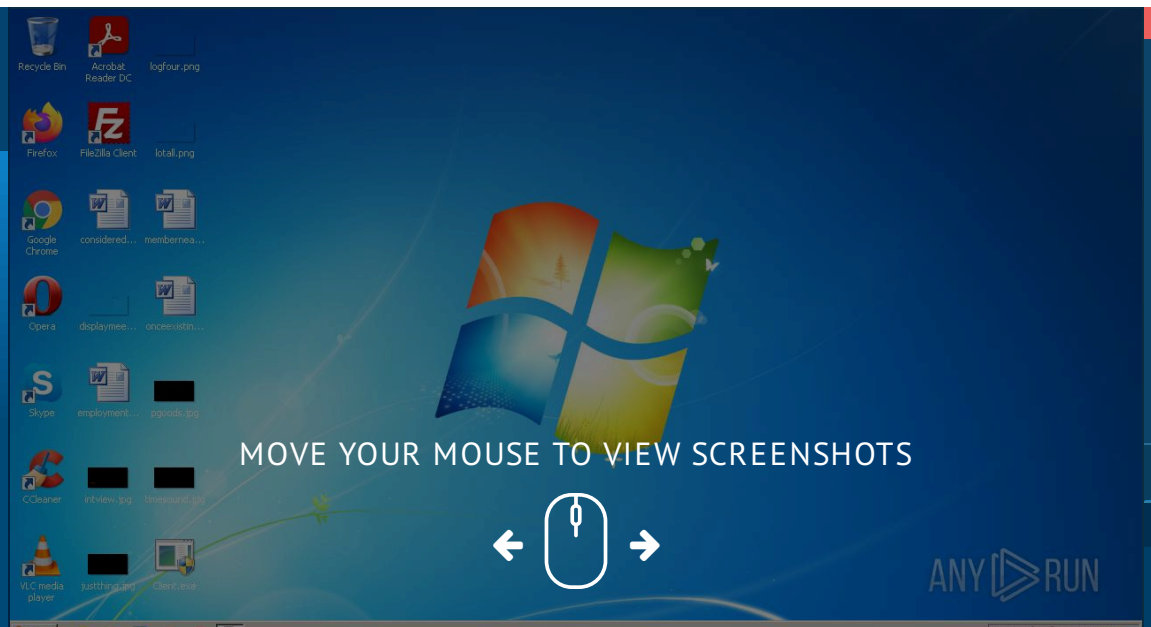

Malicious activity

Client.exe

MD5: FB16E15E2C93C12F25FE9E32A3A9D462
Start: 04.09.2022, 19:46 Total time: 240 s

Win7 32 bit
Complete

trojan rat revenge

Indicators:

Tracker: Remote Access Trojan, Revenge, Trojan

Get sample | IOC | MalConf | Restart

Text report | Graph | ATT&CK | AI Summary (beta) | Export

CPU RAM

Processes | Filter by PID or name | Only important

1748	Client.exe	PE	revenge	1k 1k 115	
2456	vbc.exe	/noconfig @"C:\Users\admin\AppData\Local\Temp\...		418 15 29	
2648	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OU...		107 17 12	
2808	vbc.exe	/noconfig @"C:\Users\admin\AppData\Local\Temp\...		384 14 28	
2712	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OU...		107 17 12	
2972	vbc.exe	/noconfig @"C:\Users\admin\AppData\Local\Temp\f...		384 14 28	
3288	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OU...		107 17 12	
1600	vbc.exe	/noconfig @"C:\Users\admin\AppData\Local\Temp\...		383 14 28	
3472	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OU...		107 17 12	
3692	vbc.exe	/noconfig @"C:\Users\admin\AppData\Local\Temp\...		383 14 28	
3672	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OU...		107 17 12	
3716	vbc.exe	/noconfig @"C:\Users\admin\AppData\Local\Temp\...		383 14 28	
2196	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OU...		107 17 12	
2224	vbc.exe	/noconfig @"C:\Users\admin\AppData\Local\Temp\l...		383 14 28	
3504	cvtres.exe	/NOLOGO /READONLY /MACHINE:IX86 "/OU...		107 17 12	
1068	RiotClientServices.exe	PE	revenge	2k 1k 183	
3300	cmd.exe			62 16 12	
2216	925.exe	PE		1k 403 92	
				62 16 12	
				w.google.com/ 1k 8k 106	
				DEF:1796 CREDAT:275457 /prefetc... 1k 6k 121	
				PE enge 925 453 115	

HTTP Requests 8 | Connections 27 | DNS Requests 15 | Threats 115 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
150.23 s	GET | 302: Found	?	1832	iexplore.exe		http://www.google.com/	2
150.25 s	GET | 200: OK	?	1832	iexplore.exe		http://ctldl.windowsupdate.com/msdo...	5
151.22 s	GET | 200: OK	?	1832	iexplore.exe		http://ocsp.pki.goog/gsr1/MFEwTzBN...	1
151.22 s	GET | 200: OK	?	1832	iexplore.exe		http://ocsp.pki.goog/gtsr1/ME4wTDBK...	72
151.22 s	GET | 200: OK	?	1832	iexplore.exe		http://ocsp.pki.goog/gts1c3/MFIwUDB...	47
151.26 s	GET | 200: OK	?	1832	iexplore.exe		http://ocsp.pki.goog/gts1c3/MFEwTzB...	47
152.25 s	GET | 200: OK	?	1832	iexplore.exe		http://ocsp.pki.goog/gts1c3/MFIwUDB...	47
180.89 s	GET | 200: OK	?	1796	iexplore.exe		http://ocsp.digicert.com/MFEwTzBNM...	47

Pricing | Contacts | FAQ | Sign In

Danger [2368] RiotClientServices.exe Changes the autorun value in the registry

Try community version for free! Register now