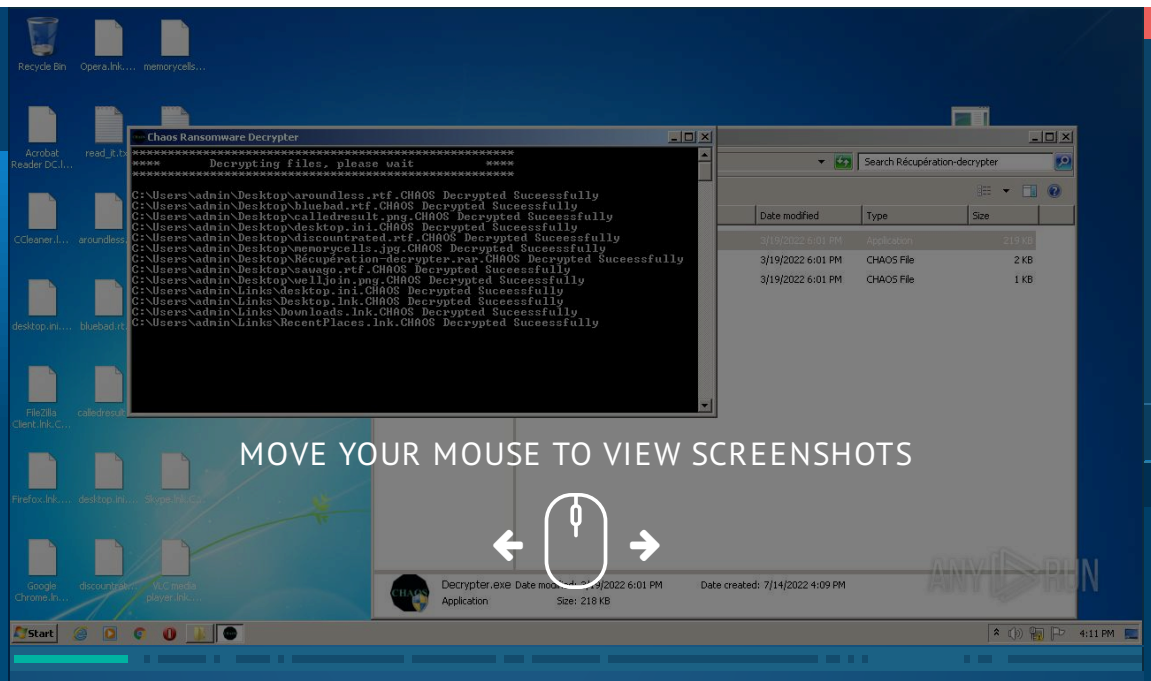

Malicious activity

CHAOS.rar

MD5: 290C887999CD7D055DF166753EA1005B

Start: 14.07.2022, 17:09 Total time: 158 s

Win7 32 bit Complete

ransomware

Indicators: Tracker: Ransomware

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes Filter by PID or name Only important

2936	WinRAR.exe	"C:\Users\admin\AppData\Local\Temp\CHAOS.rar"	1k	1k	90
2404	WinRAR.exe	"C:\Users\admin\Desktop\Récupération-decrypter.rar"	1k	832	88
2820	chrome.exe		3k	466	119
3280	chrome.exe	--type=crashpad-handler "--user-data-dir=C:\User...	111	9	22
2564	chrome.exe	--type=gpu-process --field-trial-handle=1048,5364...	431	23	77
2640	chrome.exe	--type=utility --utility-sub-type=network.mojom.Ne...	1k	5k	66
3168	chrome.exe	--type=renderer --field-trial-handle=1048,53647244...	265	17	48
1252	chrome.exe	--type=renderer --field-trial-handle=1048,53647244...	303	17	48
3616	chrome.exe	--type=renderer --field-trial-handle=1048,53647244...	265	17	48
1156	chrome.exe	--type=gpu-process --field-trial-handle=1048,5364...	419	22	76
2404	CHAOS.exe	PE	553	728	54
4060	svchost.exe	PE	10k	3k	73
3688	cmd.exe	/C vssadmin delete shadows /all /quiet & wmic...	308	18	15
2132	vssadmin.exe	delete shadows /all /quiet	115	23	25
1364	WMIC.exe	shadowcopy delete	237	62	52
1024	cmd.exe	/C bcdedit /set {default} bootstatuspolicy ignor...	254	17	14
4064	bcdedit.exe	/set {default} bootstatuspolicy ignoreall...	17	46	8
3348	bcdedit.exe	/set {default} recoveryenabled no	17	46	8
1236	cmd.exe	/C wbadmin delete catalog -quiet	215	17	14
		ete catalog -quiet	138	28	29
		rs\admin\AppData\Roaming\read_...	118	39	25
			195	34	47
			323	35	49

HTTP Requests 0 | Connections 8 | DNS Requests 5 | Threats 0 | Filter by PID, name or url | PCAP

Timeshift | Headers | Rep | PID | Process name | CN | URL | Content

No data

NETWORK FILES DEBUG

Info [4088] Decrypter.exe Dropped object may contain Bitcoin addresses

Try community version for free! Register now

New analysis | Reports | TI | Pricing | Contacts | FAQ | Sign In