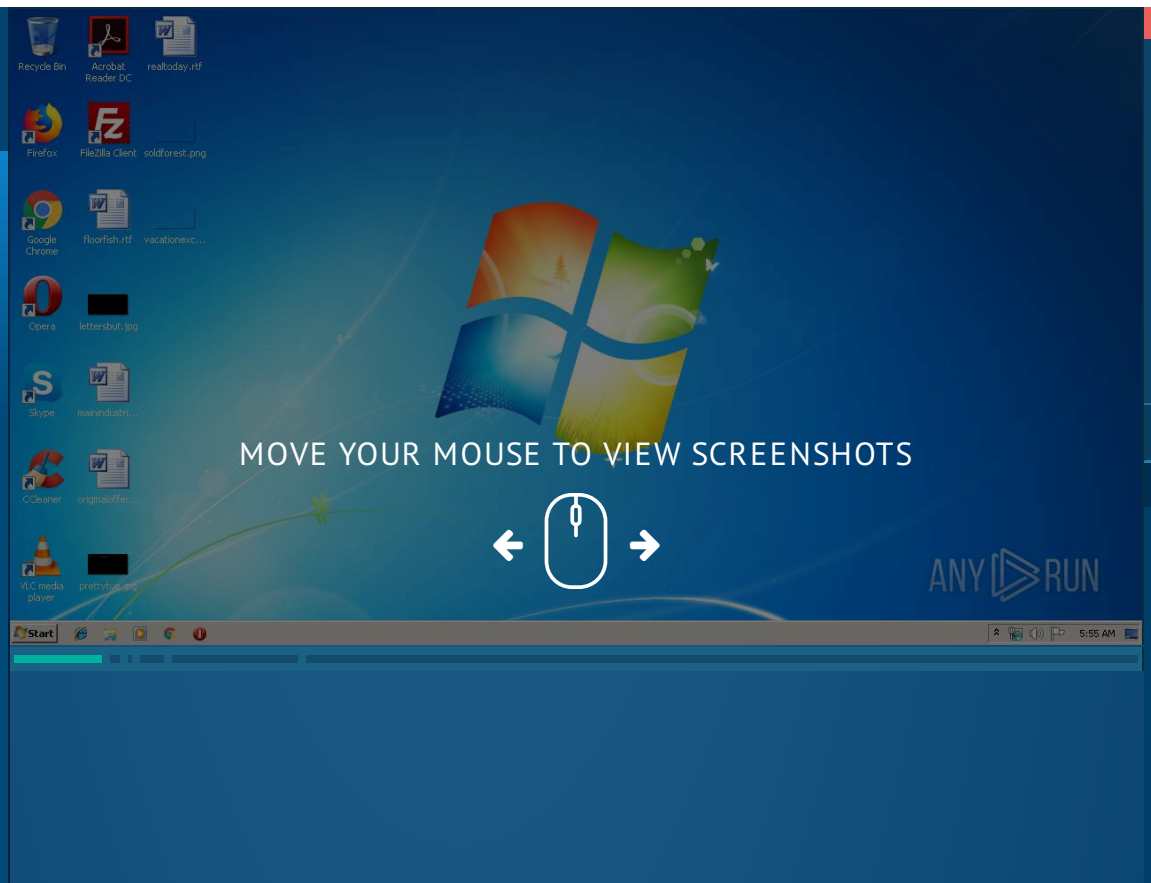


Malicious activity

General Specification.rar

MD5: 8ACC96E991578B42285287CE35238D49
Start: 24.09.2019, 06:55 Total time: 240 s

Win7 32 bit
Complete

trojan formbook stealer

Indicators: Tracker: Formbook, Stealer, 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

| | | | | | | |
|---|---|---|---|---|---|---|
| 236 | SUS | explorer.exe | formbook | 836 | 23 | 186 |
| 2920 | | WinRAR.exe "C:\Users\admin\AppData\Local\Temp\General ... | | 1k | 460 | 194 |
| 2536 | | General Specification.exe PE | | 318 | 0 | 62 |
| 1512 | | General Specification.exe PE | | 283 | 0 | 58 |
| 3984 | | services.exe | formbook | 565 | 11 | 45 |
| 2488 | | cmd.exe /c del "C:\Users\admin\AppData\Local\Temp\R... | | 59 | 6 | 24 |
| 2704 | | Firefox.exe | formbook | 321 | 0 | 98 |
| 3028 | | taskhost9rzxoh4x.exe PE | | 232 | 0 | 60 |
| 2452 | | taskhost9rzxoh4x.exe PE | | 229 | 0 | 58 |
| 4044 | | control.exe | | 42 | 0 | 34 |
| 2584 | COM | Copy/Move/Rename/Delete/Link Object | | 169 | 41 | 58 |

HTTP Requests 17 | Connections 17 | DNS Requests 10 | Threats 29 | Filter by PID, name or url | PCAP

NETWORK FILES DEBUG

| Timeshift | Headers | Rep | PID | Process name | CN | URL | Content |
|---|---|---|---|---|---|---|---|
| 61258 ms | GET \| 404: Not Found | ? | 236 | explorer.exe | | http://www.nhadatphugia.com/tl/?U4N... | |
| 84806 ms | GET \| 302: Found | ? | 236 | explorer.exe | | http://www.icemoa.com/tl/?U4Nh=IAL... | 2 |
| 87878 ms | POST \| No Response | ? | 236 | explorer.exe | | http://www.icemoa.com/tl/ | 3 |
| 87889 ms | POST \| No Response | ? | 236 | explorer.exe | | http://www.icemoa.com/tl/ | |
| 88900 ms | POST \| No Response | ? | 236 | explorer.exe | | http://www.icemoa.com/tl/ | 10 |
| 104.26 s | GET \| 404: Not Found | ? | 236 | explorer.exe | | http://www.kabsolug.com/tl/?U4Nh=zI1... | 3 |
| 106.31 s | POST \| 404: Not Found | ? | 236 | explorer.exe | | http://www.kabsolug.com/tl/ | 3 2 |

Danger [2452] taskhost9rzxoh4x.exe Application was dropped or rewritten from another process

Try community version for free! Register now