Hunting for Credentials Dumping in Windows Environment

• 22 likes • 16,951 views

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

Read more

Teymur Kheirkhabarov

More Related Content

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) IP addresses of admin workstations Account and IP used to access Remote Registry Remote registry service pipe

46. **Dumping from NTDS.dit** remotely DCSync DCSync is a variation on credential dumping which can be used to acquire sensitive information from a domain controller. The action works by simulating a domain controller replication process from a remote domain controller. Any member of Administrators, Domain Admins, or Enterprise Admins as well as Domain Controller computer accounts are able to run DCSync to pull to pull credential data. Tools: Mimikatz, secretsdump.py from Impacket How it works: • discovers Domain Controller in the specified domain name. • requests the Domain Controller replicate the user; credentials via GetNCChanges (leveraging Directory Replication Service (DRS) Remote Protocol).

47. **Dumping from NTDS.dit** remotely DCSync. Windows events DS-Replication-Get-ChangesDS-Replication-Get-Changes-All

48. **Dumping from NTDS.dit** remotely DCSync using Domain Controller account DC account

49. **Dumping from NTDS.dit** remotely DCSync. Lets hunt it! event_id:4624 AND event_data.TargetLogonId:(0x7483c4 0x6b0b8f) AND - event_data.IpAddress:(“172.16.205.140““172.16.205.141“) Our DCs event_id:4662 AND event_data.Properties:("{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}" "{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}") AND computer_name:("WIN- FJRNSLDJHD2.test.local" "dc2.test.local") DCs

50. **Dumping from NTDS.dit** remotely NetSync Based on [MS-NRPC] - Netlogon Remote Protocol Tools: Mimikatz

51. **Dumping from NTDS.dit** remotely NetSync. Windows events

52. **Credentials dumping tools** artefacts Services Dropped files Pipes Mimikatz mimikatz service (mimikatzsvc)/*path to mimikatz binary mimikatz driver (mimidrv)/*mimidrv.sys *.kirbi - wce WCESERVICE/*service image file like GUID wce_ccache, wce_krbtkts, wceaux.dll WCEServicePipe samex - SAM.out, NTDS.out, SYSTEM.out - PWDumpX PWDumpX Service / *DumpSvc.exe DumpExt.dll, DumpSvc.exe, *- PwHashes.txt - cachedump - - cachedumppipe lsadump - - lsadump* pwdump6 service name like GUID

lsremora.dll, 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**