOT encrypted in memory (XP/2003)
6. When accessed/used by owner
7. When local admin, UAC and after unlock

https://adsecurity.org/wp-content/uploads/2014/11/Delpy-CredentialDataChart-1024x441.png

www.zeronights.org
#zeronights

Dumping from LSASS memory
LSASS memory access. Sysmon events



www.zeronights.org
#zeronights

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy
Third Parties

Storage Targeted Advertising Personalization Analytics

LSASS memory access. Lets hunt it!

source_name:"Microsoft-Windows-Sysmon" AND event_id:10 AND event_data.TargetImage:"\\lsass.exe" AND -event_data.GrantedAccess:(0x40 0x1400 0x1000 0x100000) AND -event_data.SourceImage:("*\\taskmgr.exe" "*\\procexp64.exe" "*\\procexp.exe" "*\\lsm.exe" "*\\csrss.exe" "*\\wininit.exe" "\\wmiprvse.exe")*

Time	computer_name	event_data.SourceImage	event_data.TargetImage	event_data.GrantedAccess	task
November 8th 2017, 02:34:02.502	WIN-FJRNSLDJHD2.test.local	C:\tools\PwDump6\servpw64.exe	C:\Windows\system32\lsass.exe	0x1f3fff	Process accessed (rule: ProcessAccess)
November 8th 2017, 02:11:21.187	pc0002.test.local	C:\Windows\cioyj.exe	C:\Windows\system32\lsass.exe	0x1f1fff	Process accessed (rule: ProcessAccess)
November 8th 2017, 02:06:38.704	pc0002.test.local	C:\Windows\vdcpqepjk.exe	C:\Windows\system32\lsass.exe	0x1f1fff	Process accessed (rule: ProcessAccess)
November 8th 2017, 01:52:52.710	pc0002.test.local	C:\Windows\ueoimxq.exe	C:\Windows\system32\lsass.exe	0x1f1fff	Process accessed (rule: ProcessAccess)
November 7th 2017, 23:17:12.860	pc0002.test.local	C:\tools\mimikatz\Win32\mimikatz.exe	C:\Windows\system32\lsass.exe	0x1038	Process accessed (rule: ProcessAccess)
November 7th 2017, 23:17:12.859	pc0002.test.local	C:\tools\mimikatz\Win32\mimikatz.exe	C:\Windows\system32\lsass.exe	0x1010	Process accessed (rule: ProcessAccess)
November 7th 2017, 20:33:01.050	WIN-FJRNSLDJHD2.test.local	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe	C:\Windows\system32\lsass.exe	0x143a	Process accessed (rule: ProcessAccess)
November 7th 2017, 20:17:38.435	WIN-FJRNSLDJHD2.test.local	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\system32\lsass.exe	0x143a	Process accessed (rule: ProcessAccess)

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

More Related Content

What's hot (20)

Fantastic Red Team Attacks and How to Find Them
Ross Wolf • 1.1K views

Not a Security Boundary
Will Schroeder • 4.1K views

Detection Rules Coverage
Sunny Neo • 1.3K views

Kheirkhabarov24052017_phdays7

Catch Me If You Can: PowerShell Red vs Blue

A Threat Hunter H

Similar to Hunting for Credentials Dumping in Windows Environment (20)

Mitre Attack - Credential Dumping - updated.pptx

Hta w22

Memory Forensics: Defeating Disk Encryption...

Kush wadhwa _mining_digital_evidence...

Living off the land and fileless attack techniques

Mem forensic

Recently uploaded (20)

2024 PHPCon - Symfony background processing

Data in Motion Tour 2024 Riyadh, Saudi Arabia

Digitocracy without Borders: the unifying and ...

Top 10 Reasons to Use ONEMONITAR Call Tracker ...

SPSS Statistics - Customising Toolbars.pptx

Airline Ticket Boo System, Flight Tic

Related Books

Free with a 30 day trial from Everand

View All

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics

Audiobook
Linux
Ryan Turner
★★★★☆ 4 / 5

Audiobook
The Ultimate Kali Linux Bo…
Glen D. Singh
★★★★★ 5 / 5

Audiobook
Hacking Network…
Hans Weber
★★★★★ 5 / 5

Audiobook
Linux for Beginners: 3…
ATTILA KOVACS
★★★★☆ 4 / 5

Audiobook
Hacking: A Quick and…
Hans Weber
★★★☆☆ 3 / 5

Audiobook
Cybersecurity for Beginners:…
Kevin Clark
☆☆☆☆☆ 0 / 5

Audiobook
Hacking: The Ultimate…
Kevin Clark
☆☆☆☆☆ 0 / 5

Audiobook
Cybersecurity, Cryptography…
HUGO HOFFMAN
★★★★★ 5 / 5

Hunting for Credentials Dumping in Windows Environment

1. **Hunting for Credentials Dumping** in Windows Environment Teymur Kheirhabarov
2. **Who am I?** • Senior SOC Analyst @Kaspersky Lab • SibSAU (Krasnoyarsk) graduate • Ex- System admin • Ex- Infosec admin • Ex- Infosec dept. head • Twitter @HeirhabarovT • www.linkedin.com/in/teymur-kheirkhabarov-73490867/
3. **What are we** going to talks about? Credential dumping is the process of obtaining account login and password information from the operating system and software. We will look at different methods of dumping credentials in Windows environment and how to detect them via logs (native Windows, Sysmon)
4. **Why is it** so important? • APT1 has been known to use credential dumping • APT28 regularly deploys both publicly available and custom password retrieval tools on victims • APT3 has used a tool to dump credentials by injecting itself into lsass.exe • Axiom has been known to dump credentials • Cleaver has been known to dump credentials • FIN6 has used Windows Credential Editor for credential dumping, as well as Metasploit's PsExec NTDSGRAB module to obtain a copy of the victim's Active Directory database • Even ransomware use credential dumping
5. **How will adversaries** use dumped credentials? Dumped credentials can be used to perform Lateral Movement and access restricted information https://www.phdays.ru/program/231388/
6. **□LSASS memory: clear-text** passwords of logged on users, Kerberos tickets, Kerberos encryption keys, SmartCard/Token PIN codes, LM/NTLM hashes, DPAPI Domain Backup Key, Domain Trust Auth Information, cached DPAPI MasterKeys, cached SysKey (need to decrypt SAM/LSA Secrets/Cached credentials/NTDS.dit), clear-text passwords of accounts, stored in Credential Manager; □SAM registry hive/file: LM/NTLM hashes of local users; □SECURITY registry hive/file: cached credentials, LSA Secrets (account passwords for services, password used to logon to Windows if auto-logon is enabled); □NTDS.dit file: hashes of domain accounts, Domain Backup Key; □SYSTEM registry hive/file: SysKey, that need to decrypt SAM/LSA Secrets/Cached credentials/NTDS.dit. What can be dumped and where from?
7. **□LSASS memory contain** a lot of sensitive data that can be dumped! □This data protected by LsaProtectMemory and can be unprotected by LsaUnprotectMemory (used symmetric encryption, keys can be found in LSASS memory). □There several ways: • online from ring3 – OpenProcess…; • online from ring0 – use driver for accessing LSASS memory; • offline from LSASS memory dumps; • offline from other sources, that contain LSASS memory (virtual machine memory files, crashdumps, hibernation file). Dumping from LSASS memory Tools: Mimikatz, Invoke-Mimikatz, Windows Credential Editor (WCE), fgdump, pwdump6, pwdumpX, taskmgr/procdump/sqldumper, WinDbg mimikatz plugin, Volatility mimikatz plugin
8. **Dumping from LSASS** memory What data can be extracted from LSASS memory in different Windows? https://adsecurity.org/wp-content/uploads/2014/11/Delpy-CredentialDataChart-1024x441.png
9. **Dumping from LSASS** memory LSASS memory access. Sysmon events
10. **Dumping from LSASS** memory LSASS memory access. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:10 AND event_data.TargetImage:"*lsass.exe" AND -event_data.GrantedAccess:(0x40 0x1400 0x1000 0x100000) AND -event_data.SourceImage:("*taskmgr.exe" "*procexp64.exe" "*procexp.exe" "*lsm.exe" "*csrss.exe" "*wininit.exe" "wmiprvse.exe")
11. **Dumping from LSASS** memory LSASS memory access. Native Windows events. Is it possible? In Windows 10, versions 1507 a default process SACL was added to LSASS.exe to log processes attempting to access LSASS.exe. The SACL is L"S:(AU;SAFA;0x0010;;;WD)". You can enable this under Advanced Audit Policy ConfigurationObject AccessAudit Kernel Object. This can help identify attacks that steal credentials from the memory of a process https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1507- and-1511
12. **Dumping from LSASS** memory LSASS memory access. Native Windows events. And what about <Windows 10? It is also possible to change LSASS.exe SACL in earlier Windows versions (<10). To automate this process you can write script and configure it to run on system startup
13. **Dumping from LSASS** memory LSASS memory access. Native Windows events
14. **Dumping from LSASS** memory LSASS memory access. Lets hunt it, using Windows events! event_id:4656 AND event_data.ObjectName:"*lsass.exe" AND -event_data.AccessMask:(0x1400 0x40 0x1000 0x100000) AND -event_data.ProcessName:("*taskmgr.exe" "*procexp64.exe" "*procexp.exe" "*lsm.exe" "*csrss.exe" "*wininit.exe" "wmiprvse.exe" "*vmtoolsd.exe")
15. **Dumping from LSASS** memory LSASS memory access. Native Windows events. Some bad news https://tyranidslair.blogspot.ru/2017/10/bypassing- sacl-auditing-on-lsass.html
16. **Dumping from LSASS** memory CreateRemoteThread into LSASS. Sysmon eventsMimikatz (lsadump::lsa /inject) lsadump PWDump6 Windows Credential Editor (WCE)
17. **Dumping from LSASS** memory CreateRemoteThread into LSASS. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:8 AND event_data.TargetImage:"*lsass.exe"
18. **Dumping from LSASS** memory Unsigned image loading into LSASS. Sysmon eventsPWDump6 (x86) PWDump6 (x64) PWDumpX Windows Credential Editor (WCE)
19. **Dumping from LSASS** memory Unsigned image loading into LSASS. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:7 AND event_data.Image:"*lsass.exe" AND event_data.Signed:false
20. **Dumping from LSASS** memory And what about LSA protection? Windows Server 2012 R2 and Windows 8.1 includes a new feature called LSA Protection. It prevents non-protected processes from interacting with LSASS. To allow it, set the value of the registry key RunAsPPL in HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControl Lsa to dword:00000001 But… Mimikatz can bypass it, using its own driver. Even more… It can unprotect any protected processes □
21. **Dumping from LSASS** memory Installation of Mimikatz driver
22. **Dumping from LSASS** memory Installation of Mimikatz driver. Lets hunt it! event_id:7045 AND (event_data.ServiceName:*mimidrv* OR event_data.ImagePath:*mimidrv*) event_id:6 AND source_name:"Microsoft-Windows-Sysmon" AND (event_data.ImageLoaded:*mimidrv* OR event_data.Signed:false)
23. **Dumping from LSASS** memory Offline credentials dumping. LSASS memory dump SqlDumper Procdump Extract credentials from lsass memory dump
24. **Dumping from LSASS** memory Access LSASS memory for dump creation. Sysmon events
25. **Dumping from LSASS** memory Access LSASS memory for dump creation. Lets hunt it source_name:"Microsoft-Windows-Sysmon" AND event_id:10 AND event_data.TargetImage:"*lsass.exe" AND event_data.CallTrace:*dbghelp*
26. **Dumping from LSASS** memory LSASS memory dump file creation. Sysmon events Procdump create lsass memory dump file Taskmgr create lsass memory dump file Powershell create lsass memory dump file SqlDumper create lsass memory dump file
27. **Dumping from LSASS** memory LSASS memory dump file creation. Lets hunt it source_name:"Microsoft-Windows-Sysmon" AND event_id:11 AND event_data.TargetFilename:*lsass* AND event_data.TargetFilename:*dmp
28. **Dumping from LSASS** memory Offline credentials dumping. Other sources of LSASS memory It is also possible to extract credentials from other sources, containing lsass memory: • Virtual machines memory files (.vmem…); • Hibernation files (hiberfil.sys) ; • Crashdumps (.dmp, C:WindowsMinidump). Tools: Mimkatz WinDbg extension, Volatility Mimikatz plugin
29. **Dumping from LSASS** memory Offline credentials dumping. Other sources of LSASS memory
30. **Dumping from LSASS** memory Offline credentials dumping. Other sources of LSASS memory. Copying hiberfil/crashdumps via admin shares event_id:5145 AND event_data.RelativeTargetName:(*lsass* "*windowsminidump*" *hiberfil* *sqldmpr* "*sam*" "*ntds.dit" "*security*")
31. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Offline** – grab SAM/SYSTEM/SECURITY/NTDS.dit from compromised host and process it using special tools. Online – run special tool directly on compromised host (this tool will do all necessary work itself)
32. **Windows allows programs** to have direct access to logical volumes. Programs with direct access may read and write files directly from the drive by analyzing file system data structures. This technique bypasses Windows file access controls as well as file system monitoring tools. Tools: Pwdump7, Invoke-NinjaCopy, Samex Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing via direct access to logical volume
33. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via direct access to logical volume. Sysmon events. Invoke-NinjaCopy (local) PwDump7 Samex Invoke-NinjaCopy (remote)
34. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via direct access to logical volume. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND -event_data.Device:*Floppy* AND event_id:9 -event_data.Image:("*WmiPrvSE.exe" "*sdiagnhost.exe" "*SearchIndexer.exe" "*csrss.exe" "*Defrag.exe" "*smss.exe" "System" "*VSSVC.exe" "*CompatTelRunner.exe" "*wininit.exe" "*autochk.exe" "*taskhost.exe" "*dfsrs.exe" "*vds.exe" "*lsass.exe")
35. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via shadow copies. VSSAdmin Shadow Copy (also known as Volume Snapshot Service, Volume Shadow Copy Service or VSS) is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use. So, it can be used to grab SAM/SECURITY/NTDS.dit files.
36. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via shadow copies. VSSAdmin. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND *vssadmin* AND event_data.Image:"*vssadmin.exe" AND event_data.CommandLine:*shadow* AND event_data.CommandLine:(*list* *create* *delete*) event_id:466 AND *vssadmin* AND event_data.NewProcessName:"*vssadmin.exe" AND event_data.CommandLine:*shadow* AND event_data.CommandLine:(*list* *create* *delete*)
37. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via shadow copies. ntdsutil Ntdsutil.exe is a command- line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS). It can be used to create backup of NTDS database, using shadow copies mechanism.
38. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via shadow copies. ntdsutil. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.Image:"*ntdsutil.exe" AND event_data.CommandLine:*ntds* AND event_data.CommandLine:*create* AND event_data.CommandLine:*full* event_id:4688 AND event_data.NewProcessName:"*ntdsutil.exe" AND event_data.CommandLine:*ntds* AND event_data.CommandLine:*create* AND event_data.CommandLine:*full*
39. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via shadow copies. WMI. Lets hunt it! WMI can also be used for shadow copies creation. This operation can be done using wmic, powershell or programmatically via COM
40. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Grabbing** via shadow copies. WMI. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.Image:("*powershell.exe" "*wmic.exe") AND event_data.CommandLine:(*shadowcopy*) AND event_data.CommandLine:(*create*) event_id:4688 AND event_data.NewProcessName:("*powershell.exe" "*wmic.exe") AND event_data.CommandLine:(*shadowcopy*) AND event_data.CommandLine:(*create*)
41. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Shadow** copies. Copying SAM/SECURITY/NTDS.dit files. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:1 AND event_data.CommandLine:("*windowsntdsntds.dit" "*system32configsam" "*system32configsecurity" "*system32configsystem") event_id:4688 AND event_data.CommandLine:("*windowsntdsntds.dit" "*system32configsam" "*system32configsecurity" "*system32configsystem")
42. **Dumping from SAM/SYSTEM/SECURITY/NTDS.dit Shadow** copies. Create symlink to shadow copies storage. Lets hunt it! source_name:"Microsoft-Windows-Sysmon“ AND event_id:1 AND event_data.CommandLine:*mklink* AND event_data.CommandLine:*HarddiskVolumeShadowCopy* event_id:4688 AND event_data.CommandLine:*mklink* AND event_data.CommandLine:*HarddiskVolumeShadowCopy*
43. **Dumping from SAM/SYSTEM/SECURITY Grabbing** via registry. Using reg tool
44. **Dumping from SAM/SYSTEM/SECURITY Grabbing** via registry. Using reg tool. Lets hunt it! event_id:1 AND event_data.CommandLine:*reg* AND event_data.CommandLine:*save* AND event_data.CommandLine:("hklmsam" "hklmsystem" "hklmsecurity" "hkey_local_machinesam" "hkey_local_machinesystem" "hkey_local_machinesecurity")
45. **Dumping from SAM/SYSTEM/SECURITY Grabbing** via remote registry. Lets hunt it! event_id:5145 AND event_data.RelativeTargetName:winreg AND -event_data.IpAddress:(192.168.7.9 192.168.7.19) MJP addresses of admin workstations Account and IP used

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy
Third Parties

Storage Targeted Advertising Personalization Analytics

lsremora64.dll, test.pwd - fgdump fgexec/*fgexec.exe Cachedump/*cachedump.exe Cachedump/*cachedump64.exe service name like GUID/*servpw.exe service name like GUID/*servpw64.exe fgexec.exe, pwdump.exe, pstgdump.exe, lsremora.dll, lsremora64.dll, cachedump.exe, cachedump64.exe, servpw64.exe, servpw.exe, test.pwd, *.pwdump, *.fgdump-log -

53. **Credentials dumping tools** artefacts Services. Windows events PWDumpX PWDump6 Windows Credentials Editor (WCE) Mimikatz RPC service

54. **Credentials dumping tools** artefacts Services. Lets hunt it! event_id:7045 AND (event_data.ServiceName:(fgexec cachedump *mimikatz* *mimidrv* WCESERVICE *pwdump*) OR event_data.ImagePath:(*fgexec* *dumpsvc* *mimidrv* *cachedump* *servpw* *gsecdump* *pwdump*) OR event_data.ImagePath.raw:/(.*.*|.*[{]?[0-9A-Fa-f]{8}-[0-9A-Fa-f]{4}-[0-9A-Fa- f]{4}-[0-9A-Fa-f]{4}-[0-9A-Fa-f]{12}[}]?.(exe|scr|cpl|bat|js|cmd|vbs).*)/)

55. **Credentials dumping tools** artefacts Dropped files. Sysmon events Mimikatz Windows Credentials Editor (WCE) Windows Credentials Editor (WCE) PWDumpX

56. **event_id:11 AND event_data.TargetFilename:("*test.pwd"** "*lsremora.dll" "*lsremora64.dll" "*fgexec.exe" *pwdump* *kirbi "*wce_ccache" "*wce_krbtkts" "*wceaux.dll" *PwHashes* "*SAM.out" "*SECURITY.out" "*SYSTEM.out" "*NTDS.out" "*DumpExt.dll" "*DumpSvc.exe" "*cachedump64.exe" "*cachedump.exe" "*pstgdump.exe" "*servpw64.exe" "*servpw.exe" "*pwdump.exe" "*fgdump-log*") Credentials dumping tools artefacts Dropped files. Lets hunt it!

57. **Credentials dumping tools** artefacts Named pipes. Sysmon events Windows Credentials Editor (WCE) Cachedump LSADump

58. **Credentials dumping tools** artefacts Named pipes. Lets hunt it! source_name:"Microsoft-Windows-Sysmon" AND event_id:17 AND event_data.PipeName:(*lsadump* *cachedump* *WCEServicePipe*)

59. **Credentials dumping tools** artefacts Mimikatz command line event_id:1 AND (event_data.CommandLine:(*DumpCreds* *invoke-mimikatz*) OR (event_data.CommandLine:(*rpc* *token* *crypto* *dpapi* *sekurlsa* *kerberos* *lsadump* *privilege* *process*) AND event_data.CommandLine.raw:*::*)) event_id:4688 AND (event_data.CommandLine:(*DumpCreds* *invoke-mimikatz*) OR (event_data.CommandLine:(*rpc* *token* *crypto* *dpapi* *sekurlsa* *kerberos* *lsadump* *privilege* *process*) AND event_data.CommandLine.raw:*::*))

60. **Hunting for credentials** dumping by AV detects Kaspersky Microsoft Symantec TrendMicro mimikatz Exploit.Win32.Palsas.vyl HackTool.Win32.Mimikatz.gen HackTool:Win32/Mimikatz Hacktool.Mimikatz HKTL_MIMIKATZ64.A HKTL_MIMIKATZ Gsecdump PSWTool.Win64.Gsecdmp.e HackTool:Win32/Gsecdump Hacktool.PTHToolkit HKTL_PWDUMP Fgdump PSWTool.Win32.PWDump.f HackTool:Win32/Fgdump Pwdump HKTL_FGDUMP WCE HackTool.Win32.WinCred.e HackTool:Win32/Wincred.G SecurityRisk.WinCredEd HKTL_WINCRED PWDumpX HackTool.Win32.PWDump.a HackTool:Win32/PWDumpX - HKTL_PWDUMP.SM Cachedump PSWTool.Win32.CacheDump.a HackTool:Win32/Cachedump Trojan.Gen.NPE HKTL_PWDUMPBD Pwdump6 PSWTool.Win32.PWDump.lv HackTool:Win64/PWDump HackTool:Win32/PWDump.A Pwdump HKTL_PWDUMP pwdump7 PSWTool.Win32.PWDump.bve HackTool:Win32/PWDump.I Pwdump HKTL_PWDUMP lsadump HackTool.Win32.Lsadump.a - Hacktool.LSADump - samex HackTool.Win32.Samer.a - - -

61. **The End**

About Support Terms Privacy Copyright Cookie Preferences Do not sell or share my personal information Everand

© 2024 SlideShare from Scribd

We and our 10 partners store and access information on your device for personalized ads and content. Personal data may be processed, such as cookie identifiers, unique device identifiers, and browser information. Third parties may store and access information on your device and process this personal data. You may change or withdraw your preferences by clicking on the cookie icon or link; however, as a consequence, you may not see relevant ads or personalized content.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

Cookie Policy

Third Parties

Storage Targeted Advertising Personalization Analytics