ID: 651259
Sample Name: ikvNEF5d2Z
Cookbook: default.jbs
Time: 17:59:03
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

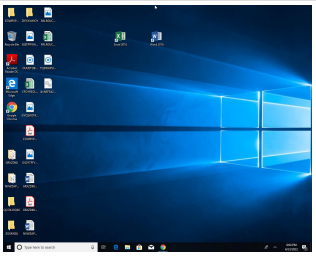
Windows Analysis Report

ikvNEF5d2Z

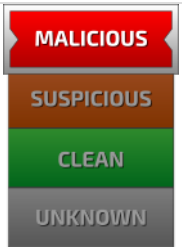
Overview

General Information

Sample Name:	ikvNEF5d2Z (renamed file extension from none to dll)
Analysis ID:	651259
MD5:	dfa62565b68736..
SHA1:	d64a755f001658..
SHA256:	6f57eb37bff30df…
Infos:	



Detection



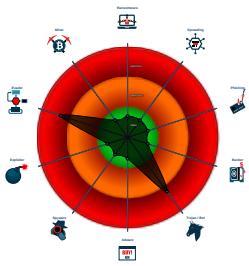
IcedID

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

Signatures

- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Yara detected IcedID
- Tries to detect virtualization through…
- Found a high number of Window / U…
- Tries to load missing DLLs
- May sleep (evasive loops) to hinder…
- Registers a DLL

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6552 cmdline: loaddll64.exe "C:\Users\user\Desktop\ikvNEF5d2Z.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6568 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\ikvNEF5d2Z.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6588 cmdline: rundll32.exe "C:\Users\user\Desktop\ikvNEF5d2Z.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6576 cmdline: regsvr32.exe /s C:\Users\user\Desktop\ikvNEF5d2Z.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 6596 cmdline: rundll32.exe C:\Users\user\Desktop\ikvNEF5d2Z.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6804 cmdline: rundll32.exe C:\Users\user\Desktop\ikvNEF5d2Z.dll,PluginInit MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000003.321553577.000000000119D000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
00000002.00000003.267642045.00000000011B1000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
00000003.00000003.274029943.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
00000003.00000003.261454717.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	
00000002.00000003.269643903.00000000011B1000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_IcedID_1	Yara detected IcedID	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 88 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.858716532023883 06/23/22-18:01:43.082878
SID:	2023883
Source Port:	58716
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.853630532023883 06/23/22-18:01:13.124714
SID:	2023883
Source Port:	53630
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.858709532023883 06/23/22-18:03:43.028981
SID:	2023883
Source Port:	58709
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.851906532023883 06/23/22-18:02:43.008995
SID:	2023883
Source Port:	51906
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.858003532023883 06/23/22-18:04:13.049394
SID:	2023883
Source Port:	58003
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.857421532023883 06/23/22-18:00:13.228137
SID:	2023883
Source Port:	57421
Destination Port:	53
Protocol:	UDP

Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.856189532023883 06/23/22-18:00:43.017885
SID:	2023883
Source Port:	56189
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.852540532023883 06/23/22-18:02:13.036582
SID:	2023883
Source Port:	52540
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.38.8.8.863030532023883 06/23/22-18:03:13.066960
SID:	2023883
Source Port:	63030
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Yara detected IcedID

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic

E-Banking Fraud

- Yara detected IcedID

Malware Analysis System Evasion

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

- System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected IcedID

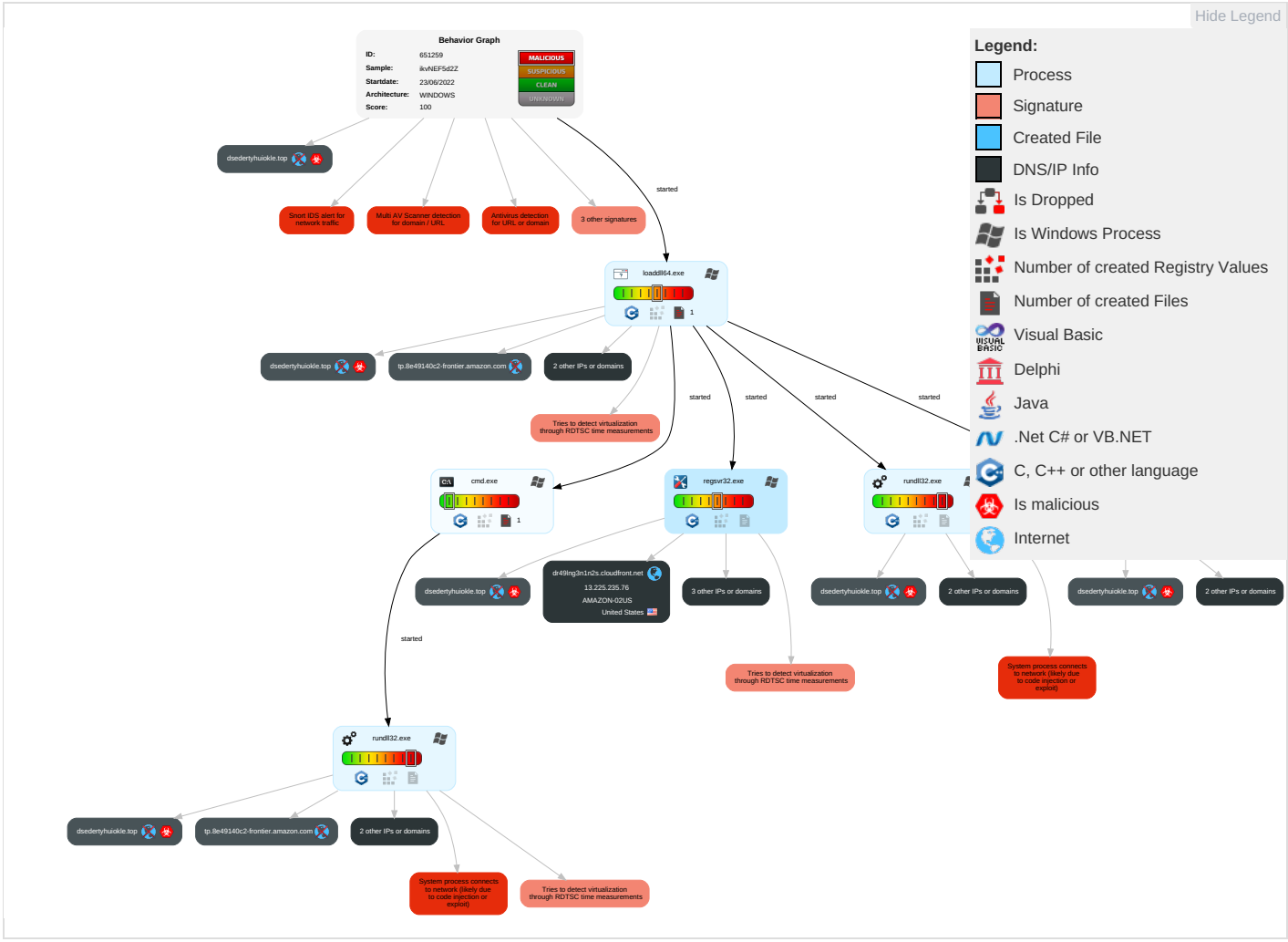
Remote Access Functionality

Yara detected IcedID

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
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 1 1 Process Injection	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Regsvr32	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Rundll32	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 1 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

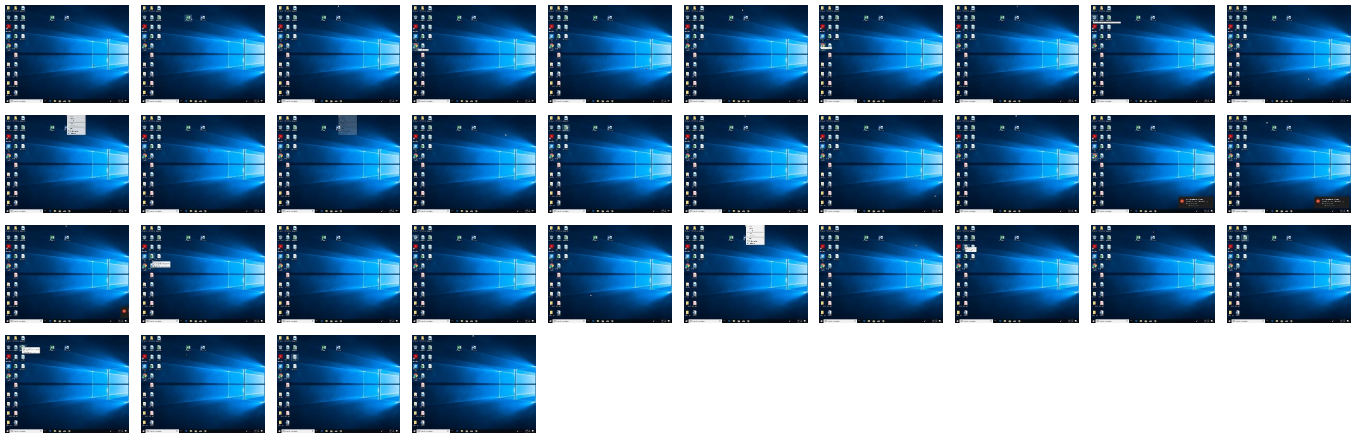
Behavior Graph



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
ikvNEF5d2Z.dll	76%	Virustotal		Browse
ikvNEF5d2Z.dll	35%	Metadefender		Browse
ikvNEF5d2Z.dll	66%	ReversingLabs	Win64.Trojan.IcedID	
ikvNEF5d2Z.dll	100%	Avira	HEUR/AGEN.1245251	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
dsedertyhuiokle.top	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://prod-us-west-2.csp-report.marketing.aws.dev	0%	URL Reputation	safe	
http://dsedertyhuiokle.top/do	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/top	100%	Avira URL Cloud	malware	
http://https://d1fgizr415o1r6.cloudfront.n	0%	Avira URL Cloud	safe	
http://dsedertyhuiokle.top/CN	100%	Avira URL Cloud	malware	
http://https://www.buzzsprout.com;	0%	Avira URL Cloud	safe	
http://dsedertyhuiokle.top/eQz	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/$l	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/;	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/?	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top:80/&j	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/3	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/7	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top:80/jY	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/	100%	Avira URL Cloud	malware	
http://https://google.com.vc	0%	Avira URL Cloud	safe	
http://https://google.com.vn	0%	Avira URL Cloud	safe	
http://dsedertyhuiokle.top/H2az	100%	Avira URL Cloud	malware	
http://dsedertyhuiokle.top/Name	100%	Avira URL Cloud	malware	
http://https://google.com.uy	0%	Avira URL Cloud	safe	
http://dsedertyhuiokle.top/Po3	100%	Avira URL Cloud	malware	
http://https://112-tzm-766.mktoutil.com	0%	URL Reputation	safe	
http://https://google.gf	0%	Avira URL Cloud	safe	
http://https://download.stormacq.com/aws/podcast/	0%	URL Reputation	safe	
http://dsedertyhuiokle.top/sop	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dr49lng3n1n2s.cloudfront.net	13.225.235.76	true	false		high
dsedertyhuiokle.top	unknown	unknown	true	• 13%, Virustotal, Browse	unknown
aws.amazon.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://console.aws.amazon.com/billing/home#/account?nc2=h_m_ma	loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273518645.00000272B360C000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://prod-us-west-2.csp-report.marketing.aws.dev	loaddll64.exe, 00000000.00000003.274973142.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.00000272B3608000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.linkedin.com	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/do	loaddll64.exe, 00000000.00000003.318334707.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.317603140.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.408901626.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.408673247.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://google.ad	loaddll64.exe, 00000000.00000003.274580506.00000272B360B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://c0.b0.p.awsstatic.com	loaddll64.exe, 00000000.00000003.274973142.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.276356958.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.00000272B3608000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://google.ac	loaddll64.exe, 00000000.00000003.274580506.00000272B360B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://aws.amazon.com/solutions/case-studies/rivian-case-study/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.ae	loaddll64.exe, 00000000.00000003.274580506.00000272B360B000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.aboutamazon.com/news/aws/making-the-invisible-visible/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.618555648.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.559478883.00000000031F6000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.00 00000003201000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.656727314.00000000031FB000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.568201754. 00000000031FC000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.266794324.0000000003204000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.26942565 6.0000000003204000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.469394560.00000000031F6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063 088.00000000031FB000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.481591686.00000000031F500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.0000 000003204000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.684397645.00000000031C7000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.696383069.00 000000031D2000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.678102368.00000000031D6000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.568338884. 00000000031FC000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.672085117.00000000031F6000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.59444508 2.00000000031F8000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.411376388.0000000003204000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.al	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.am	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/top	loaddll64.exe, 00000000.00000003.4847853 42.00000272B35B3000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.297763257.00000000011D2000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.297486719.00000 000011D2000.00000004.00000020.00020000.0 0000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://google.az	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.at	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.as	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.ba	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://aws.demdex.net	loaddll64.exe, 00000000.00000003.2756437 94.00000272B3608000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.bi	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://d1fgizr415o1r6.cloudfront.n	loaddll64.exe, 00000000.00000003.2786159 04.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.279695130.00000272B35F400 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275820288.000 00272B35F4000.00000004.00000020.00020000 .00000000.sdmp, loaddll64.exe, 00000000. 00000003.277605660.00000272B35F4000.0000 0004.00000020.00020000.00000000.sdmp, lo addll64.exe, 00000000.00000003.276356958 .00000272B35F4000.00000004.00000020.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aws.amazon.com/solutions/case-studies/maxar-case-study/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.2743736 56.00000272B5277000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.275115267.00000272B51F100 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.0000 0000031FC000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.278112709.0000000003204000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.559478883.00 000000031F6000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.423126748.0000000003201000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.481705170. 0000000003201000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.656727314.00000000031FB000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56820175 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.266794324.0000000003204000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425 656.0000000003204000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.469394560.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.0000 0000031FB000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.481591686.00000000031F5000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.312372105.00 00000003204000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.684397645.00000000031C7000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.696383069. 00000000031D2000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.678102368.00000000031D6000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56833888 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.672085117.00000000031F6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445 082.00000000031F8000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://https://google.bj	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/CN	rundll32.exe, 00000003.00000003.27402994 3.000001599AEC2000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://google.be	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://www.buzzsprout.com;	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/maryland-dhs/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.00000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://i18n-string.us-west-2.prod.pricing.aws.a2z.com	loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273518645.00000272B360C000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.274973142.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.00000272B3608000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.00000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.bg	loaddll64.exe, 00000000.00000003.274580506.00000272B360B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.bf	loaddll64.exe, 00000000.00000003.274580506.00000272B360B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://aws.amazon.com/ru/?nc1=h_ls	regsvr32.exe, 00000002.00000003.600732821.00000000031F8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.520119151.0000000003201000.00000004.00000020.00020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/eQz	loaddll64.exe, 00000000.00000003.302734691.00000272B35B3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://google.bs	loaddll64.exe, 00000000.00000003.274580506.00000272B360B000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://docs.aws.amazon.com/index.html?nc2=h_ql_doc	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 00000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.by	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.bt	loaddll64.exe, 00000000.00000003.2745805 06.00000272B360B000.00000004.00000020.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/th/	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 00000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/carrier-case-study/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.2743736 56.00000272B5277000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.275115267.00000272B51F100 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.0000 0000031FC000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.278112709.0000000003204000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.559478883.00 000000031F6000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.423126748.0000000003201000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.481705170. 0000000003201000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.656727314.00000000031FB000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56820175 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.266794324.0000000003204000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425 656.0000000003204000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.469394560.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.0000 0000031FB000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.481591686.00000000031F5000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.312372105.00 00000003204000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.684397645.00000000031C7000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.696383069. 00000000031D2000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.678102368.00000000031D6000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56833888 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.672085117.00000000031F6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445 082.00000000031F8000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/$l	loaddll64.exe, 00000000.00000003.3033051 37.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.306147533.00000272B35F400 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.419285425.000 00272B35F4000.00000004.00000020.00020000 .00000000.sdmp, loaddll64.exe, 00000000. 00000003.419463769.00000272B35F4000.0000 0004.00000020.00020000.00000000.sdmp, lo addll64.exe, 00000000.00000003.305948479 .00000272B35F4000.00000004.00000020.0002 0000.00000000.sdmp, loaddll64.exe, 00000 000.00000003.469861552.00000272B35F4000. 00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.494235596.00000 272B35F4000.00000004.00000020.00020000.0 0000000.sdmp, loaddll64.exe, 00000000.00 000003.305566557.00000272B35F4000.000000 04.00000020.00020000.00000000.sdmp, load dll64.exe, 00000000.00000003.305265867.0 0000272B35F4000.00000004.00000020.000200 00.00000000.sdmp, loaddll64.exe, 0000000 0.00000003.467448104.00000272B35F4000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dsedertyhuiokle.top/;	regsvr32.exe, 00000002.00000003.26514846 9.00000000011D2000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://console.aws.amazon.com/support/home/?nc2=h_ql_cu	loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273518645.00000272B360C000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dftu77xade0tc.cloudfront.net	loaddll64.exe, 00000000.00000003.274973142.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.00000272B360800.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://dsedertyhuiokle.top/?	loaddll64.exe, 00000000.00000003.5152544 87.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.297830845.00000272B35F400 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.449481029.000 00272B35F4000.00000004.00000020.00020000 .00000000.sdmp, loaddll64.exe, 00000000. 00000003.324742085.00000272B35F4000.0000 0004.00000020.00020000.00000000.sdmp, lo addll64.exe, 00000000.00000003.484853208 .00000272B35F4000.00000004.00000020.0002 0000.00000000.sdmp, loaddll64.exe, 00000 000.00000003.410962864.00000272B35F4000. 00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.315300667.00000 272B35F4000.00000004.00000020.00020000.0 0000000.sdmp, loaddll64.exe, 00000000.00 000003.418564767.00000272B35F4000.000000 04.00000020.00020000.00000000.sdmp, load dll64.exe, 00000000.00000003.598201964.0 0000272B35F4000.00000004.00000020.000200 00.00000000.sdmp, loaddll64.exe, 0000000 0.00000003.477298408.00000272B35F4000.00 000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.4214486 41.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.299296583.00000272B35F400 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.767376439.000 00272B35F4000.00000004.00000020.00020000 .00000000.sdmp, loaddll64.exe, 00000000. 00000003.302243734.00000272B35F4000.0000 0004.00000020.00020000.00000000.sdmp, lo addll64.exe, 00000000.00000003.294070958 .00000272B35F4000.00000004.00000020.0002 0000.00000000.sdmp, loaddll64.exe, 00000 000.00000003.292563140.00000272B35F4000. 00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.469861552.00000 272B35F4000.00000004.00000020.00020000.0 0000000.sdmp, loaddll64.exe, 00000000.00 000003.463358477.00000272B35F4000.000000 04.00000020.00020000.00000000.sdmp, load dll64.exe, 00000000.00000003.300119379.0 0000272B35F4000.00000004.00000020.000200 00.00000000.sdmp, loaddll64.exe, 0000000 0.00000003.295541331.00000272B35F4000.00 000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.3219738 08.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dsedertyhuiokle.top:80/&j	regsvr32.exe, 00000002.00000003.32155357 7.000000000119D000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dsedertyhuiokle.top/3	regsvr32.exe, 00000002.00000003.30317797 5.00000000011D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.305253871.00000000011D2000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/publicis-media/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.2743736 56.00000272B5277000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.275115267.00000272B51F100 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.0000 0000031FC000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.278112709.0000000003204000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.559478883.00 000000031F6000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.423126748.0000000003201000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.481705170. 0000000003201000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.656727314.00000000031FB000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56820175 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.266794324.0000000003204000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425 656.0000000003204000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.469394560.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.0000 0000031FB000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.481591686.00000000031F5000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.312372105.00 00000003204000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.684397645.00000000031C7000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.696383069. 00000000031D2000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.678102368.00000000031D6000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56833888 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.672085117.00000000031F6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445 082.00000000031F8000.00000004.00000020.0 0020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://pages.awscloud.com/AWS_TrainCert_Thought-Leadership-download.html?hp=tile&tile=uyt	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.00000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/7	regsvr32.exe, 00000002.00000003.294005581.00000000011D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.267736131.00000000011D2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/pearson-digitally-transforms/?hp=tile&tile=custome	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.00000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.cz	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/vi/	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 00000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.cv	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.de	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top:80/jY	regsvr32.exe, 00000002.00000003.29827265 0.000000000119D000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.295125426.000000000119D000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.305135 210.000000000119D000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://google.dk	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.dj	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.dm	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/nasdaq-case-study/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.00000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/	rundll32.exe, 00000004.00000003.300093700.000001E90C7E4000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.524383009.0000024990463000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://wrp.dse.marketing.aws.a2z.com	loaddll64.exe, 00000000.00000003.274973142.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.274580506.00000272B360B000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.00000272B3608000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.dz	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/training/ramp-up-guides/?hp=lrhttps://aws.amazon.com/training/ramp-up-guides/	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.00000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://spot-bid-advisor.s3.amazonaws.com	loaddll64.exe, 00000000.00000003.274973142.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.00000272B3608000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://d3ctxlq1ktw2nl.cloudfront.net	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.com.vc	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://google.ee	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.com.vn	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/jp/	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 00000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.es	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/netflix/	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.618555648.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.559478883.00000000031F6000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.00 00000003201000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.656727314.00000000031FB000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.568201754. 00000000031FC000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.266794324.0000000003204000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.26942565 6.0000000003204000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.469394560.00000000031F6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063 088.00000000031FB000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.481591686.00000000031F500 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.0000 000003204000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.684397645.00000000031C7000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.696383069.00 000000031D2000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.678102368.00000000031D6000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.568338884. 00000000031FC000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.672085117.00000000031F6000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.59444508 2.00000000031F8000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.411376388.0000000003204000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://https://view-stage.us-west-2.prod.pricing.aws.a2z.com	loaddll64.exe, 00000000.00000003.2749731 42.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.274580506.00000272B360B00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.000 00272B3608000.00000004.00000020.00020000 .00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/freewheel/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.00000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.fm	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://s3.amazonaws.com/public-pricing-agc/	loaddll64.exe, 00000000.00000003.274973142.00000272B35F4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275643794.00000272B360800.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/de/	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 00000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/H2az	regsvr32.exe, 00000002.00000003.26514846 9.00000000011D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.276133966.00000000011D2000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.317541 622.00000000011D2000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.262535432.00000000011D200 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.272139372.0000 0000011D2000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.267736131.00000000011D2000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.277085762.00 000000011D2000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.437665754.00000000011D2000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.263777645. 00000000011D2000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.317957028.00000000011D2000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.32016936 0.00000000011D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.269684817.00000000011D2000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.281055 159.00000000011D2000.00000004.00000020.0 0020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://google.fi	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://phd.aws.amazon.com/?nc2=h_m_sc	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 000000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://a0.awsstatic.com/libra-css/images/logos/aws_logo_smile_1200x630.png	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 00000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/Name	regsvr32.exe, 00000002.00000003.31795702 8.00000000011D2000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://google.com.uy	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://a0.awsstatic.com	regsvr32.exe, 00000002.00000003.52011915 1.0000000003201000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://google.fr	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/Po3	loaddll64.exe, 00000000.00000003.4185647 67.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.310508348.00000272B35F400 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.499476528.000 00272B35F4000.00000004.00000020.00020000 .00000000.sdmp, loaddll64.exe, 00000000. 00000003.295541331.00000272B35F4000.0000 0004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://website.spot.ec2.aws.a2z.com	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://112-tzm-766.mktoutil.com	loaddll64.exe, 00000000.00000003.2758202 88.00000272B35F4000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.274973142.00000272B35F400 0.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

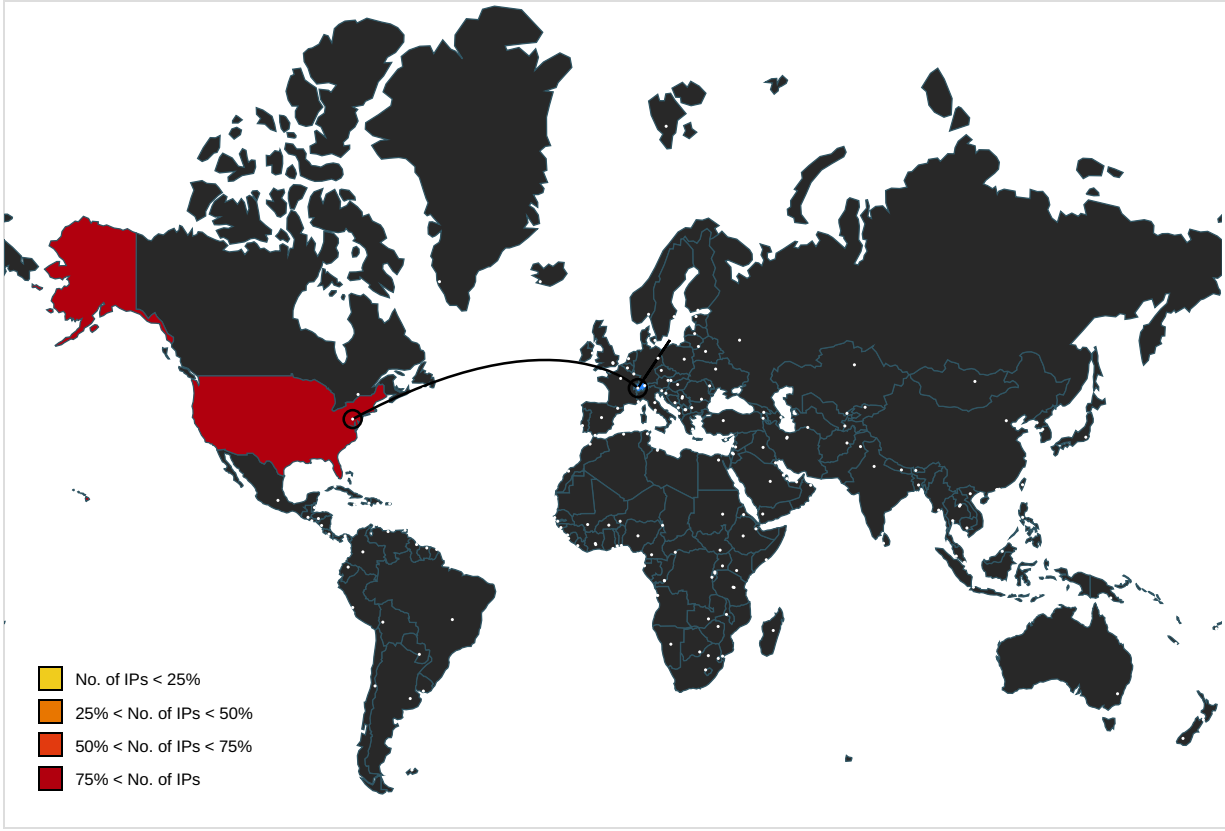
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://google.gf	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://google.ge	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://a0.awsstatic.com/da/js/1.0.48/aws-da.js	loaddll64.exe, 00000000.00000003.2754434 03.00000272B3550000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.275115267.00000272B51F100 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.0000 0000031FC000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.278112709.0000000003204000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.559478883.00 000000031F6000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.423126748.0000000003201000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.481705170. 0000000003201000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.656727314.00000000031FB000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56820175 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.266794324.0000000003204000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425 656.0000000003204000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.469394560.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.0000 0000031FB000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000002.00 000003.481591686.00000000031F5000.000000 04.00000020.00020000.00000000.sdmp, regs vr32.exe, 00000002.00000003.312372105.00 000000003204000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.684397645.00000000031C7000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.696383069. 00000000031D2000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.678102368.00000000031D6000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.56833888 4.00000000031FC000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.672085117.00000000031F6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445 082.00000000031F8000.00000004.00000020.0 0020000.00000000.sdmp	false		high
http://https://google.gg	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.ga	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.gm	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.gp	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://google.gl	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://download.stormacq.com/aws/podcast/	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://google.gr	loaddll64.exe, 00000000.00000003.2735483 40.00000272B51F5000.00000004.00000020.00 020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://a0.awsstatic.com/plc/js/1.0.129/plc	loaddll64.exe, 00000000.00000003.2751152 67.00000272B51F1000.00000004.00000020.00 020000.00000000.sdmp, loaddll64.exe, 000 00000.00000003.273518645.00000272B360C00 0.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.000 00272B51F5000.00000004.00000020.00020000 .00000000.sdmp, regsvr32.exe, 00000002.0 0000003.618555648.00000000031FC000.00000 004.00000020.00020000.00000000.sdmp, reg svr32.exe, 00000002.00000003.278112709.0 000000003204000.00000004.00000020.000200 00.00000000.sdmp, regsvr32.exe, 00000002 .00000003.559478883.00000000031F6000.000 00004.00000020.00020000.00000000.sdmp, r egsvr32.exe, 00000002.00000003.423126748 .0000000003201000.00000004.00000020.0002 0000.00000000.sdmp, regsvr32.exe, 000000 02.00000003.481705170.0000000003201000.0 0000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.6567273 14.00000000031FB000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0002.00000003.568201754.00000000031FC000 .00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.00000 00003204000.00000004.00000020.00020000.0 0000000.sdmp, regsvr32.exe, 00000002.000 00003.269425656.0000000003204000.0000000 4.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6 000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00 000000031FB000.00000004.00000020.0002000 0.00000000.sdmp, regsvr32.exe, 00000002. 00000003.481591686.00000000031F5000.0000 0004.00000020.00020000.00000000.sdmp, re gsvr32.exe, 00000002.00000003.312372105. 0000000003204000.00000004.00000020.00020 000.00000000.sdmp, regsvr32.exe, 0000000 2.00000003.684397645.00000000031C7000.00 000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.69638306 9.00000000031D2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 002.00000003.678102368.00000000031D6000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338 884.00000000031FC000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00002.00000003.672085117.00000000031F600 0.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://console.aws.amazon.com/support/home?nc2=h_ql_cu	loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273518645.00000272B360C000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://google.gy	loaddll64.exe, 00000000.00000003.273548340.00000272B51F5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://dsedertyhuiokle.top/sop	regsvr32.exe, 00000002.00000003.267736131.00000000011D2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aws.amazon.com/solutions/case-studies/astrazeneca/?hp=tile&tile=customerstories	loaddll64.exe, 00000000.00000003.274373656.00000272B5277000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.275115267.00000272B51F1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.618555648.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.278112709.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.559478883.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.423126748.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481705170.0000000003201000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.656727314.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568201754.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.266794324.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.269425656.0000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.469394560.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.540063088.00000000031FB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.481591686.00000000031F5000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.312372105.00000000003204000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.684397645.00000000031C7000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.696383069.00000000031D2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.678102368.00000000031D6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.568338884.00000000031FC000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.672085117.00000000031F6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000002.00000003.594445082.00000000031F8000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.225.235.76	dr49lng3n1n2s.cloudfront.net	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651259
Start date and time: 23/06/202217:59:03	2022-06-23 17:59:03 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ikvNEF5d2Z (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
Number of new started drivers analysed:	0
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.troj.evad.winDLL@11/0@5422/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:00:12	API Interceptor	2061x Sleep call for process: regsvr32.exe modified
18:00:12	API Interceptor	6589x Sleep call for process: rundll32.exe modified
18:00:18	API Interceptor	1987x Sleep call for process: loaddll64.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

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.431311114789898
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	ikvNEF5d2Z.dll
File size:	240216
MD5:	dfa62565b68736dc443386d68388b269
SHA1:	d64a755f001658c7bc037049259f23807105d8ba
SHA256:	6f57eb37bff30df1a66f848cb648799536dcbc05f6fb32d1ae071102ffd830ee
SHA512:	f6d4858e069016e763b4a7dc193742b7eb841f2409a3c03058255006978b7deb586fff0dd1be3b7cbef03d55fe917507876cbf34d2a0c828fe03a0845f363bee
SSDEEP:	6144:dJJLaU1mUGduNzGSijExi3oomlnG9PS9sfr8mnOySgEBmvpmCZdXWdyqL28888Ie:dJJLaU1mUGduNzGSijExi3oomlnG9PSU
TLSH:	A2346266C598D1BCF2476871357CAB58C550AE80AD12DDE3FAE6C412AF239B123213DF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j...j...j...i...j...k...j...k...j...j...j...j...j...h...j.Rich..j.....PE..d...!p.`....." .....:...l.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180005f40
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60917021 [Tue May 4 16:02:41 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	87bed5a7cba00c7e1f4015f1bdae2183

Entrypoint Preview

Instruction
push eax
cmp edx, 01h
jne 00007F0DBCCA9344h
mov eax, 0062F187h
mov dword ptr [esp], eax
mov dword ptr [esp+04h], eax
test dword ptr [esp], 00000003h
mov eax, dword ptr [esp]
je 00007F0DBCCA8E8Bh

Instruction
lea edx, dword ptr [eax+03h]
test eax, eax
cmovns edx, eax
and edx, FFFFFFFCh
sub eax, edx
mov edx, dword ptr [esp]
cmp eax, 01h
jne 00007F0DBCCA8F0Eh
inc esp
imul ecx, edx, 5EEB2A9Ch
inc ecx
add ecx, 2391704Ah
jmp 00007F0DBCCA8E76h
imul eax, eax, 89D19E3Bh
add eax, 3C3C8D0Eh
mov dword ptr [esp], eax
inc ecx
mov ecx, 2391704Ah
mov eax, dword ptr [esp]
add eax, dword ptr [esp+04h]
inc esp
imul edx, eax, AAAAAAABh
inc ecx
add edx, 2AAAAAAAh
mov edx, dword ptr [00030556h]
lea eax, dword ptr [edx-01h]
imul eax, edx
test al, 01h
sete al
cmp dword ptr [00030548h], 0Ah
inc ecx
setl al
inc ecx
or al, al
inc ecx
cmp edx, 55555555h
jc 00007F0DBCCA8E9Bh
inc ecx
add ecx, 02h
inc ebp
test al, al
je 00007F0DBCCA8E88h
inc esp
add dword ptr [esp], ecx
test dword ptr [esp], 00000003h
jne 00007F0DBCCA900Fh
inc dword ptr [esp]
inc dword ptr [esp+04h]
test dword ptr [esp], 00000003h
je 00007F0DBCCA8E52h
jmp 00007F0DBCCA8EF4h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x35250	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x352b4	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x37000	0xb4	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x35020	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x35000	0x20	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x33841	0x33a00	False	0.1523910411622276	data	6.091396505487613	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x35000	0x328	0x400	False	0.4521484375	data	3.9148957731530203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x36000	0x520	0x600	False	0.4915364583333333	data	4.112210005634511	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x37000	0xb4	0x200	False	0.26953125	data	2.0213833104584227	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ndata	0x38000	0x5fff	0x6000	False	0.9743245442708334	data	7.7238018558589765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Imports

DLL	Import
KERNEL32.dll	LoadLibraryA, GetProcAddress

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180001000
PluginInit	2	0x180011c63

Network Behavior

No network behavior found

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **6552**, Parent PID: **4792**

General

Target ID:	0
Start time:	18:00:09
Start date:	23/06/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\ikvNEF5d2Z.dll"
Imagebase:	0x7ff6fcf10000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6568**, Parent PID: **6552**

General

Target ID:	1
Start time:	18:00:09
Start date:	23/06/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\ikvNEF5d2Z.dll",#1
Imagebase:	0x7ff6dcf80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6576**, Parent PID: **6552**

General

Target ID:	2
Start time:	18:00:09
Start date:	23/06/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\ikvNEF5d2Z.dll
Imagebase:	0x7ff7bf970000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.321553577.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.267642045.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.269643903.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.297404495.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.292337146.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.277053411.00000000011B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.298272650.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.311756165.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.319014674.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.295125426.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.314754724.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.317474031.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.304327995.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.305135210.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.320094818.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.265620836.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.293963524.00000000011B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.309363516.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.411869520.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.302975794.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.282267699.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.275791438.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.262765450.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.263740751.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.299841707.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source:

00000002.00000003.351326851.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.265359115.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.271492952.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.262406305.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.278543970.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.407235069.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.437622717.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.293411402.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.491241630.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.280994457.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.297638852.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.415117148.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.416746789.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.298094562.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.268018419.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.264969343.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.272087960.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.307033359.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.270822392.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.317906358.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.267270096.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.312571750.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.290176337.00000000011B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.454332371.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.299224080.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.306791775.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.295599262.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.263807736.00000000011B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000002.00000003.274007377.000000000119D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

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: rundll32.exe PID: 6588, Parent PID: 6568

General

Target ID:	3
Start time:	18:00:10
Start date:	23/06/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\ikvNEF5d2Z.dll",#1
Imagebase:	0x7ff60eb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.274029943.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.261454717.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.269043278.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.396642532.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.264700847.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.267145571.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.270084280.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.266413828.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.261968567.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.271220559.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.265218608.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.273106192.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.262811825.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.265793313.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.719810116.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.263723615.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.272354753.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.267942385.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000003.00000003.274845604.000001599AEC2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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: rundll32.exe PID: **6596**, Parent PID: **6552**

General

Target ID:	4
Start time:	18:00:10
Start date:	23/06/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\ikvNEF5d2Z.dll,DllRegisterServer
Imagebase:	0x7ff60eb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.280507761.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.265795087.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.264618023.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.270691540.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.273346326.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.269326182.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.305936677.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.276312756.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.262421311.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.261647380.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.287602431.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.268258493.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.278246832.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.267338480.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.272644834.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.291011198.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.292690922.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_IcedID_1, Description: Yara detected IcedID, Source: 00000004.00000003.272047247.000001E90C7C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
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: rundll32.exe PID: **6804**, Parent PID: **6552**

General

Target ID:	5
Start time:	18:00:13
Start date:	23/06/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\ikvNEF5d2Z.dll,PluginInit
Imagebase:	0x7ff60eb80000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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

Disassembly

No disassembly