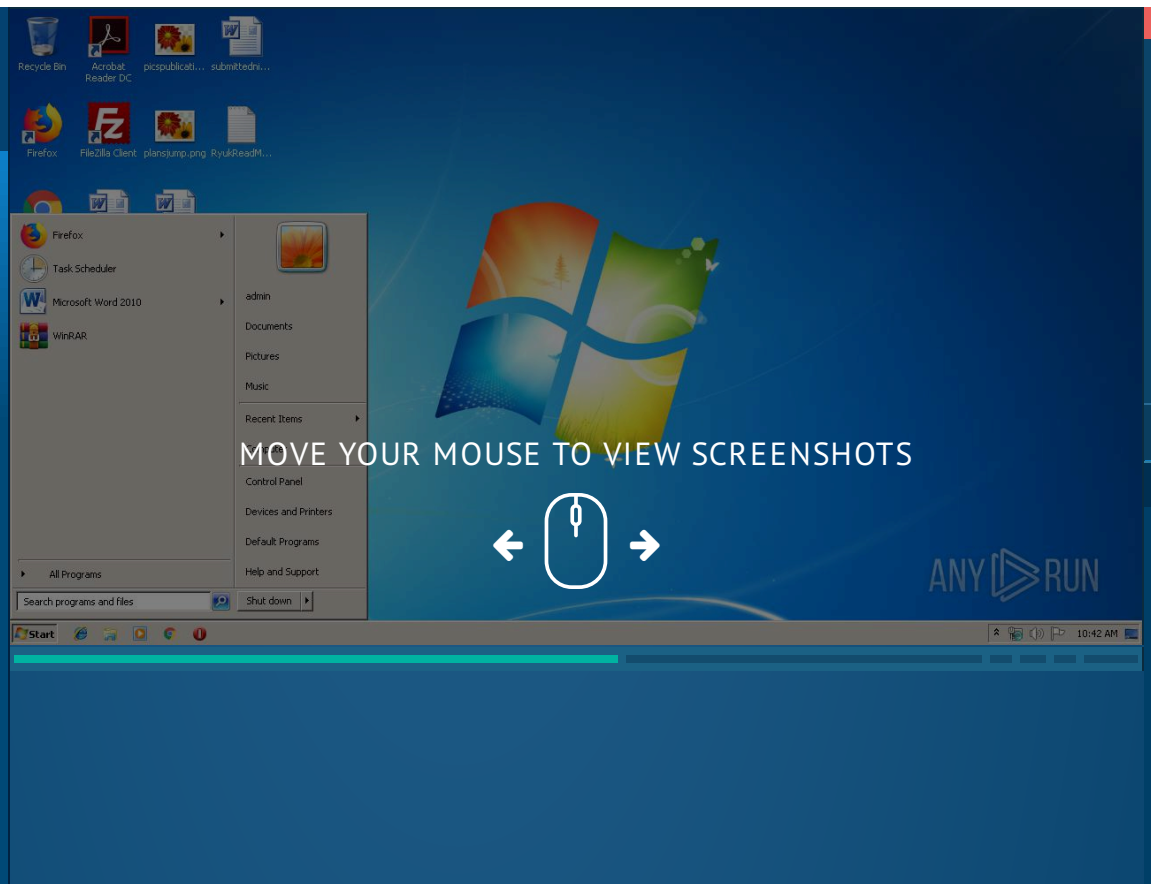

Malicious activity

23f8aa94ffb3c08a62735fe7fee5799880...

MD5: 5AC0F050F93F86E69026FAEA1FBB4450

Start: 05.10.2019, 11:41 Total time: 60 s

Win7 32 bit Complete

ransomware ryuk

Indicators: Tracker: Ransomware, Ryuk

Get sample | IOC | MalConf | Restart

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

CPU RAM

Processes Filter by PID or name Only important

3204	23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a1...	PE	369	32	76
2580	QsibK.exe	PE	C:\Users\admin\AppData\Local\Temp\23f8...	232	31 72
3960	cmd.exe	/C REG ADD "HKEY_CURRENT_USER\SOFTWAR...	99	6	26
1812	reg.exe	ADD "HKEY_CURRENT_USER\SOFTWARE\Mi...	44	1	34
1964	INJ	taskeng.exe	{B236C082-55A0-4F95-A52C-EEA3BD9C4422}	81k	0 42
360	INJ	ctfmon.exe	18	0	27
2004	INJ	dwm.exe	18	0	34
2152	INJ	windanr.exe	27	0	28
84876	NOTEPAD.EXE	C:\Users\admin\Desktop\RyukReadMe.txt	93	14	25

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

NETWORK FILES DEBUG

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

No data

Info [84876] NOTEPAD.EXE Manual execution by user

Try community version for free! Register now