Malicious activity

appveif.exe

MD5: C6DE457D1B6481B0FF2B387E03E99E08

Start: 16.07.2018, 01:01 Total time: 120 s

Win7 32 bit Complete

miner

Indicators:

Tracker: Crypto malware

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes | Filter by PID or name | Only important

1752	appveif.exe	PE	1k	49	60
2052	cmd.exe	/c schtasks /delete /tn * /f	91	6	26
1436	schtasks.exe	/delete /tn * /f	87	0	46
3628	cmd.exe	/c schtasks /create /sc minute /mo 1 /tn "Miscfos...	92	6	26
3916	schtasks.exe	/create /sc minute /mo 1 /tn "Miscfosthk...	91	0	48
2148	cmd.exe	/c schtasks /create /sc minute /mo 1 /tn "Netfram...	92	6	26
1436	schtasks.exe	/create /sc minute /mo 1 /tn "Netframew...	91	0	59
588	cmd.exe	/c schtasks /create /sc minute /mo 1 /tn "Flashhkn"...	93	6	26
764	schtasks.exe	/create /sc minute /mo 1 /tn "Flashhkn" /ru...	91	0	48
2352	cmd.exe	/c net stop SharedAccess	114	6	28
2224	net.exe	stop SharedAccess	108	0	38
1516	net1.exe	stop SharedAccess	74	0	42
2108	cmd.exe	/c net stop MpsSvc	114	6	28
2688	net.exe	stop MpsSvc	107	0	38
2860	net1.exe	stop MpsSvc	77	0	42
960	cmd.exe	/c net stop LanmanServer	115	6	28
2904	net.exe	stop LanmanServer	108	0	38
768	net1.exe	stop LanmanServer	83	0	42
808	cmd.exe	/c sc config LanmanServer start= disabled	91	6	26
		...erver start= disabled	20	0	16
		...binpath= system32\drivers\npf.sys...	91	6	26
		...path= system32\drivers\npf.sys typ...	20	0	26
		...ptonight -o mine.ppxxmr.com:7777 -...	7	0	6

HTTP Requests 1 | Connections 4 | DNS Requests 3 | Threats 0 | Filter by PID, name or url | PCAP

NETWORK | FILES | DEBUG

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content

Warning [2632] taskmgr.exe Connects to unusual port

Try community version for free! Register now