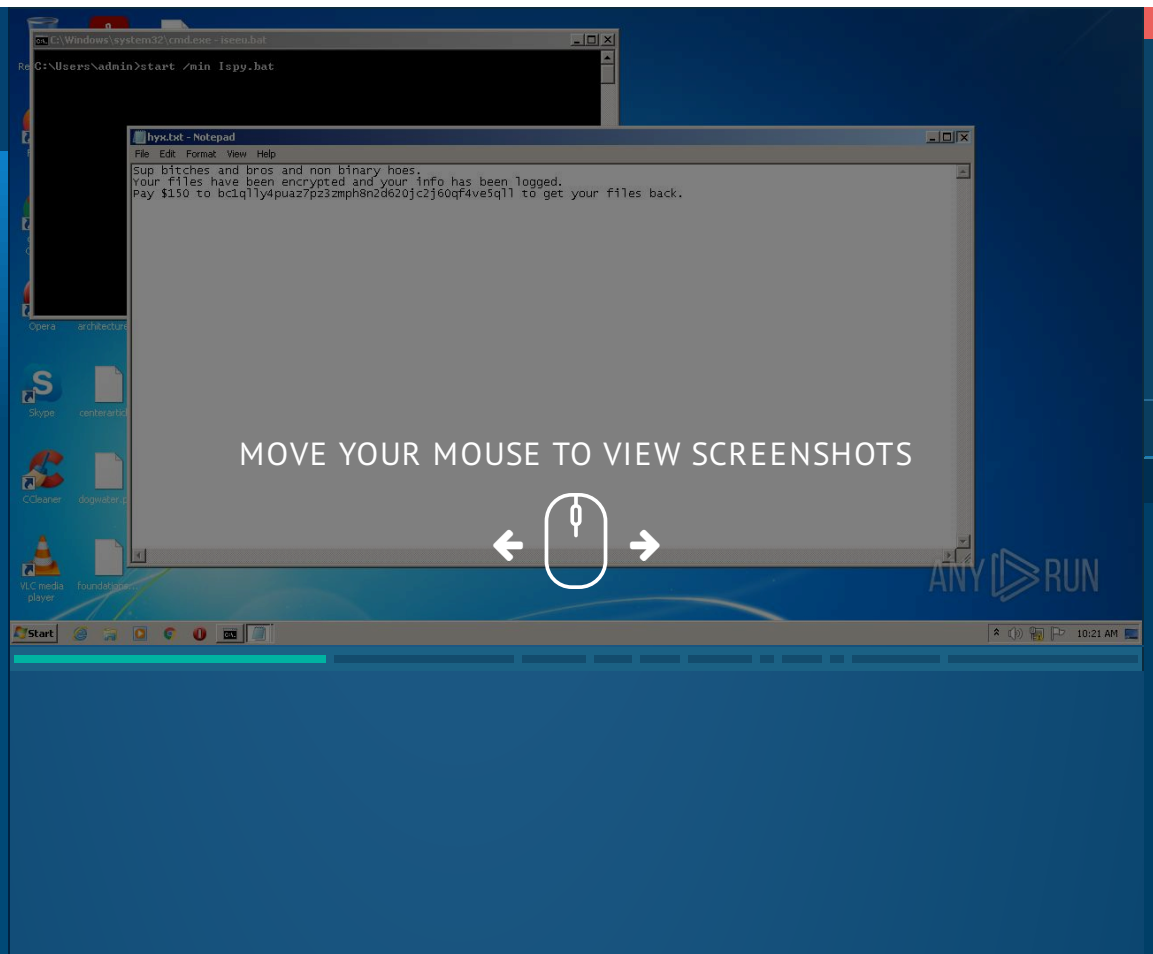

Malicious activity

hydroxide.cmd

Win7 32 bit
Complete

MD5: 46F64C63D63816C0511FE51198993BE7
Start: 04.06.2022, 11:20 Total time: 44 s

Indicators:

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes Filter by PID or name Only important

2952	cmd.exe	/c ""C:\Users\admin\Desktop\hydroxide.cmd" "	2k	724	51
2344	attrib.exe	+s +h "C:\Users\admin\Desktop\hydroxide.cmd"	49	9	15
956	reg.exe	add "hklm\Software\Microsoft\Windows\CurrentVersi...	34	6	17
2272	reg.exe	add HKEY_CURRENT_USER\Software\Microsoft\Wind...	34	6	17
3668	rundll32.exe	user32.dll, LockWorkStation	86	5	29
1836	net.exe	stop "SDRSVC"	196	7	19
3864	net1.exe	stop "SDRSVC"	80	12	21
676	net.exe	stop sharedaccess	76	6	18
1776	net1.exe	stop sharedaccess	80	12	21
2324	netsh.exe	firewall set opmode mode-disable	790	506	126
3144	net.exe	stop "wuauserv"	81	6	18
3392	net1.exe	stop "wuauserv"	85	12	21
3164	net.exe	stop "WinDefend"	81	6	18
3352	net1.exe	stop "WinDefend"	85	12	21
3216	taskkill.exe	/f /t /im "MSASCui.exe"	224	35	42
116	cmd.exe	/K iseeu.bat	386	86	48
1936	NOTEPAD.EXE	C:\Users\admin\hyx.txt	133	39	25
2108	NOTEPAD.EXE	C:\Users\admin\hyx.txt	123	39	25
4012	NOTEPAD.EXE	C:\Users\admin\hyx.txt	123	39	25
		dmin\hyx.txt	131	39	25
			115	5	39
		lock	500	3k	61

HTTP Requests 1 | Connections 1 | DNS Requests 1 | Threats 0

Filter by PID, name or url PCAP

NETWORK FILES DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
8136 ms	HEAD | 200: OK	?	3708	sipnotify.exe		http://query.prod.cms.rt.microsoft.co...	

Info [3708] sipnotify.exe Reads settings of System Certificates

Try community version for free! Register now