ID: 679413
Sample Name: 1.msi
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:21:10
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

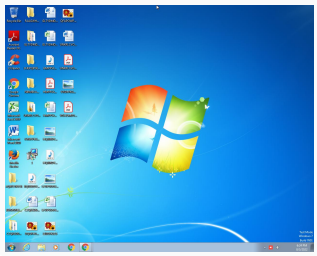
Windows Analysis Report

1.msi

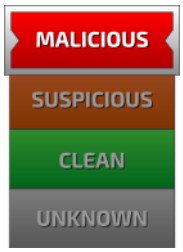
Overview

General Information

Sample Name:	1.msi
Analysis ID:	679413
MD5:	6cf5ad7a7d1b7b..
SHA1:	b06a03adc550ea..
SHA256:	fb9f0bf2b71bf57…
Tags:	msi
Infos:	



Detection

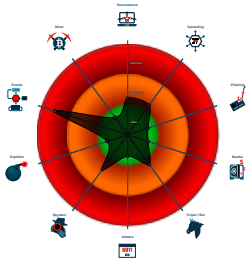


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Uses netsh to modify the Windows …
- Hides user accounts
- Creates an undocumented autostart…
- Hides that the sample has been dow…
- Modifies the windows firewall
- Tries to disable installed Antivirus / …
- Queries the volume information (nam…

Classification



Process Tree

- **System is w7x64**
- msiexec.exe (PID: 2996 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\1.msi" MD5: AC2E7152124CEED36846BD1B6592A00F)
- msiexec.exe (PID: 1184 cmdline: C:\Windows\system32\msiexec.exe /V MD5: AC2E7152124CEED36846BD1B6592A00F)
  - msiexec.exe (PID: 2876 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 6381DE7DB6BAADD41D0E24C26E59EDFC MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
    - cmd.exe (PID: 2332 cmdline: C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files" MD5: AD7B9C14083B52BC532FBA5948342B98)
  - msiexec.exe (PID: 1704 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 22388C515E15FC158EA4B11229C0F8D9 E Global\MSI0000 MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
    - icacls.exe (PID: 1820 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\." /SETINTEGRITYLEVEL (CI)(OI)HIGH MD5: 1542A92D5C6F7E1E80613F3466C9CE7F)
    - expand.exe (PID: 672 cmdline: "C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files MD5: 659CED6D7BDA047BCC6048384231DB9F)
    - install.exe (PID: 2440 cmdline: "C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe" MD5: 8C42AB81F90EE0592F7A709F0F7E320B)
      - cmd.exe (PID: 1404 cmdline: cmd /c c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent MD5: AD7B9C14083B52BC532FBA5948342B98)
        - anydesk.exe (PID: 2640 cmdline: c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent MD5: 1BC5890C9E7BF54B7712E344B0AF9D04)
      - cmd.exe (PID: 2544 cmdline: cmd /c echo 31121985west|c:\programdata\anydesk\anydesk.exe --set-password MD5: AD7B9C14083B52BC532FBA5948342B98)
        - cmd.exe (PID: 2548 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo 31121985west" MD5: AD7B9C14083B52BC532FBA5948342B98)
        - AnyDesk.exe (PID: 2856 cmdline: c:\programdata\anydesk\anydesk.exe --set-password MD5: 1BC5890C9E7BF54B7712E344B0AF9D04)
      - AnyDesk.exe (PID: 2120 cmdline: "c:\programdata\anydesk\anydesk.exe" --get-id MD5: 1BC5890C9E7BF54B7712E344B0AF9D04)
      - netsh.exe (PID: 2744 cmdline: netsh advfirewall firewall add rule name="RDP" dir=in protocol=TCP localport=3389 action=allow MD5: 784A50A6A09C25F011C3143DDD68E729)
    - icacls.exe (PID: 1004 cmdline: "C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\." /SETINTEGRITYLEVEL (CI)(OI)LOW MD5: 1542A92D5C6F7E1E80613F3466C9CE7F)
- VSSVC.exe (PID: 1232 cmdline: C:\Windows\system32\vssvc.exe MD5: B60BA0BC31B0CB414593E169F6F21CC2)
- svchost.exe (PID: 2224 cmdline: C:\Windows\System32\svchost.exe -k swprv MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- rdpdr.sys (PID: 4 cmdline: MD5: 1B6163C503398B23FF8B939C67747683)
- tdtcp.sys (PID: 4 cmdline: MD5: 51C5ECEB1CDEE2468A1748BE550CFBC8)
- tssecsrv.sys (PID: 4 cmdline: MD5: 19BEDA57F3E0A06B8D5EB6D619BD5624)
- rdpwd.sys (PID: 4 cmdline: MD5: FE571E088C2D83619D2D48D4E961BF41)
- AnyDesk.exe (PID: 2556 cmdline: "C:\ProgramData\AnyDesk\AnyDesk.exe" --service MD5: 1BC5890C9E7BF54B7712E344B0AF9D04)
- AnyDesk.exe (PID: 2336 cmdline: "C:\ProgramData\AnyDesk\AnyDesk.exe" --control MD5: 1BC5890C9E7BF54B7712E344B0AF9D04)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Data Obfuscation

Detected unpacking (changes PE section rights)

Boot Survival

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Hides user accounts

Hides that the sample has been downloaded from the Internet (zone.identifier)

Lowering of HIPS / PFW / Operating System Security Settings

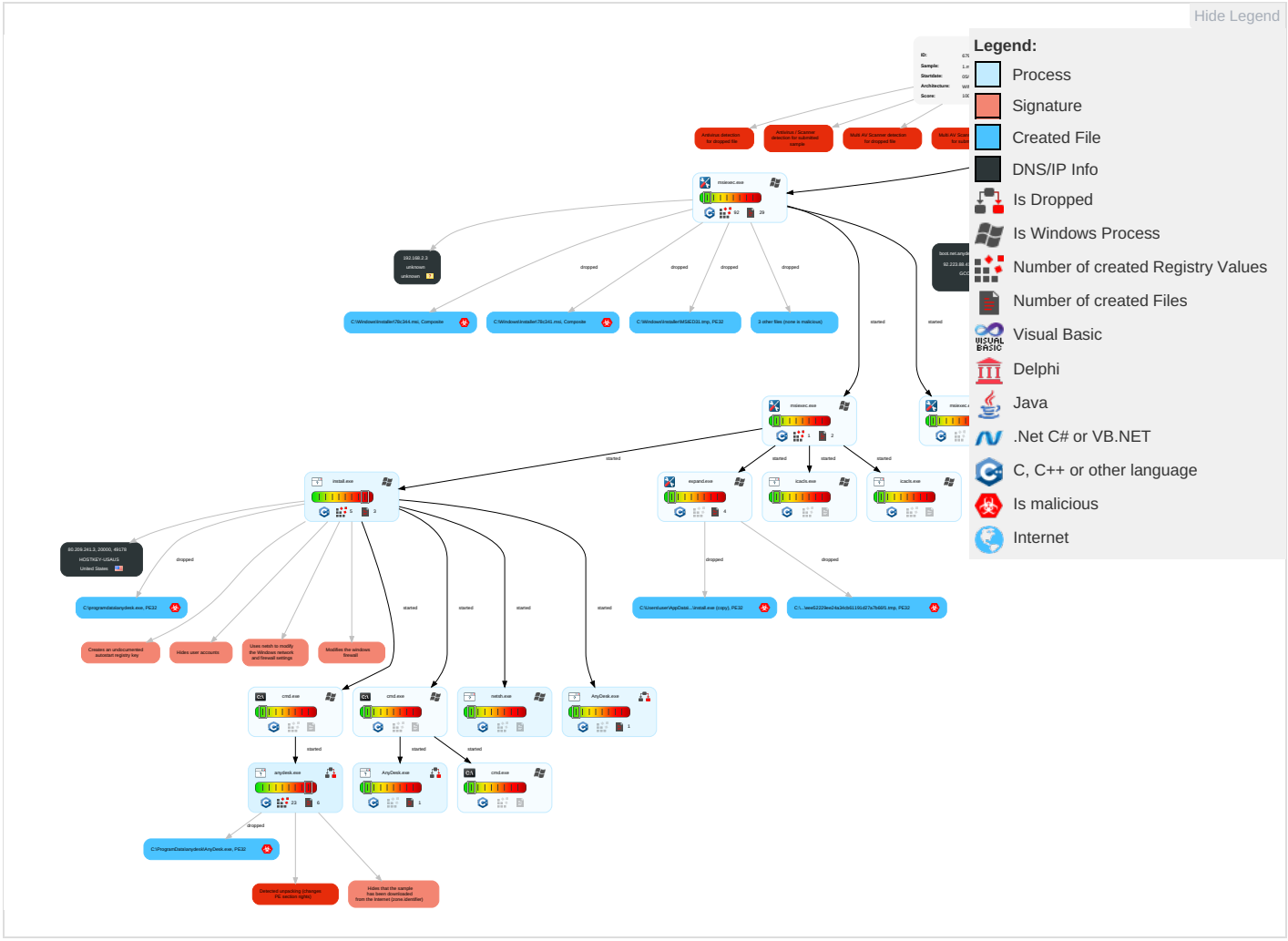
Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 Native API	1 LSASS Driver	1 LSASS Driver	2 1 1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	1 Replication Through Removable Media	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Command and Scripting Interpreter	1 Image File Execution Options Injection	1 Image File Execution Options Injection	1 Obfuscated Files or Information	LSASS Memory	1 1 Peripheral Device Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	2 Windows Service	1 Access Token Manipulation	1 1 Software Packing	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	1 Registry Run Keys / Startup Folder	2 Windows Service	1 File Deletion	NTDS	1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	1 Services File Permissions Weakness	1 1 Process Injection	2 1 Masquerading	LSA Secrets	1 3 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Registry Run Keys / Startup Folder	4 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	1 Services File Permissions Weakness	1 Access Token Manipulation	DCSync	4 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Process Injection	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Users	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Services File Permissions Weakness	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

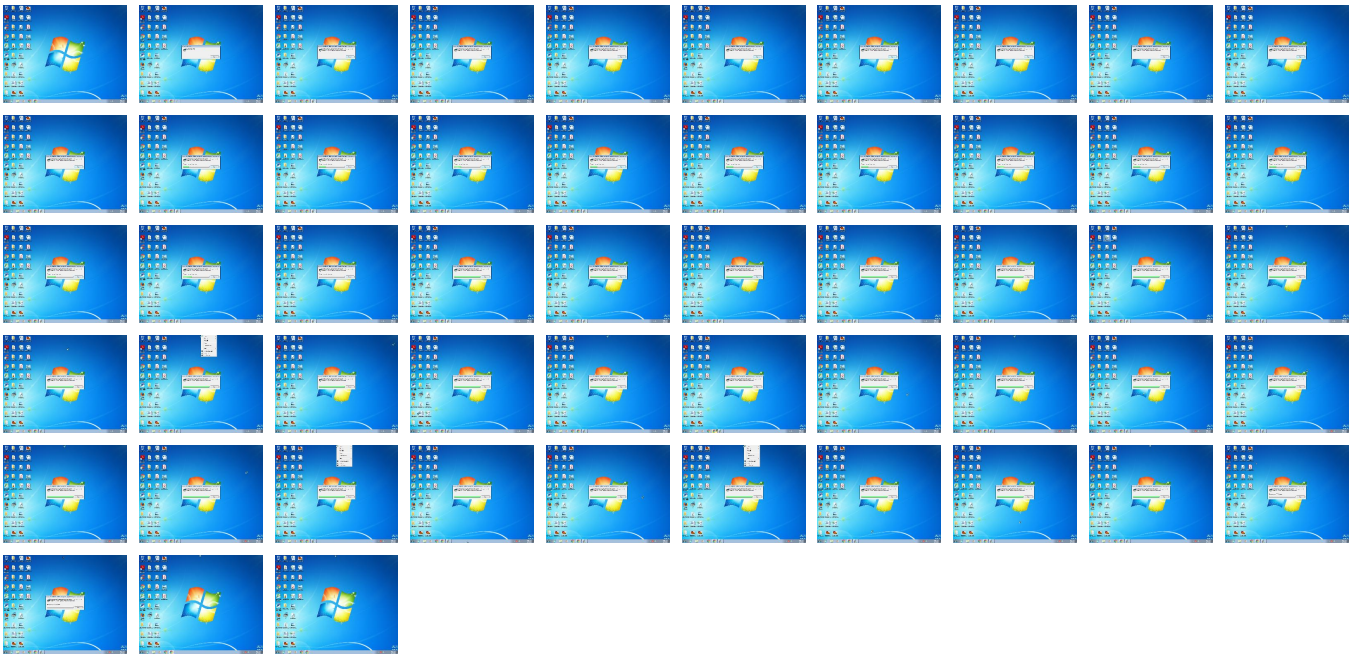
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1.msi	48%	Virustotal		Browse
1.msi	30%	ReversingLabs	Win32.Backdoor.Finfish	
1.msi	100%	Avira	BDS/Finfish.ujrxw	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Installer\78c344.msi	100%	Avira	BDS/Finfish.ujrxw	
C:\Windows\Installer\78c341.msi	100%	Avira	BDS/Finfish.ujrxw	
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\dpx.tmp\eee52229ee24a34cb61191d27a7b66f1.tmp	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\dpx.tmp\eee52229ee24a34cb61191d27a7b66f1.tmp	100%	Joe Sandbox ML		
C:\ProgramData\anydesk\AnyDesk.exe	0%	Virustotal		Browse
C:\ProgramData\anydesk\AnyDesk.exe	3%	Metadefender		Browse
C:\ProgramData\anydesk\AnyDesk.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\dpx.tmp\eee52229ee24a34cb61191d27a7b66f1.tmp	64%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\dpx.tmp\eee52229ee24a34cb61191d27a7b66f1.tmp	22%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\dpx.tmp\eee52229ee24a34cb61191d27a7b66f1.tmp	65%	ReversingLabs	Win32.Backdoor.Finfish	
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe (copy)	64%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe (copy)	22%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe (copy)	65%	ReversingLabs	Win32.Backdoor.Finfish	
C:\Windows\Installer\MSI5BE8.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSI5BE8.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI5BE8.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIB0A0.tmp	0%	Virustotal		Browse
C:\Windows\Installer\MSIB0A0.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSIB0A0.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIBA33.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSIBA33.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSIED31.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSIED31.tmp	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.install.exe.400000.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.install.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.install.exe.400000.7.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.install.exe.400000.3.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.install.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.install.exe.400000.5.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.install.exe.400000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.2.install.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.install.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://boot.net.anydesk.comabcdefABCDEFtruefalsebase.prot.packetInvalid	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
boot.net.anydesk.com	92.223.88.41	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://anydesk.com	AnyDesk.exe, 00000014.00000003.105006930 6.00000000006C0000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.anydesk.com/	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.opengl.org/registry/	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://help.anydesk.com/error-messages	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://order.anydesk.com/trial	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://anydesk.com/update	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/intl/$	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://help.anydesk.com/wol	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://help.anydesk.com/$	AnyDesk.exe, 00000014.00000003.105006930 6.00000000006C0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://my.anydesk.com	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.anydesk.com/	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://twitter.com/home? status=Do%20you%20know%20%23AnyDesk? %20AnyDesk%20is%20a%20small%20and%20qui	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.linkedin.com/shareArticle? mini=true&url=https%3A//anydesk.com/&title=Try%20A nyDesk%20Rem	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://console-ui.myanydesk2.on.anydesk.com	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.openssl.org/support/faq.html	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1041519952.00000000041B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000003.1051455 757.00000000010C0000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://anydesk.com/	AnyDesk.exe, 00000014.00000003.105006930 6.00000000006C0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://anydesk.com/privacy	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://datatracker.ietf.org/ipr/1526/	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.nayuki.io/page/qr-code-generator- library	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://policies.google.com/privacy?hl=$	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://support.anydesk.com/AnyDesk_on_macOS	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://help.anydesk.com/macos-security	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http:// https://help.anydesk.com/HelpLinkInstallLocationAnyDesk	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1041519952.00000000041B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1051455757.00000000010C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://boot-01.net.anydesk.com	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://datatracker.ietf.org/ipr/1914/	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://datatracker.ietf.org/ipr/1524/	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://anydesk.com/terms	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://anydesk.com/company#imprint	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://boot.net.anydesk.comabcdefABCDEFtruefalsebase.prot.packetInvalid	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.openssl.org/)	AnyDesk.exe, 00000014.00000003.105006930 6.00000000006C0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://anydesk.com/order	AnyDesk.exe, 00000014.00000003.105006930 6.00000000006C0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://help.anydesk.com/access	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://help.anydesk.com/backup-alias	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.openssl.org/support/faq.htmlEC_PRIVATEKEYpublicKeyparametersprivateKeyECPKPARAMETERSvalue	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1041519952.00000000041B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000003.1051455 757.00000000010C0000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://https://help.anydesk.com/share	anydesk.exe, 00000010.00000002.106967016 5.0000000001640000.00000002.00000001.010 00000.00000008.sdmp, anydesk.exe, 000000 10.00000003.1033845137.00000000037B0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000002.1169793 889.00000000018A0000.00000002.00000001.0 1000000.0000000A.sdmp, AnyDesk.exe, 0000 0014.00000003.1050069306.00000000006C000 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://my.anydesk.com/password-generator.	AnyDesk.exe, 00000014.00000003.105006930 6.00000000006C0000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://support.anydesk.com	AnyDesk.exe, 00000014.00000002.116979388 9.00000000018A0000.00000002.00000001.010 00000.0000000A.sdmp	false		high
http://https://help.anydesk.com/	AnyDesk.exe, 00000014.00000002.116979388 9.00000000018A0000.00000002.00000001.010 00000.0000000A.sdmp, AnyDesk.exe, 000000 14.00000003.1051455757.00000000010C0000. 00000004.00000800.00020000.00000000.sdmp, AnyDesk.exe, 00000014.00000003.1050069 306.00000000006C0000.00000004.00000800.0 0020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.223.88.41	boot.net.anydesk.com	Austria		199524	GCOREAT	false
195.181.174.174	unknown	United Kingdom		60068	CDN77GB	false
80.209.241.3	unknown	United States		395839	HOSTKEY-USAUS	false
195.181.174.167	unknown	United Kingdom		60068	CDN77GB	false

Private

IP
192.168.2.3

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679413
Start date and time: 05/08/202218:21:10	2022-08-05 18:21:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1.msi
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	4
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.evad.winMSI@34/28@4/5
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 100% (good quality ratio 83.3%) • Quality average: 57.3% • Quality standard deviation: 31.2%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .msi • Adjust boot time • Enable AMSI • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtFsControlFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:22:14	API Interceptor	3181x Sleep call for process: msiexec.exe modified
18:22:16	API Interceptor	959x Sleep call for process: VSSVC.exe modified
18:22:16	API Interceptor	896x Sleep call for process: svchost.exe modified
18:23:06	API Interceptor	2x Sleep call for process: icacls.exe modified
18:23:15	API Interceptor	206x Sleep call for process: install.exe modified
18:23:23	API Interceptor	99x Sleep call for process: anydesk.exe modified
18:23:28	API Interceptor	277x Sleep call for process: AnyDesk.exe modified
18:23:59	API Interceptor	3x Sleep call for process: netsh.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\78c343.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	7322
Entropy (8bit):	5.5670592053751085
Encrypted:	false
SSDEEP:	96:89EuAeuAD8tekIQBUwVPVfbCsAqGxUwVPVfbC6j2PBOuA5AqGSHLuAlv5qZW9MNz:8euZuLev6tfm86tfmuuUumk+uNdEpW
MD5:	B7025B12AA3BE2CAE5DEF3833655E219
SHA1:	102FA7B4C4260D9D5BD7C30281BD08001BEEB23C
SHA-256:	7B29024A6914C3B956525901EF818DABF62C9C89B6368612547024862E7BF148
SHA-512:	5C72611C364608962962D2ECF12D7A1B4673BD25D7A8427A2E8898ACE59B1E34D613098E807F772833DB86F5A1786EF0D86F96AE7C1F4E226A1844AFB312B0B7
Malicious:	false
Preview:	...@IXOS.@.....@`..U.@.....@.....@.....@.....@.....@.....&.{AC4583F8-6694-473E-BB77-32CDFC9BA940}F.Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com..1.msi.@.....@.....@.....@.....@.....&.{8CB27BF3-59BC-4419-BE15-E9E385453F27}.....@.....@.....@.....@.....@.....@.....@.....@....F.Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}&.{AC4583F8-6694-473E-BB77-32CDFC9BA940}.@.....bz.LateInstallFinish1....bz.LateInstallFinish2....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]$..@....1.SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\AnyDesk...@....(.&...LogonUser..user'.&...USERNAME..Peter Miller'.&...Date..8/5/2022'.&...Time..19:02:58'.&...WRAPPED_ARGUMENTS....RegisterProduct..Registering product..[1].....C:\Windows\Installer\78c

C:\ProgramData\anydesk\AnyDesk.exe

Process:	C:\ProgramData\anydesk.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3829888
Entropy (8bit):	**7.999053982852042**
Encrypted:	**true**
SSDEEP:	98304:nDFWG1bqjvcLIsoh5GbmkNC3dv2tthJ2/Ev6l3H:n7svcsImkN4chYECl3
MD5:	1BC5890C9E7BF54B7712E344B0AF9D04
SHA1:	78C9302C7A387A8D158F38D501784BE9B8B2716D
SHA-256:	AF61905129F377F5934B3BBF787E8D2417901858BB028F40F02200E985EE62F6
SHA-512:	7113888A8439AE5AF1B260C40229F7EBB98BDECE52EBAB0CE97137933AF4E9777D92D68166DBCF87A95CF88615452CAE7ECDF555B4785FFFE63C5783DBCB595D
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h.}.;.}.;.}.;..";.}.;..#;.}.;...;.}.;...;.}.;Rich.}.;.....PE..L.....1b.....".....*.....^.....@....@.....:...@.....p..PH.....4:..<.....text...5(.....*..... ..`.itext...^...@.....rdata.....@..@.data.....9.....9..2.....@....rsrc...PH...p...J....9.....@..@.reloc.....0:.....@..B..... .....

C:\ProgramData\anydesk\service.conf

Process:	C:\ProgramData\anydesk\AnyDesk.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	2898
Entropy (8bit):	6.03920180688192
Encrypted:	false
SSDEEP:	48:uISTiIhiUqIhAIH/ARw+Pi+2ZeFL8GjZnHA5OFh31vtd9CgtiFjRcFmKBI45:uIST/iUx1/AJPi2FNpAwFjP9TtccFFd5
MD5:	D78C36C1B2DF59D1D7A19E89218822A8
SHA1:	9D14F9FE8AF7BDF5EB25F7BEA366E4C7C6DB8389
SHA-256:	1932C23AE6AB035EF6AB0E224EF58638AF13DFD12C53A2BC13E7A281CFE51717
SHA-512:	974080C66AA8AD073450A3A44F97FA48FAB8F872BEEBE0CC25801E2D66ADF6BF184B9C6D1D80A9C3941EC991496D327393228A0A902D65AD0D4B7B55EA3F381
Malicious:	false

Preview:	ad.anynet.cert=-----BEGIN CERTIFICATE-----\nMIICqDCCAZACAQEwDQYJKoZIhvcNAQELBQAwGTEXMBUGA1UEAwwOQW55RGVzayBD\nbGllbnQwIBcNMjIwODA2MDEyMzMwWhgPMjA3MjA3MjQwMTIzMzBaMBkxFzAVBgNV\nBAMMDkFueURlc2sgQ2xpZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC\nAQEA3m9s0Xt1t6ybpCuW6GUgR24wf33iMQUiJAkO3evQMW3zyFFXrNZcRj0gHy6w\nBL21EgWWFj2otf99+2oj08znVPz3mdvxzGSw/UoyvVxy/gmtRT3WsMxcAvfd9EDV\nyAPwLRcp3mII7ngo1WZi0jDp0gWsbbDtdTXnNjJeTSKgLhh0VUIhYG4GpCPYcCzF\nzLUb+u1d6dYRj1r2nIhLHJ5a8Z2KcGlYtWvpin/OcMSw154LmU+WpLriSvk2acpu\nxpVJ65OTluRkbl4jmxjseMDXhK9cRLjPEHYCcERRJO+JsAO0h7oMEA8kb0YDQTz4\nxnIGxSU5NbzP5mXYU3Db0+7DyQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBgKZcB\ndwulkUuSK1r+HxcUkJlxVhs2UJvxaDaj7xsNFiH8+U+ljppHLIPE/OGC/ENBjrQm\n8FMll3kBnZh751nIsaYK5LoPXOFz9wTesecg7kQzYsFJOmwdg9pTMT8gIh9kzU3W\n3SQH6kvGz7EPfSRxl1JjzVLqbI5xGCtOi4WFl3Y0upNHz8wVAdHt9+ReuYH1cC0t\nCAljwdr26SmLy9XCcwcx6NsGf1FWYG4kURtaU/vJaqb+HDWZXICa11e2msyfIq1m\n4dGSYqDD+LTLd61V16rRBlY747w2QTxgc47coAPCaRhaKMWOY9oYWWHTaP6MJZVi\nLolPxJ9cTEJ8dHHY\n-----END CERTI

C:\ProgramData\anydesk\system.conf

Process:	C:\ProgramData\anydesk.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	664
Entropy (8bit):	4.694299449856687
Encrypted:	false
SSDEEP:	12:oUrQM3uqQHvWhOLroBGgFBGgItgw/T5hgnx7b0wlcpv:dF37AwetBVBTPC7bJlSv
MD5:	49B7C6D323D2E373B0CEAEB28B4BBDC5
SHA1:	0E5D4E26427190E07495FCC5FBFE46A20C07FCAA
SHA-256:	4E120EA4CAECD70BF796C634FA2278FAF0BA5424406D1AA367957210B666644A
SHA-512:	BC5EF736EC71E6940422240523978D6B918B5747AE30437188757458DDA415B02FB9CD61B208C59C5B89991D0557E4BEE4FE6ABB61BBBC3D63C0A5C73332657
Malicious:	false
Preview:	ad.anynet.fpr=ad8fec6ce2ea9587309c50b97175d8ed639a9f09.ad.anynet.relay.fatal_result=1.0.ad.anynet.relay.state=0.ad.security.frontend_clipboard=1.ad.security.frontend_clipboard_files=1.ad.security.frontend_clipboard_version=1.ad.security.permission_profiles._default.permissions.sas=1.ad.security.permission_profiles._unattended_access.permissions.sas=1.ad.security.permission_profiles._unattended_access.pwd=29a3bbba8f6029c5e4ab4fe97081df7dfcfd6458966ad8df64e9a620697bfd59.ad.security.permission_profiles._unattended_access.salt=a3a4ac0604db119fa69085484617bf37.ad.security.permission_profiles.version=1.ad.security.update_channel=stable.ad.security.update_type=0.

C:\System Volume Information\SPP\OnlineMetadataCache\{13f380d2-c95e-45d3-8b58-ce3c6d9cc4c1}_OnDiskSnapshotProp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	3048
Entropy (8bit):	3.694456222285318
Encrypted:	false
SSDEEP:	48:2QzaN38RN3x0/7wP8aZntCwL7feGp9bHfOIgbR1fOIgBKEBKRC6v6ReyZ:2QzI4uU/vfHzbOHXOHB9BpiW
MD5:	5F246453E47299A07D8C949665C8A0FE
SHA1:	5B341BA26C94F782A34C5523FAC302B7BCD3411A
SHA-256:	2EA3134921D1CD1F5E95079CE163D36DE1351A6361410967016DC69F0291F419
SHA-512:	DE72396CF4181BAC60E006E18A83519A9B3DF6E56FFACAAEDF9308CD8C4717B9E520DCACEE735803663DB6F661C5E5E04647B1443B73CFA474307AFC75C0C28
Malicious:	false
Preview:	.D.....M..,....c.Pc<.....^..E.X.<m...8.....@..5.....M..0.<fK...; .....$.....8...Q.....Q...I.n.s.t.a.l.l.e.d. .A.n.y.d.e.s.k. .-. .U.N.R.E.G.I.S.T.E.R.E.D. .-. .W.r.a.p.p.e.d. .u.s.i.n.g. .M.S.I. .W.r.a.p.p.e.r. .f.r.o.m. .w.w.w...e.x.e.m.s.i...c.o.m.....C.:.\.W.i.n.d.o.w.s.\.....1.7.9.6.0.5.....W.O.R.K.G.R.O.U.P.....Zi.A.@.H..i.tE<.....).(?..P..... ...2.....2...\.\.?.\.V.o.l.u.m.e.{.8.0.4.9.f.1.9.8.-.1.0.1.6.-.1.1.e.7.-.b.8.7.b.-.8.0.6.e.6.f.6.e.6.9.6.3.}.\.....C.:.\.....N).A.j..j.....(...0.....,...2.....2...\.\.?.\.V.o.l.u.m.e.{.8.0.4.9.f.1.9.8.-.1.0.1.6.-.1.1.e.7.-.b.8.7.b.-.8.0.6.e.6.f.6.e.6.9.6.3.}.\.....4.....(.C.:.).....<...@...D...H...L...P...T...X...\...`...d...h...l...p...t...x...|.....%.....%...A.d.o.b.e. .A.c.r.o.b.a.t. .R.e.a.d.e.r. .D.C. .1.9...0.1.0...2.0.0.9.8.....).....)...A.d.o.b.e. .F.l.a.s.h. .P.l.

C:\System Volume Information\SPP\metadata-2

Process:	C:\Windows\System32\msiexec.exe
File Type:	SysEx File - Twister
Category:	dropped
Size (bytes):	8734472
Entropy (8bit):	3.681659655459525
Encrypted:	false
SSDEEP:	12288:+8+YgDYEzT4G09wYKc9rMjG/BWigr7dCKV0/HwLQt+Y/g4zsuAvm7gPI+PhgcIrd:d0jYY8BWitXZh7TeQsPIy1YQza
MD5:	9CC465911CDBD0BFC8D7BFC74ECCE88B
SHA1:	867E1C21ADBC08A0BC12B1ED50F59EB3A78EC23F
SHA-256:	BA671D105C6C5A76B5B2D369E12887BCF3C729CFCF34F222A6DB2D4FF3AA666E
SHA-512:	04D495AC9EBEDC50F9FF325912A19A31B00A54EB0FA99830FBB6B1CBFB1847A21447BE699FE42AD45F80842E1D672F44FAEA0C38519CFEFAB4C86547106CDCF0
Malicious:	false

Preview:	.%..=..J....>.(_kb.....F..... ...Y.....Y...<.B.A.C.K.U.P._.C.O.M.P.O.N.E.N.T.S. .x.m.l.n.s.=.".x.-.s.c.h.e.m.a.:.#.V.s.s.C.o.m.p.o.n.e.n.t.M.e.t.a.d.a.t.a.". .v.e.r.s.i.o.n.=.".1...2.". .b.o.o.t.a.b.l.e.S.y.s.t.e.m.S.t.a.t.e.B.a.c.k.u.p.=.".y.e.s.". .s.e.l.e.c.t.C.o.m.p.o.n.e.n.t.s.=.".y.e.s.". .b.a.c.k.u.p.T.y.p.e.=.".f.u.l.l.". .p.a.r.t.i.a.l.F.i.l.e.S.u.p.p.o.r.t.=.".y.e.s.". .s.n.a.p.s.h.o.t.S.e.t.I.d.=.".1.3.f.3.8.0.d.2.-.c.9.5.e.-.4.5.d.3.-.8.b.5.8.-.c.e.3.c.6.d.9.c.c.4.c.1.".>.<.W.R.I.T.E.R._.C.O.M.P.O.N.E.N.T.S. .i.n.s.t.a.n.c.e.I.d.=.".4.5.8.b.f.6.d.0.-.9.8.7.c.-.4.5.2.7.-.b.7.b.9.-.5.d.4.0.5.2.4.a.2.1.2.4.". .w.r.i.t.e.r.I.d.=.".e.8.1.3.2.9.7.5.-.6.f.9.3.-.4.4.6.4.-.a.5.3.e.-.1.0.5.0.2.5.3.a.e.2.2.0.". .b.a.c.k.u.p.S.c.h.e.m.a.=.".0.".>.<.C.O.M.P.O.N.E.N.T. .c.o.m.p.o.n.e.n.t.N.a.m.e.=.".S.y.s.t.e.m. .F.i.l.e.s.". .c.o.m.p.o.n.e.n.t.T.y.p.e.=.".f.i.l.e.g.r.o.u.p."./.>.</.W.R.I.T.E.R._.C.O.M.P.O.N.E.N.T.S.>.<.W.R.I.T.E.R._.C.O.M.P.O.N.E.N.T.S. .i.

C:\System Volume Information\SPP\snapshot-2

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	3048
Entropy (8bit):	3.694456222285318
Encrypted:	false
SSDEEP:	48:2QzaN38RN3x0/7wP8aZntCwL7feGp9bHfOIgbR1fOIgBKEBKRC6v6ReyZ:2QzI4uU/vfHzbOHXOHB9BpiW
MD5:	5F246453E47299A07D8C949665C8A0FE
SHA1:	5B341BA26C94F782A34C5523FAC302B7BCD3411A
SHA-256:	2EA3134921D1CD1F5E95079CE163D36DE1351A6361410967016DC69F0291F419
SHA-512:	DE72396CF4181BAC60E006E18A83519A9B3DF6E56FFACAAEDF9308CD8C4717B9E520DCACEE735803663DB6F661C5E5E04647B1443B73CFA474307AFC75C0CA28
Malicious:	false
Preview:	.D.....M..,.....c.Pc<.....^..E.X.<m...8.....@..5.....M..0.<fK...; .....$.....8...Q.....Q...I.n.s.t.a.l.l.e.d. .A.n.y.d.e.s.k. .-. .U.N.R.E.G.I.S.T.E.R.E.D. .-. .W.r.a.p.p.e.d. .u.s.i.n.g. .M.S.I. .W.r.a.p.p.e.r. .f.r.o.m. .w.w.w...e.x.e.m.s.i...c.o.m.....C.:.\.W.i.n.d.o.w.s.\.....1.7.9.6.0.5.....W.O.R.K.G.R.O.U.P.....Zi.A.@.H..i.tE<.....).(?..P..... ...2.....2...\.\.?.\.V.o.l.u.m.e.{.8.0.4.9.f.1.9.8.-.1.0.1.6.-.1.1.e.7.-.b.8.7.b.-.8.0.6.e.6.f.6.e.6.9.6.3.}.\.....C.:.\.....N).A.j..j.....(...0.....,..2.....2...\.\.?.\.V.o.l.u.m.e.{.8.0.4.9.f.1.9.8.-.1.0.1.6.-.1.1.e.7.-.b.8.7.b.-.8.0.6.e.6.f.6.e.6.9.6.3.}.\.....4.....(.C.:.).....<...@...D...H...L...P...T...X...\...`...d...h...l...p...t...x...|.....%.....%...A.d.o.b.e. .A.c.r.o.b.a.t. .R.e.a.d.e.r. .D.C. .1.9...0.1.0...2.0.0.9.8.....).....)...A.d.o.b.e. .F.l.a.s.h. .P.l.

C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files.cab

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Microsoft Cabinet archive data, 3811024 bytes, 1 file
Category:	dropped
Size (bytes):	3811024
Entropy (8bit):	**7.999935868582085**
Encrypted:	**true**
SSDEEP:	98304:bvXhd7YjjTcLO6KnQh5YUNa/ckQGQCWijuYAHwO:bzkTcilYUNuNCAuPHD
MD5:	223FA9756FCE44168ABD5DB7AFA03FAD
SHA1:	2E8BFC88819353490EC4C201445DC004FA9AAFF5
SHA-256:	A929C064C064A1B5013B8FBCE01FEB7AE08E6BD9B05106DCDA8320F9DB0FB13D
SHA-512:	0EFE5917995E6EE837AADBB9951AD1F7BCADFA9638DE747B219E6A9BBE53FD586118A291776C6FF1C0416B3B439DADB0336AE61E74B1E6D12E9A38F11DAC33EC
Malicious:	false
Preview:	MSCF.....&:.....,.....~...H...v.....:.....T.p .install.exe.....W..[.....H..."T.#..m...U.e..p..n.I:....h<d.r)R.*+.-[...y/c..1..x.w...>..."...TI1[(.....5.H.....F..j.....}}K.....O....%. ..o".Pj/M2Io..t.....B/Z...Bk.....8...jA.rI`..rr....I#)R...5?I...h.....C..L...S.fP$..$H.D4..iq6....4.....kq.....#.*..!X....+.C.....-p-.'..Od...lY...E...!.A..'..qY.%l.....6....1.....~.}.4....{ ."...e.(/M^,N..x|d.../..@.,.Wb..I.j..]D'....T..w..Y_...*.{.....R.-.....r...;..)...f..!/.:....l+.t5....V...Q+.Q.#.I..@..k...Q..'(...T\.7...A.'?..K....b_.o.[...w.....|.....r.7....'].ys.P.N.....o. K7.....{..(.y3..o..I.....wp.....w.^.]..g.n.;lp.$..p.....p^.....=r.R.LH...{....|..^=..ZM2....n.L...$...S.....<E`.7o.{-MX.U,.t..I.7..[.<.IH...T..A.....Y=._V..0...4h.....([.%W_..,{.?.#.C .s]..<Q]Q...AM...w.....S.!.B.q....vR.V>..I..#....+%..X.m&}.d-.<.'$..6.{.....!.`..%....ZF.`{.u.P....mZ4...H.....J3h)....(..0(...2..

C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\dpx.tmp\eee52229ee24a34cb61191d27a7b66f1.tmp

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3837440
Entropy (8bit):	**7.998303388385036**
Encrypted:	**true**
SSDEEP:	98304:dDFWG1bqjvcLIsoh5GbmkNC3dv2tthJ2/Ev6l3:d7svcsImkN4chYECl
MD5:	8C42AB81F90EE0592F7A709F0F7E320B
SHA1:	6656C6CA4611245CDA44958BAB84866196C9D95B
SHA-256:	BEB6182CEAB6EA0B0FDC0F41F8069632317E0F941419B75EDE4145593CD6A21C
SHA-512:	57A444D1B03DCD428EB386E5551137DF5B7D401AC39F5B3481DAD6A94C7A95C3DD90B638532EFDD813C293CF4F949ED4461424FA940410F2D59E2DFDD88CA5A
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 64%, Browse • Antivirus: Metadefender, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*r..n...n...n.....q....3..o.....o...Richn.....PE..L..... b.....\|:....$..... ....@.....:.....m;.....p ..P....@...p:..... ..l.....text...z.... ....`.rdata..... .....@..@.data.....0.....@....rsrc....p:..@...r:.....@..@..... ....

C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe (copy)

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3837440
Entropy (8bit):	**7.998303388385036**
Encrypted:	**true**
SSDEEP:	98304:dDFWG1bqjvcLIsoh5GbmkNC3dv2tthJ2/Ev6l3:d7svcsImkN4chYECl
MD5:	8C42AB81F90EE0592F7A709F0F7E320B
SHA1:	6656C6CA4611245CDA44958BAB84866196C9D95B
SHA-256:	BEB6182CEAB6EA0B0FDC0F41F8069632317E0F941419B75EDE4145593CD6A21C
SHA-512:	57A444D1B03DCD428EB386E5551137DF5B7D401AC39F5B3481DAD6A94C7A95C3DD90B638532EFDD813C293CF4F949ED4461424FA940410F2D59E2DFDD88CA5A
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 64%, Browse • Antivirus: Metadefender, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*r..n...n...n.....q....3..o.....o...Richn.....PE..L..... b.....\|:....$..... ....@.....:.....m;.....p ..P....@...p:..... ..l.....text...z.... ....`.rdata..... .....@..@.data.....0.....@....rsrc....p:..@...r:.....@..@..... ....

C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\msiwrapper.ini

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	1426
Entropy (8bit):	3.650455137438292
Encrypted:	false
SSDEEP:	24:udX8DW8XjsjToZkESrFEqNbH+qNbH4yDqNbHgO+sD+n:uYg1JFxNvNE7Nxyn
MD5:	F03B2CD5999D483E566FED5D7E1BD078
SHA1:	EBC636C000806FBCD93952B3B4BFB97BF281E2F9
SHA-256:	36CCB8B1213585E1CD56DEF34AC141DD8653AA0050A0C4105FA4C285AC3CC084
SHA-512:	83690F70DCD916684C0CBE302A35C96909D31D6C6D06F0BE6950D59ACE0B834EC69021B851E9C30A0B594A5DA7044EBA3F0CADD0417FA588DCE148AFB921E5C6
Malicious:	false
Preview:	W.r.a.p.p.e.d.A.p.p.l.i.c.a.t.i.o.n.I.d.=.A.n.y.D.e.s.k...W.r.a.p.p.e.d.R.e.g.i.s.t.r.a.t.i.o.n.=.H.i.d.d.e.n...I.n.s.t.a.l.l.S.u.c.c.e.s.s.C.o.d.e.s.=.0...E.l.e.v.a.t.i.o.n.M.o.d.e.=.n.e.v.e.r...B.a.s.e.N.a.m.e.=.i.n.s.t.a.l.l...e.x.e...C.a.b.H.a.s.h.=.a.9.2.9.c.0.6.4.c.0.6.4.a.1.b.5.0.1.3.b.8.f.b.c.e.0.1.f.e.b.7.a.e.0.8.e.6.b.d.9.b.0.5.1.0.6.d.c.d.a.8.3.2.0.f.9.d.b.0.f.b.1.3.d...S.e.t.u.p.P.a.r.a.m.e.t.e.r.s.=...W.o.r.k.i.n.g.D.i.r.=...C.u.r.r.e.n.t.D.i.r.=.*.S.O.U.R.C.E.D.I.R.*...U.I.L.e.v.e.l.=.5...F.o.c.u.s.=.y.e.s...S.e.s.s.i.o.n.D.i.r.=.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.4.a.7.5.4.4.4.8.-.1.3.7.2.-.4.b.6.2.-.a.f.7.7.-.6.f.1.6.5.0.2.4.6.a.5.a.\...F.i.l.e.s.D.i.r.=.C.:.\.U.s.e.r.s.\.A.l.b.u.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.M.W.-.4.a.7.5.4.4.4.8.-.1.3.7.2.-.4.b.6.2.-.a.f.7.7.-.6.f.1.6.5.0.2.4.6.a.5.a.\.f.i.l.e.s.\...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.F.i.l.e.=...R.u.n.B.e.f.o.r.e.I.n.s.t.a.l.l.P.a.r.a.m.e.t.e.r.s.=...R.u.n.A.f.t.e.r.I.n.

C:\Users\user\AppData\Local\Temp\~DF0154135B388C6B07.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.06743406194521226
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOv+eHmNfftCVky6lh1:2F0i8n0itFzDHFv+eGBTj
MD5:	F6D7E066F3F3BFE6E80C388A8E80530D
SHA1:	4113DA23B498529E7D373BB6B15C511E6215CBF0

SHA-256:	6FD79F05C77A1C8CB5D73B1FEC2B16E09273E029DDC196F24115C57178C7D1EC
SHA-512:	AB982CEEAEF2E1D690BC761C129EC387C4919BCF910513387D9D46111FDD9768F66E1CD46311FD169BD1122356DE71964590DE087B06A8BA966216EA7736E46
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF49DA8C305B58D2AD.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.12990324508728232
Encrypted:	false
SSDEEP:	24:Ojd8vdOQCwY+8JfAebfddipV7sddipVlVIwGVlrkg9Syve+QG:I8virfddSBsddSH2rjeNG
MD5:	DAEC78D92F1DF6670EB07754808C3ECC
SHA1:	F59648041B22EC5BFE871E08EDB40278B85A5BD2
SHA-256:	8DCAE1DCF7F1AA8B3F96C78805593524994AA603C611E6B9523CBCB93A774354
SHA-512:	FC8D121F8B877528B6E902869E931A74F88097870B8F0CD66213F9F3ACC8A431619EAD27D45DD4EE75B79CE77BB414E641FCC0A495C0B67A1FE900FB36B5183B
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFFAFE55FFC650FC61.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\AnyDesk\ad.trace

Process:	C:\ProgramData\anydesk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	10515
Entropy (8bit):	4.228344603555986
Encrypted:	false
SSDEEP:	96:EtFBqt1tNtFZmKJ4FgzgFN5mj4b515wvOQ8kQVQbQWttAhDFhttFCxxv:0wPHFcKFjw9ksQNttvxV
MD5:	C4D40B6620A5E49C215BFB0C04D9FA94
SHA1:	84C02E79A8DD2CEA191AF99341F2271A6139DC48
SHA-256:	1604100784E9D590149D5221F7F4318AFAE913A22EA07F6EA461F8D215EDFA25
SHA-512:	06F4EE0DFFB5231F59327920110B48566C4B6FFA35FEC1113F84CE1FAE0C932ACD07F01E2AEA022FF7DDE2A5601C2391B6333E0FFCC2B4B8D7F1DC270F03E14
Malicious:	false

Preview:	..... info 2022-08-06 01:23:23.745 installer 2640 2428 main - * AnyDesk Windows Startup *.. info 2022-08-06 01:23:23.745 installer 2640 2428 main - * Version 7.0.7 (release/win_7.0.x 96f8d80eac273a9144abccce2f66dbc2200cc81d).. info 2022-08-06 01:23:23.745 installer 2640 2428 main - * Custom Client (no ID).. info 2022-08-06 01:23:23.745 installer 2640 2428 main - .. info 2022-08-06 01:23:23.745 installer 2640 2428 main - Process started at 2022-08-06. PID 2640. OS is Windows 7 (64 bit).. info 2022-08-06 01:23:23.745 installer 2640 2428 impl_selector - using sse2 (intrinsics)..warning 2022-08-06 01:23:23.745 installer 2640 2428 terminator - All clear!.. info 2022-08-06 01:23:23.745 installer

C:\Users\user\AppData\Roaming\AnyDesk\user.conf

Process:	C:\ProgramData\anydesk\AnyDesk.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1003
Entropy (8bit):	4.272230203413794
Encrypted:	false
SSDEEP:	24:snKoXHZgCJg2cZ0FmienKoX1M61n0Q17/iMQBbSI:sn1j2genMa0CHQBbSI
MD5:	BB28C065F16674CB7688B72C683EC985
SHA1:	2D7E18B400398CDC33A387C315D434C9FFDA0CB0
SHA-256:	FE5DD9BE649AB519A47659B151A2607AC623179F150765C399B1EF0C7A90F82E
SHA-512:	6995413F415F6D708254C0BD6388B397B181B6BAF28B3D9182E50404556CBC8C38AB0CED5A2A93550DA5FBD2EDBC7945E3E2F24AD0358FBC00A3494A7040DDE
Malicious:	false
Preview:	ad.invite.created_list_encrypted=6fa74c609a01f31f1f670668df954f4642a4aae8018a18da425960b3eca6f8f4a1ec65a7e7bb22120bf648310f1fa2df0b53d2e90e4e008262013ecaea920fe5fd03c1aa69649c8b8b7110ec222522013f23dfea2c5de548b20a73a9d414c27374ab0862b47b212f41cf5778b89cca6521ac5f446f5a2ffbbe9811a458492e39926770649a38e9721366902a51645470f0d9e8a0d72bdda1c667dc1fbaea3cca74dd806804e91cbf13cfc3d8e58bf6cc1ef38cac7e2c3206610342c063879a2bdf13cf19bf043a5ac522ccccbbc23a319d59a30a59c069535a7b8f54c7cdf18ddd032a16d9ee.ad.invite.received_list_encrypted=6fa74c609a01f31f1f670668df954f4642a4aae8018a18da425960b3eca6f8f4a1ec65a7e7bb22120bf648310f1fa2df0b53d2e90e4e008262013ecaea920219e161c9e6f996ad5835c58dfc95d32660f8f91a7ceb734bd5c905f6e04db3c27374ab0862b47b212f41cf5778b89c037c550169499eb92f75a169d19422002633e9f784bb1abb9c7461a00b08edbb5470f0d99f57071e94afc197f90cdd3c896084ac806804e96c7ac9eb148905cb1bf54d6113d0c1ffff947be9e29fdf46c726ed7608deda5eebf876a0049476f5d19458050a6ce61fb3fbce38819f06f911de17a54117d6af.ad.ui.lang=

C:\Windows\Installer\78c341.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 0.7.0.0, Subject: Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Anydesk, Keywords: Installer, Template: Intel;1033, Revision Number: {8CB27BF3-59BC-4419-BE15-E9E385453F27}, Create Time/Date: Thu Feb 18 21:32:30 2021, Last Saved Time/Date: Thu Feb 18 21:32:30 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Category:	dropped
Size (bytes):	4063232
Entropy (8bit):	7.978539254164263
Encrypted:	false
SSDEEP:	98304:pp+vXhd7YjjTcLO6KnQh5YUNa/ckQGQCWijuYAHw:+zkTcilYUNuNCAuPH
MD5:	6CF5AD7A7D1B7BAB0C62E246CF41A985
SHA1:	B06A03ADC550EAD96534F5E723395C4E16BFDF44
SHA-256:	FB9F0BF2B71BF576053C56CB913EA4E93581FC9D3AA9D6D8A0AE572A1622F050
SHA-512:	46CD8BD1EAD75A8ADB7D5BFF81A2FDC04567D462E965664F6F9F796237839F07F74D2201C3DA8F7F37C9DFC45749ED88708DB5A216D84F7AC146E5AF58A860E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	.....>..... ....

C:\Windows\Installer\78c342.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5498517775518001
Encrypted:	false
SSDEEP:	24:J7rFC/llm6cpmUHCpVluqo+QG0/rddipVlVIwGVlrkg9SCddipV7eJfAebpQCwYi:1r0pcDHoluzNG0zddSH2rbddSBerF8v
MD5:	14F8EB017B55B6EFBBC74E949581F9F7
SHA1:	E9B5537C29E22FAC2A7535C766579710CC901AC4
SHA-256:	486813FA64D996C93CB8251845F093C0F26C0277ACFF9C06004DE34EB825CFBE

SHA-512:	E9222151D1E201A06F39CBFFE9F786F968B45226DBDFEA99A0DC6746820247D23AEEB74312277BBF40B060ADDDF7734E70527CE824C55DB32A55D637012202DA
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Installer\78c344.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 0.7.0.0, Subject: Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Anydesk, Keywords: Installer, Template: Intel;1033, Revision Number: {8CB27BF3-59BC-4419-BE15-E9E385453F27}, Create Time/Date: Thu Feb 18 21:32:30 2021, Last Saved Time/Date: Thu Feb 18 21:32:30 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Category:	dropped
Size (bytes):	4063232
Entropy (8bit):	7.978539254164263
Encrypted:	false
SSDEEP:	98304:pp+vXhd7YjjTcLO6KnQh5YUNa/ckQGQCWijuYAHw:+zkTciIYUNuNCAuPH
MD5:	6CF5AD7A7D1B7BAB0C62E246CF41A985
SHA1:	B06A03ADC550EAD96534F5E723395C4E16BFDF44
SHA-256:	FB9F0BF2B71BF576053C56CB913EA4E93581FC9D3AA9D6D8A0AE572A1622F050
SHA-512:	46CD8BD1EAD75A8ADB7D5BFF81A2FDC04567D462E965664F6F9F796237839F07F74D2201C3DA8F7F37C9DFC45749ED88708DB5A216D84F7AC146E5AF58A860E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	.....>..... ....

C:\Windows\Installer\MSI5B7A.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	428024
Entropy (8bit):	6.5173927188942296
Encrypted:	false
SSDEEP:	12288:stJRQ+gjpjegLyo8ktJRQ+gjpjegLyo8J:stBcpVLSktBcpVLSJ
MD5:	9069E5D699573FA8DE65F4D66FC36782
SHA1:	3F6D828772867E2708F4491DE44C57FE3987F931
SHA-256:	7F7DDF73140A3568819DE6AC422D2B42A76856FE96C2A658AF531ADB3BBD9B33
SHA-512:	C7614A19E126273A7464F16EF3470C4B4CE459119CBC489DE9DCDDDC5DBE2057AAAE77D551F8C26A9EB59E2FEAB373C1C565921379564EFF9ED4CE85EDF977C
Malicious:	false
Preview:	...@IXOS.@.....@...U.@.....@.....@.....@.....@.....@.....&.{AC4583F8-6694-473E-BB77-32CDFC9BA940}F.Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com..1.msi.@.....@.....@.....@.....@.....&.{8CB27BF3-59BC-4419-BE15-E9E385453F27}.....@.....@.....@.....@.....@.....@.....@....F.Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....@.....ProcessComponents..Updating component registration.....@.....@.....@.].....&.{EDE10F6C-30F4-42CA-B5C7-ADB905E45BFC}?.02:\SOFTWARE\EXEMSI.COM\MSI Wrapper\Installed\AnyDesk\LogonUser.@.....@.....@.....@.....@.....bz.LateInstallFinish1....J...bz.LateInstallFinish1.@.....@..MZ.....@.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p.....p..../.p.....p...q.%.p.....p.....p.....p.Rich..p.....PE..

C:\Windows\Installer\MSI5BE8.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513444216841171
Encrypted:	false
SSDEEP:	3072:AspAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLw2loHUvU4yGxr53qM2a8:2tOdiRQYpgjpjew5LLyGx1qo8
MD5:	4CAAA03E0B59CA60A3D34674B732B702
SHA1:	EE80C8F4684055AC8960B9720FB108BE07E1D10C
SHA-256:	D01AF2B8C692DFFB04A5A04E3CCD0D0A3B2C67C8FC45A4B68C0A065B4E64CC3D
SHA-512:	25888848871286BDD1F9C43A0FBA35640EDB5BAFBE0C6AA2F9708A070EA4E5B16745B7C4F744AE4F5643F75EF47F196D430BF70921ED27715F712825EC590A34

Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p....p.Rich..p... .....PE..L.....`.....!....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\MSIB0A0.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513444216841171
Encrypted:	false
SSDEEP:	3072:AspAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLw2loHUvU4yGxr53qM2a8:2tOdiRQYpgjpjew5LLyGx1qo8
MD5:	4CAAA03E0B59CA60A3D34674B732B702
SHA1:	EE80C8F4684055AC8960B9720FB108BE07E1D10C
SHA-256:	D01AF2B8C692DFFB04A5A04E3CCD0D0A3B2C67C8FC45A4B68C0A065B4E64CC3D
SHA-512:	25888848871286BDD1F9C43A0FBA35640EDB5BAFBE0C6AA2F9708A070EA4E5B16745B7C4F744AE4F5643F75EF47F196D430BF70921ED27715F712825EC590A34
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p....p.Rich..p... .....PE..L.....`.....!....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\MSIBA33.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	212992
Entropy (8bit):	6.513444216841171
Encrypted:	false
SSDEEP:	3072:AspAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLw2loHUvU4yGxr53qM2a8:2tOdiRQYpgjpjew5LLyGx1qo8
MD5:	4CAAA03E0B59CA60A3D34674B732B702
SHA1:	EE80C8F4684055AC8960B9720FB108BE07E1D10C
SHA-256:	D01AF2B8C692DFFB04A5A04E3CCD0D0A3B2C67C8FC45A4B68C0A065B4E64CC3D
SHA-512:	25888848871286BDD1F9C43A0FBA35640EDB5BAFBE0C6AA2F9708A070EA4E5B16745B7C4F744AE4F5643F75EF47F196D430BF70921ED27715F712825EC590A34
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p....p.Rich..p... .....PE..L.....`.....!....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\MSIED31.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	212992
Entropy (8bit):	6.513444216841171
Encrypted:	false
SSDEEP:	3072:AspAtOdmXwCGjtYNKbYO2gjpcm8rRuqpjCLw2loHUvU4yGxr53qM2a8:2tOdiRQYpgjpjew5LLyGx1qo8
MD5:	4CAAA03E0B59CA60A3D34674B732B702
SHA1:	EE80C8F4684055AC8960B9720FB108BE07E1D10C
SHA-256:	D01AF2B8C692DFFB04A5A04E3CCD0D0A3B2C67C8FC45A4B68C0A065B4E64CC3D

SHA-512:	25888848871286BDD1F9C43A0FBA35640EDB5BAFBE0C6AA2F9708A070EA4E5B16745B7C4F744AE4F5643F75EF47F196D430BF70921ED27715F712825EC590A34
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p.....p....p..../.p.....p...q.%.p.....p....p.....p.Rich..p... .....PE..L.....`.....!....h.....K.....@.....P...]....P.....`.....p...@.....t..... .....text....f.....h..... ..`.rdata.....l.....@..@.data....5.....@....rsrc.....P.....@..@.reloc...)...`...*.....@..B..... ....

C:\Windows\Installer\SourceHash{AC4583F8-6694-473E-BB77-32CDFC9BA940}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.160574548383438
Encrypted:	false
SSDEEP:	12:JSbX72FjEiAGiLIlHVRpgh/77777777777777777777777vDHFv+eGB3Jpjl0G:JqiQI5o5+eOGF
MD5:	80A87B6E2D6888C84B8F90246E263EE4
SHA1:	ACB5270E5112C472F6D91B94322A8F3C8671EFB5
SHA-256:	1E86519BF9767892FC4ED05A712D90415E02B8C6B260E7556E5AF00174F0092F
SHA-512:	F98006A315B6FAA2C939A789E36EBA40860AEA58A95B845463B8B4C66B6E5C9A4978BFF4C034EB90169516B7E1F0EA458BA6CB8E68FE65148703580219D2761B
Malicious:	false
Preview:	.....>..... ....

C:\Windows\Logs\DPX\setupact.log

Process:	C:\Windows\SysWOW64\expand.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	969
Entropy (8bit):	4.316698873864823
Encrypted:	false
SSDEEP:	24:Y6mE76KbEE76KbE76KbEE76KbEE6mE6mE76KbEE76KbEE6r:YVE76KbEm6KbE76KbEm6KbE+EVE76KbY
MD5:	62DEA788F4FAC87F00521EB4D5BDE650
SHA1:	B1DE499D3485674F25810AD3B4EC35C2B79CE2B9
SHA-256:	7B341C7ED6AECCF2058AE39B62BF891D02664BC7399ED3F8B2FE0277E8E16BAA
SHA-512:	0A4AA1B760AAE3BABA90ACCA55075206794F55160B4096C1B61C4C653CD3930DACAFAC46E6E37CDA488E7BFF5797C6024D33C28B163362236DBDCB1EB0D2FB0E
Malicious:	false
Preview:	.2022-08-05 18:23:08, Info DPX Started DPX phase: Resume and Download Job..2022-08-05 18:23:08, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-08-05 18:23:08, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-08-05 18:23:08, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-08-05 18:23:08, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-08-05 18:23:08, Info DPX Ended DPX phase: Resume and Download Job..2022-08-05 18:23:08, Info DPX Started DPX phase: Resume and Download Job..2022-08-05 18:23:08, Info DPX Started DPX phase: Apply Deltas Provided In File..2022-08-05 18:23:08, Info DPX Ended DPX phase: Apply Deltas Provided In File..2022-08-05 18:23:08, Info DPX Ended DPX phase: Resume and Download Job..

C:\Windows\SysWOW64\log1.txt

Process:	C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	14
Entropy (8bit):	3.8073549220576055
Encrypted:	false
SSDEEP:	3:i1lfoN:i1lAN
MD5:	2451B91DDBC6BE55D3D1FF81E7269D71
SHA1:	70E56DBCB95AF007F3B08F86C0A22050991DDF02
SHA-256:	BF5EAAB0BE11F12556F4CEEB507DA91D8E5178BEE032C003A26070B5794774B4
SHA-512:	7B08E8E00CD20D78D84A9BA2D8C8B4E7C7804BA6D1013D886FE640A70394B1484AF2658C1A94D23EC0BCAA692E8651434BAE48B20B4A895BBB9FD3A438AEAD4F
Malicious:	false

Preview:	anydesk-ID:..0

C:\programdata\anydesk.exe

Process:	C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3829888
Entropy (8bit):	**7.999053982852042**
Encrypted:	**true**
SSDEEP:	98304:nDFWG1bqjvcLIsoh5GbmkNC3dv2tthJ2/Ev6l3H:n7svcsImkN4chYECl3
MD5:	1BC5890C9E7BF54B7712E344B0AF9D04
SHA1:	78C9302C7A387A8D158F38D501784BE9B8B2716D
SHA-256:	AF61905129F377F5934B3BBF787E8D2417901858BB028F40F02200E985EE62F6
SHA-512:	7113888A8439AE5AF1B260C40229F7EBB98BDECE52EBAB0CE97137933AF4E9777D92D68166DBCF87A95CF88615452CAE7ECDF555B4785FFFE63C5783DBCB595D
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h.}.;.}.;.}.;..";.}.;..#;.}.;...;.}.;...;.}.;Rich.}.;.....PE..L.....1b .....".....*....:..^.....@....@.....:...@.....p..PH.....4:..<.....text...5(.... ...*..... ..`.itext...^...@.....rdata.....@..@.data.....9.....9..2.....@....rsrc...PH...p...J....9.....@..@.reloc.....0:..... ..@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Code page: 1252, Title: Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 0.7.0.0, Subject: Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, Author: Anydesk, Keywords: Installer, Template: Intel;1033, Revision Number: {8CB27BF3-59BC-4419-BE15-E9E385453F27}, Create Time/Date: Thu Feb 18 21:32:30 2021, Last Saved Time/Date: Thu Feb 18 21:32:30 2021, Number of Pages: 200, Number of Words: 2, Name of Creating Application: MSI Wrapper (10.0.50.0), Security: 2
Entropy (8bit):	7.978539254164263
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	1.msi
File size:	4063232
MD5:	6cf5ad7a7d1b7bab0c62e246cf41a985
SHA1:	b06a03adc550ead96534f5e723395c4e16bfdf44
SHA256:	fb9f0bf2b71bf576053c56cb913ea4e93581fc9d3aa9d6d8a0ae572a1622f050
SHA512:	46cd8bd1ead75a8adb7d5bff81a2fdc04567d462e965664f6f9f796237839f07f74d2201c3da8f7f37c9dfc45749ed88708db5a216d84f7ac146e5af58a8608e
SSDEEP:	98304:pp+vXhd7YjjTcLO6KnQh5YUNa/ckQGQCWijuYAHw:+zkTcilYUNuNCAuPH
TLSH:	411633603AD8C537D2DA0636092E8BAA3A657D755F21C0DB2B587CBC5E317D3AC39342
File Content Preview:	.....>.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "1.msi"

Indicators

Has Summary Info:	
Application Name:	MSI Wrapper (10.0.50.0)
Encrypted Document:	False
Contains Word Document Stream:	False

Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary	
Code Page:	1252
Title:	Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com 0.7.0.0
Subject:	Anydesk - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com
Author:	Anydesk
Keywords:	Installer
Template:	Intel;1033
Revion Number:	{8CB27BF3-59BC-4419-BE15-E9E385453F27}
Create Time:	2021-02-18 21:32:30
Last Saved Time:	2021-02-18 21:32:30
Number of Pages:	200
Number of Words:	2
Creating Application:	MSI Wrapper (10.0.50.0)
Security:	2

Document Summary	
Document Code Page:	1251
Company:	Anydesk

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 120	
General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	120
Entropy:	2.826912441242884
Base64 Encoded:	False
Data ASCII:	. . . . + , 0 . . . H . . . . (. . . . . . 0 . . . . 8 . . . . A n y d e s k .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 48 00 00 00 03 00 00 00 01 00 00 00 28 00 00 00 00 00 00 80 30 00 00 00 0f 00 00 00 38 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 e3 04 00 00 13 00 00 00 19 04 00 00 1e 00 00 00 08 00 00 00 41 6e 79 64 65 73 6b 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 528	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	528
Entropy:	4.752216684650982
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . + ' 0 . . . . x . . . . p . . . . I n s t a l l e r . . . . I n t e l ; 1 0 3 3 . . . . . . ' . . . { 8 C B 2 7 B F 3 - 5 9 B C - 4 4 1 9 - B E 1 5 - E 9 E 3 8 5 4 5 3 F 2 7 } . . @ . . . . k p = . . @ . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 e0 01 00 00 0d 00 00 00 01 00 00 00 78 00 00 00 02 00 00 00 18 01 00 00 03 00 00 00 70 01 00 00 04 00 00 00 08 01 00 00 05 00 00 00 80 00 00 00 07 00 00 00 94 00 00 00 09 00 00 00 a8 00 00 00 0c 00 00 00 d8 00 00 00 0d 00 00 00 e4 00 00 00

Stream Path: \x17163\x16689\x18229\x16766\x18365\x17760\x17636\x16947\x16167\x17896\x17656\x17753\x17074\x16693\x18480, File Type: Microsoft Cabinet archive data, 3811024 bytes, 1 file, Stream Size: 3811024	
General	
Stream Path:	\x17163\x16689\x18229\x16766\x18365\x17760\x17636\x16947\x16167\x17896\x17656\x17753\x17074\x16693\x18480
File Type:	Microsoft Cabinet archive data, 3811024 bytes, 1 file
Stream Size:	3811024
Entropy:	7.999935868582085
Base64 Encoded:	True

General	
Data ASCII:	MSCF....&:.....,...............~..H...v....:.......Tp .install.exe..W.[..H.."T#..m.Uep.nI:...h<d.r)R*+-[y/c1.xw>."TI1[(....5.H...Fj...}}K..O.%.o".Pj/M2Iot..B/ZBk....8.,jArI`rrI#)R..5?Ih.......CLSfP$.$HD4.iq6.4..kq.....#.*.!X..+.C..-p-.'..OdIYE.!.A'.qY%I..
Data Raw:	4d 53 43 46 00 00 00 00 d0 26 3a 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00 7e ea 00 00 48 00 00 00 76 00 03 12 00 8e 3a 00 00 00 00 00 00 00 c6 54 d7 70 20 00 69 6e 73 74 61 6c 6c 2e 65 78 65 00 b8 ea a5 05 d4 57 00 80 5b 80 80 8d 04 10 48 a9 07 00 22 54 80 23 00 00 6d 00 fe b7 55 ab 65 97 99 70 b9 1b 6e c9 49 3a 09 12 9d 11 68 3c 64 19 72 29 52 cb 2a 2b 1a 2d

Stream Path: \x17163\x16689\x18229\x16766\x18365\x17932\x17910\x17458\x16778\x17207\x17522\x17357\x18479, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 212992

General	
Stream Path:	\x17163\x16689\x18229\x16766\x18365\x17932\x17910\x17458\x16778\x17207\x17522\x17357\x18479
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	212992
Entropy:	6.513444216841171
Base64 Encoded:	True
Data ASCII:	MZ..................@..!.L!This program cannot be run in DOS mode....$........pppp.p/p..pq%pp.p.pRichp........................PE..L....`..........!.....h.........K..@..
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x18496\x15167\x17394\x17464\x17841, File Type: data, Stream Size: 672

General	
Stream Path:	\x18496\x15167\x17394\x17464\x17841
File Type:	data
Stream Size:	672
Entropy:	4.764474142026
Base64 Encoded:	False
Data ASCII:	...................".".".).).).*.*.*.+.+./././././.5.5.5.=.=.=.=.=.M.M.M.M.M.M.M.M.\\.\\.a.a.a.a.a.a.a.a.o.o.r.r.r.s.s.s.t.t.w.w.w.w.w.w...
Data Raw:	06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2f 00 2f 00 2f 00 2f 00 2f 00 2f 00 35 00 35 00 35 00 3d 00 3d 00 3d 00 3d 00 3d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 5c 00 5c 00 61 00 61 00 61 00 61 00 61 00 61 00 61 00 61 00 6f 00 6f 00 72 00 72 00 72 00 73 00 73 00 73 00 74 00 74 00 77 00

Stream Path: \x18496\x16191\x17783\x17516\x15210\x17892\x18468, File Type: ASCII text, with very long lines, with no line terminators, Stream Size: 8546

General	
Stream Path:	\x18496\x16191\x17783\x17516\x15210\x17892\x18468
File Type:	ASCII text, with very long lines, with no line terminators
Stream Size:	8546
Entropy:	5.082724064913251
Base64 Encoded:	True
Data ASCII:	NameTableTypeColumn_ValidationValueNPropertyId_SummaryInformationDescriptionSetCategoryKeyColumnMaxValueNullableKeyTableMinValueIdentifierName of tableName of columnY;NWhether the column is nullableYMinimum value allowedMaximum value allowedFor foreign key
Data Raw:	4e 61 6d 65 54 61 62 6c 65 54 79 70 65 43 6f 6c 75 6d 6e 5f 56 61 6c 69 64 61 74 69 6f 6e 56 61 6c 75 65 4e 50 72 6f 70 65 72 74 79 49 64 5f 53 75 6d 6d 61 72 79 49 6e 66 6f 72 6d 61 74 69 6f 6e 44 65 73 63 72 69 70 74 69 6f 6e 53 65 74 43 61 74 65 67 6f 72 79 4b 65 79 43 6f 6c 75 6d 6e 4d 61 78 56 61 6c 75 65 4e 75 6c 6c 61 62 6c 65 4b 65 79 54 61 62 6c 65 4d 69 6e 56 61 6c 75 65

Stream Path: \x18496\x16191\x17783\x17516\x15978\x17586\x18479, File Type: data, Stream Size: 1216

General	
Stream Path:	\x18496\x16191\x17783\x17516\x15978\x17586\x18479
File Type:	data
Stream Size:	1216
Entropy:	3.1068972075441508
Base64 Encoded:	False
Data ASCII:	................................,...*..........6...$........... ....B..............o..............'..............;...........>.................'.........................^........
Data Raw:	00 00 00 00 04 00 06 00 05 00 02 00 00 00 00 00 04 00 02 00 06 00 02 00 0b 00 15 00 05 00 05 00 01 00 2c 00 0a 00 01 00 13 00 02 00 0b 00 06 00 03 00 02 00 08 00 02 00 09 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 0a 00 19 00 0d 00 01 00 0e 00 01 00 03 00 01 00 1e 00 01 00 01 00 2a 00 15 00 01 00 15 00 01 00 36 00 01 00 24 00 01 00 f5 00 01 00 0f 00 01 00 04 00 09 00

Stream Path: \x18496\x16255\x16740\x16943\x18486, File Type: data, Stream Size: 38

General	
Stream Path:	\x18496\x16255\x16740\x16943\x18486
File Type:	data
Stream Size:	38
Entropy:	3.123963756721792
Base64 Encoded:	False
Data ASCII:	. . " .) . * . + . / . 5 . = . M . \\ . a . o . r . s . t . w . . . .
Data Raw:	06 00 22 00 29 00 2a 00 2b 00 2f 00 35 00 3d 00 4d 00 5c 00 61 00 6f 00 72 00 73 00 74 00 77 00 82 00 86 00 90 00

Stream Path: \x18496\x16383\x17380\x16876\x17892\x17580\x18481, File Type: data, Stream Size: 2064	
General	
Stream Path:	\x18496\x16383\x17380\x16876\x17892\x17580\x18481
File Type:	data
Stream Size:	2064
Entropy:	2.381269221109181
Base64 Encoded:	False
Data ASCII:	. . . . . " . " . " .) .) . * . * . * . + . + . / . / . / . / . / . 5 . 5 . 5 . = . = . = . = . = . M . M . M . M . M . M . M . M . \\ . \\ . a . a . a . a . a . a . a . a . o . o . r . r . r . s . s . s . t . t . w . w . w . w . w . w . . . . . # . % . ' . # . % . ' . # . % . ' . . . - . % . / . 1 . 4 7 . : . 5 . I . K . . . # . @ . C . F . . . 4 . 7 . M . O . Q . T . V .] . _ . ' . 7 . _
Data Raw:	06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 06 00 0a 00 0a 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2f 00 2f 00 2f 00 2f 00 2f 00 2f 00 35 00 35 00 35 00 3d 00 3d 00 3d 00 3d 00 3d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 4d 00 5c 00 5c 00 61 00 61 00 61 00 61 00 61 00 61 00 61 00 6f 00 6f 00 72 00 72 00 72 00 73 00 73 00 73 00 74 00

Stream Path: \x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481
File Type:	data
Stream Size:	4
Entropy:	1.5
Base64 Encoded:	False
Data ASCII:	. .
Data Raw:	e1 00 e2 00

Stream Path: \x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48	
General	
Stream Path:	\x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	48
Entropy:	3.0684210940655055
Base64 Encoded:	False
Data ASCII:	. . . . . x . < .
Data Raw:	9d 00 9e 00 9f 00 a0 00 a1 00 a2 00 a3 00 a4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 78 85 dc 85 3c 8f a0 8f c8 99

Stream Path: \x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 24	
General	
Stream Path:	\x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	24
Entropy:	2.594360937770434
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	9d 00 9e 00 9f 00 a5 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 14 85

Stream Path: \x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 42	
General	
Stream Path:	\x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	42
Entropy:	2.9135675273020816
Base64 Encoded:	False
Data ASCII:	. . . . . x . . .

General	
Data Raw:	9d 00 9f 00 a0 00 a1 00 a4 00 a6 00 a7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 e8 83 78 85 dc 85 c8 99 9c 98 00 99

Stream Path: \x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486
File Type:	data
Stream Size:	4
Entropy:	1.5
Base64 Encoded:	False
Data ASCII:	. .
Data Raw:	cc 00 aa 00

Stream Path: \x18496\x16911\x17892\x17784\x18472, File Type: 386 compact demand paged pure executable, Stream Size: 16	
General	
Stream Path:	\x18496\x16911\x17892\x17784\x18472
File Type:	386 compact demand paged pure executable
Stream Size:	16
Entropy:	1.9197367178034825
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	cc 00 00 00 cd 00 00 00 02 80 01 80 00 00 00 80

Stream Path: \x18496\x16918\x17191\x18468, File Type: MIPSEB Ucode, Stream Size: 14	
General	
Stream Path:	\x18496\x16918\x17191\x18468
File Type:	MIPSEB Ucode
Stream Size:	14
Entropy:	0.946372935985442
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 80 00 00 00 80 00 00 00 00 00 00 00 00

Stream Path: \x18496\x16923\x17194\x17910\x18229, File Type: data, Stream Size: 60	
General	
Stream Path:	\x18496\x16923\x17194\x17910\x18229
File Type:	data
Stream Size:	60
Entropy:	3.5292412679834797
Base64 Encoded:	False
Data ASCII:	. . . " . % . (. . . . . # . & .) . . . ! . $. ' . * . . . . .
Data Raw:	ad 00 1f 01 22 01 25 01 28 01 ff 7f ff 7f ff 7f ff 7f ff 7f 1c 01 1c 01 1c 01 1c 01 1c 01 1d 01 20 01 23 01 26 01 29 01 1e 01 21 01 24 01 27 01 2a 01 aa 00 aa 00 aa 00 aa 00 aa 00

Stream Path: \x18496\x17163\x16689\x18229, File Type: data, Stream Size: 8	
General	
Stream Path:	\x18496\x17163\x16689\x18229
File Type:	data
Stream Size:	8
Entropy:	1.75
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	a8 00 a9 00 01 00 01 00

Stream Path: \x18496\x17165\x16949\x17894\x17778\x18492, File Type: data, Stream Size: 18	
General	
Stream Path:	\x18496\x17165\x16949\x17894\x17778\x18492
File Type:	data
Stream Size:	18
Entropy:	2.102187170949333
Base64 Encoded:	False

General	
Data ASCII:	. . . .
Data Raw:	ac 00 c7 00 c9 00 c7 00 c9 00 00 00 c8 00 ca 00 cb 00

Stream Path: \x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 216	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	216
Entropy:	4.294855551942891
Base64 Encoded:	False
Data ASCII:	. . . . x . . . . . . d @ . (p . ! y .
Data Raw:	9d 00 9e 00 9f 00 a0 00 a1 00 a3 00 a4 00 a6 00 a7 00 ae 00 b0 00 b1 00 b4 00 b6 00 b7 00 b9 00 ba 00 bb 00 bd 00 bf 00 c0 00 c2 00 c3 00 cf 00 d0 00 d1 00 d2 00 d3 00 d4 00 d5 00 d6 00 d7 00 d8 00 d9 00 db 00 df 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc 00 dc 00 dc 00 de 00 de 00 de 00 de 00 de 00 de 00 da 00 dd 00 dd 00 dd 00 dd 00 dd 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 48	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	48
Entropy:	3.110087760732172
Base64 Encoded:	False
Data ASCII:	. . . . d
Data Raw:	9d 00 9e 00 9f 00 a5 00 cf 00 d0 00 d1 00 d2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 14 85 19 80 64 80 bc 82 b0 84

Stream Path: \x18496\x17548\x17648\x17522\x17512\x18487, File Type: Dyalog APL aplcore version 171.0, Stream Size: 12	
General	
Stream Path:	\x18496\x17548\x17648\x17522\x17512\x18487
File Type:	Dyalog APL aplcore version 171.0
Stream Size:	12
Entropy:	2.292481250360578
Base64 Encoded:	False
Data ASCII:	. . . .
Data Raw:	aa 00 ab 00 ac 00 04 80 00 00 ad 00

Stream Path: \x18496\x17630\x17770\x16868\x18472, File Type: data, Stream Size: 32	
General	
Stream Path:	\x18496\x17630\x17770\x16868\x18472
File Type:	data
Stream Size:	32
Entropy:	2.198391110799899
Base64 Encoded:	False
Data ASCII:	/ . / . . . - . - . . . .
Data Raw:	2f 01 2f 01 00 00 2d 01 2d 01 00 00 00 00 00 00 01 00 00 80 02 00 00 80 00 00 00 00 19 01 18 01

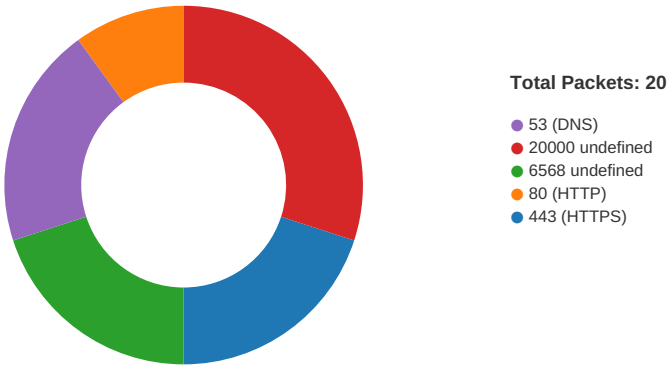
Stream Path: \x18496\x17753\x17650\x17768\x18231, File Type: data, Stream Size: 88	
General	
Stream Path:	\x18496\x17753\x17650\x17768\x18231
File Type:	data
Stream Size:	88
Entropy:	3.9470457308545095
Base64 Encoded:	False
Data ASCII:	. . . . , . / . . . . - . . . .
Data Raw:	91 00 e3 00 e5 00 e6 00 f0 00 f1 00 f3 00 f5 00 f7 00 f9 00 fb 00 fd 00 ff 00 01 01 03 01 10 01 11 01 13 01 15 01 17 01 1a 01 2c 01 2f 01 e4 00 e4 00 e4 00 ee 00 02 01 f4 00 f6 00 f8 00 fa 00 fc 00 fe 00 00 01 02 01 02 01 2e 01 12 01 14 01 16 01 2d 01 1b 01 e4 00

Stream Path: \x18496\x17932\x17910\x17458\x16778\x17207\x17522, File Type: data, Stream Size: 180	
General	
Stream Path:	\x18496\x17932\x17910\x17458\x16778\x17207\x17522
File Type:	data

General	
Stream Size:	180
Entropy:	2.754589929626484
Base64 Encoded:	False
Data ASCII:	. . . . . 3 . . 3 . 3 . . . 3 . 3 . . . . .
Data Raw:	ae 00 b0 00 b1 00 b4 00 b6 00 b7 00 b9 00 ba 00 bb 00 bd 00 bf 00 c0 00 c2 00 c3 00 c5 00 01 80 33 80 01 80 01 80 33 80 01 8c 33 80 01 8c 01 80 01 80 33 80 01 8c 33 80 01 8c 01 80 a9 00 b1 00 a9 00 a9 00 b7 00 a9 00 ba 00 a9 00 a9 00 a9 00 c0 00 a9 00 c3 00 a9 00 a9 00 af 00 b2 00 b3 00 b5 00 b2 00 b8 00 b2 00 b3 00 bc 00 be 00 b2 00 c1 00 b2 00 c4 00 c6 00 00 00 00 00 00 00 00 00

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 18:23:17.955034971 CEST	49175	443	192.168.2.22	195.181.174.167
Aug 5, 2022 18:23:17.955077887 CEST	443	49175	195.181.174.167	192.168.2.22
Aug 5, 2022 18:23:17.955163002 CEST	49175	443	192.168.2.22	195.181.174.167
Aug 5, 2022 18:23:17.956656933 CEST	49175	443	192.168.2.22	195.181.174.167
Aug 5, 2022 18:23:17.956707001 CEST	443	49175	195.181.174.167	192.168.2.22
Aug 5, 2022 18:23:17.956804037 CEST	49175	443	192.168.2.22	195.181.174.167
Aug 5, 2022 18:23:18.078598976 CEST	49176	80	192.168.2.22	92.223.88.41
Aug 5, 2022 18:23:18.109005928 CEST	80	49176	92.223.88.41	192.168.2.22
Aug 5, 2022 18:23:18.109520912 CEST	49176	80	192.168.2.22	92.223.88.41
Aug 5, 2022 18:23:18.117553949 CEST	49177	6568	192.168.2.22	195.181.174.174
Aug 5, 2022 18:23:18.136924982 CEST	6568	49177	195.181.174.174	192.168.2.22
Aug 5, 2022 18:23:18.137054920 CEST	49177	6568	192.168.2.22	195.181.174.174
Aug 5, 2022 18:23:18.137501955 CEST	49177	6568	192.168.2.22	195.181.174.174
Aug 5, 2022 18:23:18.158116102 CEST	6568	49177	195.181.174.174	192.168.2.22
Aug 5, 2022 18:23:18.158333063 CEST	49177	6568	192.168.2.22	195.181.174.174
Aug 5, 2022 18:23:45.921768904 CEST	49178	20000	192.168.2.22	80.209.241.3
Aug 5, 2022 18:23:46.016635895 CEST	20000	49178	80.209.241.3	192.168.2.22
Aug 5, 2022 18:23:46.019696951 CEST	49178	20000	192.168.2.22	80.209.241.3
Aug 5, 2022 18:23:46.019758940 CEST	49178	20000	192.168.2.22	80.209.241.3
Aug 5, 2022 18:23:46.153834105 CEST	20000	49178	80.209.241.3	192.168.2.22
Aug 5, 2022 18:23:46.159286976 CEST	49178	20000	192.168.2.22	80.209.241.3
Aug 5, 2022 18:23:46.294455051 CEST	20000	49178	80.209.241.3	192.168.2.22
Aug 5, 2022 18:23:46.294933081 CEST	20000	49178	80.209.241.3	192.168.2.22
Aug 5, 2022 18:23:46.295002937 CEST	20000	49178	80.209.241.3	192.168.2.22
Aug 5, 2022 18:23:46.299264908 CEST	49178	20000	192.168.2.22	80.209.241.3
Aug 5, 2022 18:23:47.520963907 CEST	49178	20000	192.168.2.22	80.209.241.3
Aug 5, 2022 18:23:47.615866899 CEST	20000	49178	80.209.241.3	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 18:23:17.905138016 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 5, 2022 18:23:17.924896002 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 5, 2022 18:23:17.925493956 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 5, 2022 18:23:17.944211960 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 5, 2022 18:23:18.053093910 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 5, 2022 18:23:18.075155973 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 5, 2022 18:23:18.088778019 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 5, 2022 18:23:18.109394073 CEST	53	58836	8.8.8.8	192.168.2.22

DNS Queries

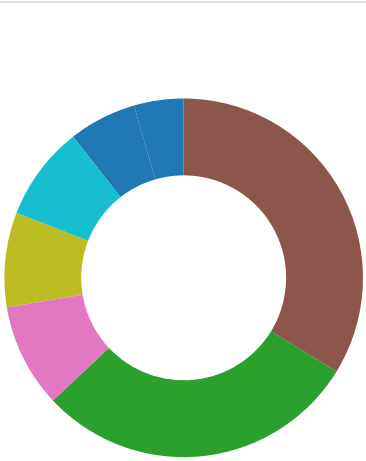
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 18:23:17.905138016 CEST	192.168.2.22	8.8.8.8	0x8710	Standard query (0)	boot.net.anydesk.com	A (IP address)	IN (0x0001)
Aug 5, 2022 18:23:17.925493956 CEST	192.168.2.22	8.8.8.8	0x8710	Standard query (0)	boot.net.anydesk.com	A (IP address)	IN (0x0001)
Aug 5, 2022 18:23:18.053093910 CEST	192.168.2.22	8.8.8.8	0xcfca	Standard query (0)	boot.net.anydesk.com	A (IP address)	IN (0x0001)
Aug 5, 2022 18:23:18.088778019 CEST	192.168.2.22	8.8.8.8	0x5d9d	Standard query (0)	boot.net.anydesk.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 18:23:17.924896002 CEST	8.8.8.8	192.168.2.22	0x8710	No error (0)	boot.net.anydesk.com		92.223.88.41	A (IP address)	IN (0x0001)
Aug 5, 2022 18:23:17.944211960 CEST	8.8.8.8	192.168.2.22	0x8710	No error (0)	boot.net.anydesk.com		195.181.174.167	A (IP address)	IN (0x0001)
Aug 5, 2022 18:23:18.075155973 CEST	8.8.8.8	192.168.2.22	0xcfca	No error (0)	boot.net.anydesk.com		92.223.88.41	A (IP address)	IN (0x0001)
Aug 5, 2022 18:23:18.109394073 CEST	8.8.8.8	192.168.2.22	0x5d9d	No error (0)	boot.net.anydesk.com		195.181.174.174	A (IP address)	IN (0x0001)

Statistics

Behavior



- msiexec.exe
- msiexec.exe
- VSSVC.exe
- svchost.exe
- msiexec.exe
- msiexec.exe
- icacls.exe
- expand.exe
- install.exe
- cmd.exe
- rdpdr.sys
- tdtcp.sys
- anydesk.exe
- tssecsrv.sys
- rdpwd.sys
- AnyDesk.exe
- AnyDesk.exe
- cmd.exe
- cmd.exe
- AnyDesk.exe
- AnyDesk.exe
- netsh.exe
- icacls.exe
- cmd.exe

Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 2996, Parent PID: 2628

General

Target ID:	1
Start time:	18:22:14
Start date:	05/08/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\1.msi"
Imagebase:	0xff1c0000
File size:	128512 bytes
MD5 hash:	AC2E7152124CEED36846BD1B6592A00F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 1184, Parent PID: 404

General

Target ID:	2
Start time:	18:22:15
Start date:	05/08/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0xff1c0000
File size:	128512 bytes
MD5 hash:	AC2E7152124CEED36846BD1B6592A00F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: VSSVC.exe PID: **1232**, Parent PID: **404**

General

Target ID:	3
Start time:	18:22:16
Start date:	05/08/2022
Path:	C:\Windows\System32\VSSVC.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\vssvc.exe
Imagebase:	0xff910000
File size:	1600512 bytes
MD5 hash:	B60BA0BC31B0CB414593E169F6F21CC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **2224**, Parent PID: **404**

General

Target ID:	4
Start time:	18:22:16
Start date:	05/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k swprv
Imagebase:	0xff7d0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msiexec.exe PID: **2876**, Parent PID: **1184**

General

Target ID:	5
Start time:	18:22:57
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 6381DE7DB6BAADD41D0E24C26E59EDFC
Imagebase:	0xd00000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **1704**, Parent PID: **1184**

General

Target ID:	6
Start time:	18:23:03
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 22388C515E15FC158EA4B11229C0F8D9 E Global\MSI0000
Imagebase:	0xd00000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: **1820**, Parent PID: **1704**

General	
Target ID:	7
Start time:	18:23:04
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\." /SETINTEGRITYLEVEL (CI)(OI)HIGH
Imagebase:	0x5b0000
File size:	27136 bytes
MD5 hash:	1542A92D5C6F7E1E80613F3466C9CE7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: expand.exe PID: **672**, Parent PID: **1704**

General	
Target ID:	9
Start time:	18:23:06
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\expand.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
Imagebase:	0xf70000
File size:	53248 bytes
MD5 hash:	659CED6D7BDA047BCC6048384231DB9F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: install.exe PID: **2440**, Parent PID: **1704**

General	
Target ID:	11
Start time:	18:23:11
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files\install.exe"
Imagebase:	0x400000
File size:	3837440 bytes
MD5 hash:	8C42AB81F90EE0592F7A709F0F7E320B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\log1.txt	append data or add subdirectory or create pipe instance | read attributes | synchronize	device | sparse file	synchronous io non alert | non directory file	success or wait	1	401146	CreateFileA
c:\programdata\anydesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401266	CreateDirectoryA
c:\programdata\anydesk.exe	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4012B7	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\programdata\anydesk.exe	0	3829888	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 1c fd 68 fd 7d fd 3b fd 7d fd 3b fd 7d fd 3b fd 0b 22 3b fd 7d fd 3b fd 0b 23 3b fd 7d fd 3b fd fd 13 3b fd 7d fd 3b fd 0b 14 3b fd 7d fd 3b 52 69 63 68 fd 7d fd 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd 31 62 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 0a 00 00 2a 00 00 00 0a 3a 00 00 5e fd 00 fd 1c 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$h}:};}:"};#;} ;:};:};Rich};PEL1b"*:^	success or wait	1	4012CE	WriteFile
C:\Windows\SysWOW64\log1.txt	0	13	61 6e 79 64 65 73 6b 2d 49 44 3a 0d 0a	anydesk-ID:	success or wait	1	4012EF	WriteFile
C:\Windows\SysWOW64\log1.txt	13	1	30	0	success or wait	1	4013B8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	unknown	1023	success or wait	1	401395	ReadFile
\pipe	unknown	1023	success or wait	1	401395	ReadFile
C:\Windows\SysWOW64\log1.txt	unknown	14	success or wait	1	401479	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe	success or wait	1	4018D1	RegCreateKeyA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Magnify.exe	success or wait	1	401948	RegCreateKeyA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HelpPane.exe	success or wait	1	4019BF	RegCreateKeyA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe	success or wait	1	401A36	RegCreateKeyA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT \CurrentVersion\Winlogon\SpecialAccounts	success or wait	1	401A9B	RegCreateKeyA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT \CurrentVersion\Winlogon\SpecialAccounts\UserList	success or wait	1	401A9B	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe	Debugger	unicode	c:\windows\system32\cmd.exe	success or wait	1	4018F5	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Magnify.exe	Debugger	unicode	c:\windows\system32\cmd.exe	success or wait	1	40196C	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HelpPane.exe	Debugger	unicode	c:\windows\system32\cmd.exe	success or wait	1	4019E3	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe	Debugger	unicode	c:\windows\system32\cmd.exe	success or wait	1	401A5A	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT \CurrentVersion\Winlogon\SpecialAccounts\UserList	Administartor	dword	0	success or wait	1	401ABF	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server	fDenyTSConnections	dword	1	0	success or wait	1	40187E	RegSetValueExA

Analysis Process: cmd.exe PID: **1404**, Parent PID: **2440**

General

Target ID:	12
Start time:	18:23:16
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent
Imagebase:	0x4a350000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rdpdr.sys PID: 4, Parent PID: -1

General

Target ID:	13
Start time:	18:23:16
Start date:	05/08/2022
Path:	C:\Windows\System32\drivers\rdpdr.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	165888 bytes
MD5 hash:	1B6163C503398B23FF8B939C67747683
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	success or wait	1	FFFFF80002AD46D3	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	success or wait	1	FFFFF80002AD46D3	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	success or wait	16	FFFFF80002AD46D3	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	success or wait	16	FFFFF80002AD46D3	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{091BC97E-2352-4362-A539-10A6D8FF7596}	success or wait	1	FFFFF80002AD46D3	NtCreateKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{091BC97E-2352-4362-A539-10A6D8FF7596}\Properties	success or wait	1	FFFFF80002AD46D3	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	Class	unicode	RDPDR	success or wait	1	FFFFF80002AD46D3	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	NoDisplayClass	unicode	1	success or wait	1	FFFFF80002AD46D3	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}	NoUseClass	unicode	1	success or wait	1	FFFFF80002AD46D3	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	Security	binary	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 1C 00 01 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 14 00 00 00	success or wait	1	FFFFF80002AD46D3	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{091BC97E-2352-4362-A539-10A6D8FF7596}	Class	unicode	RDPDR	success or wait	1	FFFFF80002AD46D3	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{091BC97E-2352-4362-A539-10A6D8FF7596}	NoDisplayClass	unicode	1	success or wait	1	FFFFF80002AD46D3	NtSetValueKey
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{091BC97E-2352-4362-A539-10A6D8FF7596}	NoUseClass	unicode	1	success or wait	1	FFFFF80002AD46D3	NtSetValueKey

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{091BC97E-2352-4362-A539-10A6D8FF7596}\Properties	Security	binary	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 1C 00 01 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 12 00 00 00	success or wait	1	FFFFF80002AD46D3	NtSetValueKey

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{CC41EBA2-AB57-4F4E-8C3D-1BC33B1E74E3}\Properties	Security	binary	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 1C 00 01 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 14 00 00 00	01 00 0C 90 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 02 00 30 00 02 00 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 14 00 00 00 00 00 14 00 00 00 00 10 01 01 00 00 00 00 00 05 12 00 00 00	success or wait	1	FFFFF80002AD46D3	NtSetValueKey

Analysis Process: tdtcp.sys PID: **4**, Parent PID: **-1**

General

Target ID:	15
Start time:	18:23:17
Start date:	05/08/2022
Path:	C:\Windows\System32\drivers\tdtcp.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	23552 bytes
MD5 hash:	51C5ECEB1CDEE2468A1748BE550CFBC8
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: anydesk.exe PID: **2640**, Parent PID: **1404**

General

Target ID:	16
Start time:	18:23:18
Start date:	05/08/2022
Path:	C:\ProgramData\anydesk.exe
Wow64 process (32bit):	true
Commandline:	c:\programdata\anydesk.exe --install C:\ProgramData\AnyDesk --silent
Imagebase:	0x1040000
File size:	3829888 bytes
MD5 hash:	1BC5890C9E7BF54B7712E344B0AF9D04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	149BAF0	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1499BAA	CreateFileW
C:\ProgramData\AnyDesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	124B11E	CreateDirectoryW
C:\ProgramData\AnyDesk\AnyDesk.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	124C37A	CopyFileW
C:\ProgramData\AnyDesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	124B44F	SHCreateDirectoryExW
C:\ProgramData\AnyDesk\system.conf	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	3	14B5ED6	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	0	38	20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 0d 0a	* * * * * * * * * * * * * * * * * *	success or wait	1	1499FF0	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	38	126	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 41 6e 79 44 65 73 6b 20 57 69 6e 64 6f 77 73 20 53 74 61 72 74 75 70 20 2a 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 main - * AnyDesk Windows Startup *	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	164	175	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 56 65 72 73 69 6f 6e 20 37 2e 30 2e 37 20 28 72 65 6c 65 61 73 65 2f 77 69 6e 5f 37 2e 30 2e 78 20 39 36 66 38 64 38 30 65 61 63 32 37 33 61 39 31 34 34 61 62 63 63 65 32 66 36 36 64 62 63 32 32 30 30 63 63 38 31 64 29 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 main - * Version 7.0.7 (release/win_7.0.x 96f8d80eac273a9144 abccce2f66dbc2200cc81 d)	success or wait	1	1499EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	339	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 43 75 73 74 6f 6d 20 43 6c 69 65 6e 74 20 28 6e 6f 20 49 44 29 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 main - * Custom Client (no ID)	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	461	99	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 main -	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	560	164	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 50 72 6f 63 65 73 73 20 73 74 61 72 74 65 64 20 61 74 20 32 30 32 32 2d 30 38 2d 30 36 2e 20 50 49 44 20 32 36 34 30 2e 20 4f 53 20 69 73 20 57 69 6e 64 6f 77 73 20 37 20 28 36 34 20 62 69 74 29 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 main - Process started at 2022-08-06. PID 2640. OS is Windows 7 (64 bit)	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	724	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6d 70 6c 5f 73 65 6c 65 63 74 6f 72 20 2d 20 75 73 69 6e 67 20 73 73 65 32 20 28 69 6e 74 72 69 6e 73 69 63 73 29 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 impl_selector - using sse2 (intrinsics)	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	846	109	77 61 72 6e 69 6e 67 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 65 72 6d 69 6e 61 74 6f 72 20 2d 20 41 6c 6c 20 63 6c 65 61 72 21 0d 0a	warning 2022-08-06 01:23:23.745 installer 2640 2428 terminator - All clear!	success or wait	1	1499EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	955	135	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 65 72 2e 69 6e 73 74 61 6c 6c 65 72 20 2d 20 49 6e 73 74 61 6c 6c 69 6e 67 20 41 6e 79 44 65 73 6b 20 6f 6e 20 74 68 69 73 20 63 6f 6d 70 75 74 65 72 2e 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 installer.installer - Installing AnyDesk on t his computer.	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	1090	120	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 53 74 6f 70 70 69 6e 67 20 74 68 65 20 73 65 72 76 69 63 65 2e 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 installation.svc_installer - Stopping the service.	success or wait	2	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	1210	144	20 20 65 72 72 6f 72 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 67 65 74 20 61 20 68 61 6e 64 6c 65 20 74 6f 20 74 68 65 20 73 65 72 76 69 63 65 20 28 31 30 36 30 29 2e 0d 0a	error 2022-08-06 01:23:23.745 installer 2640 2428 installation.svc_installer - Could not get a handle to the service (1060).	success or wait	2	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	1627	133	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 33 2e 37 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 65 72 2e 69 6e 73 74 61 6c 6c 65 72 20 2d 20 50 72 65 76 69 6f 75 73 20 76 65 72 73 69 6f 6e 20 6f 66 20 41 6e 79 44 65 73 6b 20 66 6f 75 6e 64 2e 0d 0a	info 2022-08-06 01:23:23.745 installer 2640 2428 installer.installer - Previous version of Any Desk found.	success or wait	1	1499EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\anydesk\AnyDesk.exe	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 1c fd 68 fd 7d fd 3b fd 7d fd 3b fd 7d fd 3b fd 0b 22 3b fd 7d fd 3b fd 0b 23 3b fd 7d fd 3b fd fd 13 3b fd 7d fd 3b fd 0b 14 3b fd 7d fd 3b 52 69 63 68 fd 7d fd 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd fd 31 62 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 0a 00 00 2a 00 00 00 0a 3a 00 00 5e fd 00 fd 1c 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$h};};};";};#;};;};;};Rich};PEL1b"*:^	success or wait	59	124C37A	CopyFileW
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	1760	124	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 34 30 30 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 55 6e 69 6e 73 74 61 6c 6c 69 6e 67 20 74 68 65 20 73 65 72 76 69 63 65 2e 0d 0a	info 2022-08-06 01:23:24.400 installer 2640 2428 installation.svc_installer - Uninstalling the service.	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	1884	144	20 20 65 72 72 6f 72 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 34 30 30 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 67 65 74 20 61 20 68 61 6e 64 6c 65 20 74 6f 20 74 68 65 20 73 65 72 76 69 63 65 20 28 31 30 36 30 29 2e 0d 0a	error 2022-08-06 01:23:24.400 installer 2640 2428 installation.svc_installer - Could not get a handle to the service (1060).	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	2028	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 34 30 30 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 49 6e 73 74 61 6c 6c 69 6e 67 20 74 68 65 20 73 65 72 76 69 63 65 2e 0d 0a	info 2022-08-06 01:23:24.400 installer 2640 2428 installation.svc_installer - Installing the service.	success or wait	1	1499EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	2150	179	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 34 34 37 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 54 68 65 20 73 65 72 76 69 63 65 20 68 61 73 20 62 65 65 6e 20 69 6e 73 74 61 6c 6c 65 64 20 28 22 43 3a 5c 50 72 6f 67 72 61 6d 44 61 74 61 5c 41 6e 79 44 65 73 6b 5c 41 6e 79 44 65 73 6b 2e 65 78 65 22 20 2d 2d 73 65 72 76 69 63 65 29 2e 0d 0a	info 2022-08-06 01:23:24.447 installer 2640 2428 installation.svc_installer - The service has been installed ("C:\ProgramData\AnyDesk\AnyDesk.exe" --service).	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	2329	139	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 34 34 37 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 65 72 2e 69 6e 73 74 61 6c 6c 65 72 20 2d 20 43 6f 70 79 69 6e 67 20 74 68 65 20 73 65 74 74 69 6e 67 73 20 28 6e 65 77 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 29 2e 0d 0a	info 2022-08-06 01:23:24.447 installer 2640 2428 installer.installer - Copying the settings (new installation).	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	2468	133	20 20 65 72 72 6f 72 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 34 34 37 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 65 72 2e 69 6e 73 74 61 6c 6c 65 72 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 63 6f 70 79 20 73 65 72 76 69 63 65 20 63 6f 6e 66 69 67 20 28 33 29 2e 0d 0a	error 2022-08-06 01:23:24.447 installer 2640 2428 installer.installer - Could not copy service config (3).	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	2601	132	20 20 65 72 72 6f 72 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 34 34 37 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 65 72 2e 69 6e 73 74 61 6c 6c 65 72 20 2d 20 43 6f 75 6c 64 20 6e 6f 74 20 63 6f 70 79 20 73 79 73 74 65 6d 20 63 6f 6e 66 69 67 20 28 33 29 2e 0d 0a	error 2022-08-06 01:23:24.447 installer 2640 2428 installer.installer - Could not copy system config (3).	success or wait	1	1499EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	2733	133	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 38 35 33 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 65 72 2e 69 6e 73 74 61 6c 6c 65 72 20 2d 20 49 6e 73 74 61 6c 6c 20 73 74 61 74 75 73 3a 20 6e 6f 74 20 69 6e 73 74 61 6c 6c 65 64 20 28 3c 34 29 0d 0a	info 2022-08-06 01:23:24.853 installer 2640 2428 installer.installer - Install status: not installed (<4)	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	2866	145	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 34 2e 38 35 33 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 65 72 2e 69 6e 73 74 61 6c 6c 65 72 20 2d 20 55 70 64 61 74 69 6e 67 20 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 66 6f 72 20 61 75 74 6f 2d 75 70 64 61 74 65 20 28 30 2c 20 30 29 2e 0d 0a	info 2022-08-06 01:23:24.853 installer 2640 2428 installer.installer - Updating configuration for auto-update (0, 0).	success or wait	1	1499EC5	WriteFile
C:\ProgramData\anydesk\system.conf	0	34	61 64 2e 61 6e 79 6e 65 74 2e 66 70 72 3d 61 64 38 66 65 63 36 63 65 32 65 61 39 35 38 37 33 30 39 63	ad.anynet.fpr=ad8fec6ce2ea9587309c	success or wait	2	14A3D3E	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	3011	120	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 35 2e 35 30 38 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 53 74 61 72 74 69 6e 67 20 74 68 65 20 73 65 72 76 69 63 65 2e 0d 0a	info 2022-08-06 01:23:25.508 installer 2640 2428 installation.svc_installer - Starting the service.	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	3131	115	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 38 2e 37 35 33 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 53 65 72 76 69 63 65 20 73 74 61 72 74 65 64 2e 0d 0a	info 2022-08-06 01:23:28.753 installer 2640 2428 installation.svc_installer - Service started.	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	3246	119	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 32 38 2e 37 35 33 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 57 61 69 74 69 6e 67 20 66 6f 72 20 73 65 72 76 69 63 65 2e 0d 0a	info 2022-08-06 01:23:28.753 installer 2640 2428 installation.svc_installer - Waiting for service.	success or wait	1	1499EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	3365	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 33 31 2e 35 34 35 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 2e 73 76 63 5f 69 6e 73 74 61 6c 6c 65 72 20 2d 20 54 68 65 20 73 65 72 76 69 63 65 20 69 73 20 72 75 6e 6e 69 6e 67 2e 0d 0a	info 2022-08-06 01:23:31.545 installer 2640 2428 installation.svc_installer - The service is running.	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	3487	121	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 38 3a 33 33 2e 31 39 38 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 66 69 6e 69 73 68 65 64 2e 0d 0a	info 2022-08-06 01:28:33.198 installer 2640 2428 installer.installer - Installation finished.	success or wait	1	1499EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	3608	110	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 39 3a 33 33 2e 31 34 34 20 20 69 6e 73 74 61 6c 6c 65 72 20 20 20 32 36 34 30 20 20 20 32 34 32 38 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 54 65 72 6d 69 6e 61 74 65 64 2e 0d 0a	info 2022-08-06 01:29:33.144 installer 2640 2428 main - Terminated.	success or wait	1	1499EC5	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	success or wait	1	124A385	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.anydesk	success or wait	1	124FAE9	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.anydesk\DefaultIcon	success or wait	1	124FB59	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.anydesk\shell	success or wait	1	124FBF3	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.anydesk\shell\open	success or wait	1	124FC4A	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.anydesk\shell\open\command	success or wait	1	124FC95	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk	success or wait	1	124F804	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk\Capabilities	success or wait	1	124F835	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk\Capabilities\FileAssociations	success or wait	1	124F8B7	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk	success or wait	1	1251BDF	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk\DefaultIcon	success or wait	1	1251C6A	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk\shell	success or wait	1	1251CDF	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk\shell\open	success or wait	1	1251D0E	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk\shell\open\command	success or wait	1	1251D47	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	DisplayIcon	unicode	"C:\ProgramData\AnyDesk\AnyDesk.exe"	success or wait	1	124A489	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	DisplayName	unicode	AnyDesk	success or wait	1	124A4AF	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	DisplayVersion	unicode	ad 7.0.7	success or wait	1	124A516	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	EstimatedSize	dword	2048	success or wait	1	124A575	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	HelpLink	unicode	https://help.anydesk.com/	success or wait	1	124A5A7	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	InstallLocation	unicode	"C:\ProgramData\AnyDesk"	success or wait	1	124A612	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	Publisher	unicode	AnyDesk Software GmbH	success or wait	1	124A683	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	UninstallString	unicode	"C:\ProgramData\AnyDesk\AnyDesk.exe" --uninstall	success or wait	1	124A6BF	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	VersionMajor	dword	7	success or wait	1	124A6ED	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	VersionMinor	dword	0	success or wait	1	124A70E	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	VersionBuild	dword	7	success or wait	1	124A72F	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	VersionTimestamp	B	E0 A8 C2 E8 63 12 00 00	success or wait	1	124A752	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\AnyDesk	WindowsInstaller	dword	0	success or wait	1	124A773	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.anydesk\DefaultIcon	NULL	unicode	"C:\ProgramData\AnyDesk\AnyDesk.exe",0	success or wait	1	124FBC0	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.anydesk\shell\open\command	NULL	unicode	"C:\ProgramData\AnyDesk\AnyDesk.exe" --play "%1"	success or wait	1	124FCEE	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk\Capabilities	ApplicationDescription	unicode	AnyDesk	success or wait	1	124F86C	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk\Capabilities	ApplicationName	unicode	AnyDesk	success or wait	1	124F891	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Media\AnyDesk\Capabilities\FileAssociations	.anydesk	unicode	AnyDesk.anydesk	success or wait	1	124F8FB	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications	AnyDesk	unicode	SOFTWARE\Clients\Media\AnyDesk\Capabilities	success or wait	1	124F9A8	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk	NULL	unicode	URL:AnyDesk Protocol	success or wait	1	1251C17	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk	URL Protocol	unicode		success or wait	1	1251C40	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk\DefaultIcon	NULL	unicode	AnyDesk.exe,0	success or wait	1	1251CAC	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AnyDesk\shell\open\command	NULL	unicode	"C:\ProgramData\AnyDesk\AnyDesk.exe" "%1"	success or wait	1	1251DAE	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: tssecsrv.sys PID: **4**, Parent PID: **-1**

General

Target ID:	17
Start time:	18:23:18
Start date:	05/08/2022
Path:	C:\Windows\System32\drivers\tssecsrv.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	39936 bytes
MD5 hash:	19BEDA57F3E0A06B8D5EB6D619BD5624
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: rdpwd.sys PID: **4**, Parent PID: **-1**

General

Target ID:	18
Start time:	18:23:18
Start date:	05/08/2022
Path:	C:\Windows\System32\drivers\rdpwd.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	212480 bytes
MD5 hash:	FE571E088C2D83619D2D48D4E961BF41
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: AnyDesk.exe PID: **2556**, Parent PID: **404**

General

Target ID:	20
Start time:	18:23:25
Start date:	05/08/2022
Path:	C:\ProgramData\anydesk\AnyDesk.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\AnyDesk\AnyDesk.exe" --service

Imagebase:	0x12a0000
File size:	3829888 bytes
MD5 hash:	1BC5890C9E7BF54B7712E344B0AF9D04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 2%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\AnyDesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	16FBAF0	CreateDirectoryW
C:\ProgramData\AnyDesk\ad_svc.trace	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	16F9BAA	CreateFileW
C:\ProgramData\AnyDesk\service.conf	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	1715ED6	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	38	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9FF0	WriteFile
unknown	38	126	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	164	175	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	339	122	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	461	142	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	603	121	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	724	143	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	867	99	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	966	164	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	1130	122	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	1252	125	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	1377	126	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	1503	117	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	1620	206	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	1826	107	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\anydesk\system.conf	0	343	61 64 2e 61 6e 79 6e 65 74 2e 66 70 72 3d 61 64 38 66 65 63 36 63 65 32 65 61 39 35 38 37 33 30 39 63 35 30 62 39 37 31 37 35 64 38 65 64 36 33 39 61 39 66 30 39 0a 61 64 2e 61 6e 79 6e 65 74 2e 72 65 6c 61 79 2e 66 61 74 61 6c 5f 72 65 73 75 6c 74 3d 31 2e 30 0a 61 64 2e 61 6e 79 6e 65 74 2e 72 65 6c 61 79 2e 73 74 61 74 65 3d 30 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 5f 66 69 6c 65 73 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 5f 76 65 72 73 69 6f 6e 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 70 65 72 6d 69 73 73 69 6f 6e 5f 70 72 6f 66 69 6c 65	ad.anynet.fpr=ad8fec6ce2ea9587 309c50b97175d8ed639a9f09ad.any net.relay.fatal_result=1.0ad.a nynet.relay.state=0ad.security .frontend_clipboard=1ad.securi ty.frontend_clipboard_files=1a d.security.frontend_clipboard_ version=1ad.security.permission_profile	success or wait	1	1703D3E	WriteFile
unknown	1933	132	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2065	121	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2186	117	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2303	125	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2428	110	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2538	130	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2668	139	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2807	122	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	2929	136	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
C:\ProgramData\anydesk\service.conf	0	1748	61 64 2e 61 6e 79 6e 65 74 2e 63 65 72 74 3d 2d 2d 2d 2d 2d 42 45 47 49 4e 20 43 45 52 54 49 46 49 43 41 54 45 2d 2d 2d 2d 2d 5c 6e 4d 49 49 43 71 44 43 43 41 5a 41 43 41 51 45 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 4c 42 51 41 77 47 54 45 58 4d 42 55 47 41 31 55 45 41 77 77 4f 51 57 35 35 52 47 56 7a 61 79 42 44 5c 6e 62 47 6c 6c 62 6e 51 77 49 42 63 4e 4d 6a 49 77 4f 44 41 32 4d 44 45 79 4d 7a 4d 77 57 68 67 50 4d 6a 41 33 4d 6a 41 33 4d 6a 51 77 4d 54 49 7a 4d 7a 42 61 4d 42 6b 78 46 7a 41 56 42 67 4e 56 5c 6e 42 41 4d 4d 44 6b 46 75 65 55 52 6c 63 32 73 67 51 32 78 70 5a 57 35 30 4d 49 49 42 49 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 67 4b 43 5c 6e 41 51 45 41 33 6d 39 73 30 58 74 31 74	ad.anynet.cert=----- BEGIN CERTIFICATE----- \nMIICqDCCAZACAQEwDQYJKoZIhvcNAQELBQAwGTEXMBUGA1UEAwwOQW55RGVzayBD\nbGllbnQwIBcNMjIwODA2MDEyMzMwWhgPMjA3MjA3MjQwMTIzMzBaMBkxFzAVBgNV\nBAMMDkFueURlc2sgQ2xpZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC\nAQEA3m9s0Xt1t	success or wait	2	1703D3E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\anydesk\system.conf	0	398	61 64 2e 61 6e 79 6e 65 74 2e 66 70 72 3d 61 64 38 66 65 63 36 63 65 32 65 61 39 35 38 37 33 30 39 63 35 30 62 39 37 31 37 35 64 38 65 64 36 33 39 61 39 66 30 39 0a 61 64 2e 61 6e 79 6e 65 74 2e 72 65 6c 61 79 2e 66 61 74 61 6c 5f 72 65 73 75 6c 74 3d 31 2e 30 0a 61 64 2e 61 6e 79 6e 65 74 2e 72 65 6c 61 79 2e 73 74 61 74 65 3d 30 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 5f 66 69 6c 65 73 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 5f 76 65 72 73 69 6f 6e 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 70 65 72 6d 69 73 73 69 6f 6e 5f 70 72 6f 66 69 6c 65	ad.anynet.fpr=ad8fec6ce2ea9587 309c50b97175d8ed639a9f09ad.any net.relay.fatal_result=1.0 ad.a nynet.relay.state=0ad.security .frontend_clipboard=1ad.securi ty.frontend_clipboard_files=1a d.security.frontend_clipboard_ version=1ad.security.permission_profile	success or wait	5	1703D3E	WriteFile
unknown	3065	126	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	3191	121	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	3312	121	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	3433	119	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	3552	121	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	16F9EC5	WriteFile
unknown	3673	129	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	3923	125	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4048	208	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4256	118	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4374	120	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4494	133	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	16F9EC5	WriteFile
unknown	4760	120	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4880	133	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	5013	130	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	5143	141	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	16F9EC5	WriteFile
unknown	5425	153	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	16F9EC5	WriteFile
unknown	5864	126	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	5990	139	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6129	120	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6249	132	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6381	132	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6513	123	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6636	118	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6754	139	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6893	139	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	7032	122	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	7154	145	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	7299	163	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	16F9EC5	WriteFile
unknown	7785	115	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	7900	188	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	8088	126	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	16F9EC5	WriteFile
unknown	8214	133	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	16F9EC5	WriteFile
unknown	8862	158	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	9020	123	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	9143	131	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	16F9EC5	WriteFile
unknown	9274	118	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	16F9EC5	WriteFile
unknown	9525	129	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	16F9EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	9654	129	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	16F9EC5	WriteFile
unknown	9783	122	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	16F9EC5	WriteFile
unknown	9905	129	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	11078	117	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	11195	135	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	11330	113	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	11443	119	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	16F9EC5	WriteFile
unknown	11562	116	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	16F9EC5	WriteFile
unknown	11797	118	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	16F9EC5	WriteFile
unknown	12433	169	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	12602	133	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	12735	157	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\anydesk\system.conf	unknown	60	success or wait	1	170402C	ReadFile
C:\ProgramData\anydesk\system.conf	unknown	343	success or wait	1	170402C	ReadFile
C:\ProgramData\anydesk\service.conf	unknown	2762	success or wait	2	170402C	ReadFile
C:\ProgramData\anydesk\system.conf	unknown	455	success or wait	6	170402C	ReadFile

Analysis Process: AnyDesk.exe PID: **2336**, Parent PID: **1860**

General

Target ID:	21
Start time:	18:23:32
Start date:	05/08/2022
Path:	C:\ProgramData\anydesk\AnyDesk.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\AnyDesk\AnyDesk.exe" --control
Imagebase:	0x12a0000
File size:	3829888 bytes
MD5 hash:	1BC5890C9E7BF54B7712E344B0AF9D04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	16FBAF0	CreateDirectoryW
C:\Users\user\AppData\Roaming\AnyDesk\user.conf	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	5	1715ED6	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	3718	38	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9FF0	WriteFile
unknown	3756	126	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	3882	175	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4057	122	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4179	99	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4278	164	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4442	122	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4564	125	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	4689	126	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4815	123	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	4938	128	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\user.conf	0	14	61 64 2e 69 6e 76 69 74 65 2e 63 72 65 61	ad.invite.crea	success or wait	3	1703D3E	WriteFile
unknown	5066	109	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	5175	116	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	5291	105	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	5396	118	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	5881	120	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6128	120	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile
unknown	6387	116	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	16F9EC5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\user.conf	unknown	1003	success or wait	2	170402C	ReadFile
C:\ProgramData\anydesk\system.conf	unknown	455	success or wait	2	170402C	ReadFile

Analysis Process: cmd.exe PID: **2544**, Parent PID: **2440**

General

Target ID:	22
Start time:	18:23:41
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c echo 31121985west|c:\programdata\anydesk\anydesk.exe --set-password
Imagebase:	0x4a0e0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **2548**, Parent PID: **2544**

General

Target ID:	24
Start time:	18:23:42
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo 31121985west"
Imagebase:	0x4a0e0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AnyDesk.exe PID: **2856**, Parent PID: **2544**

General

Target ID:	25
Start time:	18:23:42
Start date:	05/08/2022
Path:	C:\ProgramData\anydesk\AnyDesk.exe
Wow64 process (32bit):	true
Commandline:	c:\programdata\anydesk\anydesk.exe --set-password
Imagebase:	0x12a0000
File size:	3829888 bytes
MD5 hash:	1BC5890C9E7BF54B7712E344B0AF9D04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	16FBAF0	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	6763	38	20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 0d 0a	* * * * * * * * * * * * * * * * * *	success or wait	1	16F9FF0	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	6801	126	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 41 6e 79 44 65 73 6b 20 57 69 6e 64 6f 77 73 20 53 74 61 72 74 75 70 20 2a 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 main - * AnyDesk Windows Startup *	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	6927	175	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 56 65 72 73 69 6f 6e 20 37 2e 30 2e 37 20 28 72 65 6c 65 61 73 65 2f 77 69 6e 5f 37 2e 30 2e 78 20 39 36 66 38 64 38 30 65 61 63 32 37 33 61 39 31 34 34 61 62 63 63 63 65 32 66 36 36 64 62 63 32 32 30 30 63 63 38 31 64 29 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 main - * Version 7.0.7 (release/win_7.0.x 96f8d80eac273a9144 abccce2f66dbc2200cc81 d)	success or wait	1	16F9EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	7102	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 43 75 73 74 6f 6d 20 43 6c 69 65 6e 74 20 28 6e 6f 20 49 44 29 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 main - * Custom Client (no ID)	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	7224	99	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 main -	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	7323	164	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 50 72 6f 63 65 73 73 20 73 74 61 72 74 65 64 20 61 74 20 32 30 32 32 2d 30 38 2d 30 36 2e 20 50 49 44 20 32 38 35 36 2e 20 4f 53 20 69 73 20 57 69 6e 64 6f 77 73 20 37 20 28 36 34 20 62 69 74 29 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 main - Process started at 2022-08-06. PID 2856. OS is Windows 7 (64 bit)	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	7487	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6d 70 6c 5f 73 65 6c 65 63 74 6f 72 20 2d 20 75 73 69 6e 67 20 73 73 65 32 20 28 69 6e 74 72 69 6e 73 69 63 73 29 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 impl_selector - using sse2 (intrinsics)	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	7609	136	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 53 65 74 74 69 6e 67 20 61 20 6e 65 77 20 70 61 73 73 77 6f 72 64 20 66 72 6f 6d 20 63 6d 64 20 6c 69 6e 65 2e 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 main - Setting a new password from cmd line.	success or wait	1	16F9EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	7745	109	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 35 2e 38 32 30 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 73 65 2e 73 69 67 6e 61 6c 2e 68 75 62 20 2d 20 31 20 74 68 72 65 61 64 73 2e 0d 0a	info 2022-08-06 01:23:45.820 cmdif_p 2856 2416 base.signal.hub - 1 threads.	success or wait	1	16F9EC5	WriteFile
C:\ProgramData\anydesk\service.conf	0	2898	61 64 2e 61 6e 79 6e 65 74 2e 63 65 72 74 3d 2d 2d 2d 2d 2d 2d 42 45 47 49 4e 20 43 45 52 54 49 46 49 43 41 54 45 2d 2d 2d 2d 2d 5c 6e 4d 49 49 43 71 44 43 43 41 5a 41 43 41 51 45 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 4c 42 51 41 77 47 54 45 58 4d 42 55 47 41 31 55 45 41 77 77 4f 51 57 35 35 52 47 56 7a 61 79 42 44 5c 6e 62 47 6c 6c 62 6e 51 77 49 42 63 4e 4d 6a 49 77 4f 44 41 32 4d 44 45 79 4d 7a 4d 77 57 68 67 50 4d 6a 41 33 4d 6a 41 33 4d 6a 51 77 4d 54 49 7a 4d 7a 42 61 4d 42 6b 78 46 7a 41 56 42 67 4e 56 5c 6e 42 41 4d 4d 44 6b 46 75 65 55 52 6c 63 32 73 67 51 32 78 70 5a 57 35 30 4d 49 49 42 49 6a 41 4e 42 67 6b 71 68 6b 69 47 39 77 30 42 41 51 45 46 41 41 4f 43 41 51 38 41 4d 49 49 42 43 67 4b 43 5c 6e 41 51 45 41 33 6d 39 73 30 58 74 31 74	ad.anynet.cert=-----BEGIN CERTIFICATE-----\nMIICqDCCAZACAQEwDQYJKoZIhvcNAQELBQAwGTEXMBUGA1UEAwwOQW55RGVzayBD\nbGllbnQwIBcNMjIwODA2MDEyMzMwWhgPMjA3MjA3MjQwMTIzMzBaMBkxFzAVBgNV\nBAMMDkFueURlc2sgQ2xpZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC\nAQEA3m9s0Xt1t	success or wait	1	1703D3E	WriteFile
C:\ProgramData\anydesk\system.conf	0	664	61 64 2e 61 6e 79 6e 65 74 2e 66 70 72 3d 61 64 38 66 65 63 36 63 65 32 65 61 39 35 38 37 33 30 39 63 35 30 62 39 37 31 37 35 64 38 65 64 36 33 39 61 39 66 30 39 0a 61 64 2e 61 6e 79 6e 65 74 2e 72 65 6c 61 79 2e 66 61 74 61 6c 5f 72 65 73 75 6c 74 3d 31 2e 30 0a 61 64 2e 61 6e 79 6e 65 74 2e 72 65 6c 61 79 2e 73 74 61 74 65 3d 30 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 5f 66 69 6c 65 73 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 66 72 6f 6e 74 65 6e 64 5f 63 6c 69 70 62 6f 61 72 64 5f 76 65 72 73 69 6f 6e 3d 31 0a 61 64 2e 73 65 63 75 72 69 74 79 2e 70 65 72 6d 69 73 73 69 6f 6e 5f 70 72 6f 66 69 6c 65	ad.anynet.fpr=ad8fec6ce2ea9587309c50b97175d8ed639a9f09ad.anynet.relay.fatal_result=1.0ad.anynet.relay.state=0ad.security.frontend_clipboard=1ad.security.frontend_clipboard_files=1ad.security.frontend_clipboard_version=1ad.security.permission_profile	success or wait	1	1703D3E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	8476	121	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 38 2e 31 32 39 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 73 65 2e 70 72 6f 74 2e 6a 6f 62 5f 64 69 73 70 61 74 63 68 65 72 20 2d 20 30 20 75 6e 64 65 6c 69 76 65 72 65 64 20 70 61 63 6b 65 74 73 2e 0d 0a	info 2022-08-06 01:23:48.129 cmdif_p 2856 2416 base.prot.job_dispatcher - 0 undelivered packets.	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	8597	110	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 34 38 2e 31 32 39 20 20 20 20 63 6d 64 69 66 5f 70 20 20 20 32 38 35 36 20 20 20 32 34 31 36 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 54 65 72 6d 69 6e 61 74 65 64 2e 0d 0a	info 2022-08-06 01:23:48.129 cmdif_p 2856 2416 main - Terminated.	success or wait	1	16F9EC5	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	unknown	254	success or wait	1	1598204	ReadFile
C:\ProgramData\anydesk\service.conf	unknown	2762	success or wait	1	170402C	ReadFile
C:\Users\user\AppData\Roaming\AnyDesk\user.conf	unknown	1003	success or wait	1	170402C	ReadFile
C:\ProgramData\anydesk\system.conf	unknown	455	success or wait	1	170402C	ReadFile
C:\ProgramData\anydesk\service.conf	unknown	2898	success or wait	1	170402C	ReadFile
C:\Users\user\AppData\Roaming\AnyDesk\user.conf	unknown	1003	success or wait	1	170402C	ReadFile
C:\ProgramData\anydesk\system.conf	unknown	664	success or wait	1	170402C	ReadFile

Analysis Process: AnyDesk.exe PID: **2120**, Parent PID: **2440**

General

Target ID:	26
Start time:	18:23:54
Start date:	05/08/2022
Path:	C:\ProgramData\anydesk\AnyDesk.exe
Wow64 process (32bit):	true
Commandline:	"c:\programdata\anydesk\anydesk.exe" --get-id
Imagebase:	0x12a0000
File size:	3829888 bytes
MD5 hash:	1BC5890C9E7BF54B7712E344B0AF9D04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	16FBAF0	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	8707	38	20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 20 2a 0d 0a	* * * * * * * * * * * * * * * * * *	success or wait	1	16F9FF0	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	8745	126	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 37 2e 38 32 36 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 41 6e 79 44 65 73 6b 20 57 69 6e 64 6f 77 73 20 53 74 61 72 74 75 70 20 2a 0d 0a	info 2022-08-06 01:23:57.826 cmdif_i 2120 924 main - * AnyDesk Windows Startup *	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	8871	175	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 37 2e 38 32 36 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 56 65 72 73 69 6f 6e 20 37 2e 30 2e 37 20 28 72 65 6c 65 61 73 65 2f 77 69 6e 5f 37 2e 30 2e 78 20 39 36 66 38 64 38 30 65 61 63 32 37 33 61 39 31 34 34 61 62 63 63 63 65 32 66 36 36 64 62 63 32 32 30 30 63 63 38 31 64 29 0d 0a	info 2022-08-06 01:23:57.826 cmdif_i 2120 924 main - * Version 7.0.7 (release/win_7.0.x 96f8d80eac273a9144 abccce2f66dbc2200cc81 d)	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	9046	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 37 2e 38 32 36 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 2a 20 43 75 73 74 6f 6d 20 43 6c 69 65 6e 74 20 28 6e 6f 20 49 44 29 0d 0a	info 2022-08-06 01:23:57.826 cmdif_i 2120 924 main - * Custom Client (no ID)	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	9168	99	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 37 2e 38 32 36 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 0d 0a	info 2022-08-06 01:23:57.826 cmdif_i 2120 924 main -	success or wait	1	16F9EC5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	9267	164	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 37 2e 38 32 36 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 50 72 6f 63 65 73 73 20 73 74 61 72 74 65 64 20 61 74 20 32 30 32 32 2d 30 38 2d 30 36 2e 20 50 49 44 20 32 31 32 30 2e 20 4f 53 20 69 73 20 57 69 6e 64 6f 77 73 20 37 20 28 36 34 20 62 69 74 29 0d 0a	info 2022-08-06 01:23:57.826 cmdif_i 2120 924 main - Process started at 2022-08-06. PID 2120. OS is Windows 7 (64 bit)	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	9431	122	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 37 2e 38 32 36 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6d 70 6c 5f 73 65 6c 65 63 74 6f 72 20 2d 20 75 73 69 6e 67 20 73 73 65 32 20 28 69 6e 74 72 69 6e 73 69 63 73 29 0d 0a	info 2022-08-06 01:23:57.826 cmdif_i 2120 924 impl_selector - using sse2 (intrinsics)	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	9553	109	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 37 2e 38 32 36 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 73 65 2e 73 69 67 6e 61 6c 2e 68 75 62 20 20 2d 20 31 20 74 68 72 65 61 64 73 2e 0d 0a	info 2022-08-06 01:23:57.826 cmdif_i 2120 924 base.signal.hub - 1 threads.	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	10284	121	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 38 2e 32 36 33 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 73 65 2e 70 72 6f 74 2e 6a 6f 62 5f 64 69 73 70 61 74 63 68 65 72 20 20 2d 20 30 20 75 6e 64 65 6c 69 76 65 72 65 64 20 70 61 63 6b 65 74 73 2e 0d 0a	info 2022-08-06 01:23:58.263 cmdif_i 2120 924 base.prot.job_dispatcher - 0 undelivered packets.	success or wait	1	16F9EC5	WriteFile
C:\Users\user\AppData\Roaming\AnyDesk\ad.trace	10405	110	20 20 20 69 6e 66 6f 20 32 30 32 32 2d 30 38 2d 30 36 20 30 31 3a 32 33 3a 35 38 2e 32 36 33 20 20 20 20 63 6d 64 69 66 5f 69 20 20 20 32 31 32 30 20 20 20 20 39 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 69 6e 20 2d 20 54 65 72 6d 69 6e 61 74 65 64 2e 0d 0a	info 2022-08-06 01:23:58.263 cmdif_i 2120 924 main - Terminated.	success or wait	1	16F9EC5	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: netsh.exe PID: **2744**, Parent PID: **2440**

General	
Target ID:	27
Start time:	18:23:58
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh advfirewall firewall add rule name="RDP" dir=in protocol=TCP localport=3389 action=allow
Imagebase:	0x13a0000
File size:	96256 bytes
MD5 hash:	784A50A6A09C25F011C3143DDD68E729
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: icacls.exe PID: **1004**, Parent PID: **1704**

General	
Target ID:	29
Start time:	18:24:02
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\ICACLS.EXE" "C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\." /SETINTEGRITYLEVEL (CI)(OI)LOW
Imagebase:	0xf00000
File size:	27136 bytes
MD5 hash:	1542A92D5C6F7E1E80613F3466C9CE7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2332**, Parent PID: **2876**

General	
Target ID:	31
Start time:	18:24:06
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\user\AppData\Local\Temp\MW-4a754448-1372-4b62-af77-6f1650246a5a\files"
Imagebase:	0x4aab0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly