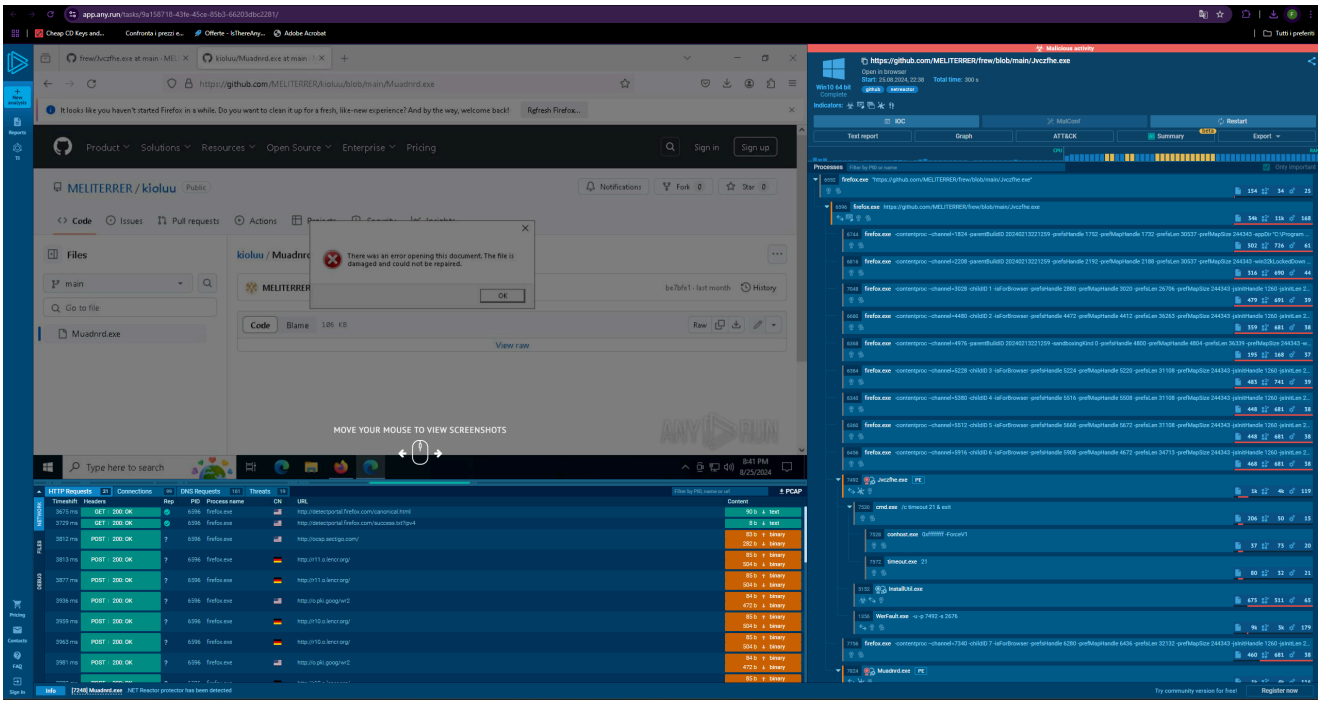
BW3 es.5 Bonus 1 Malware Jvczfhe.exe

Introduzione all'Analisi del Malware

⚜️ **Tag:** #malware #analisi #security

Questo report descrive l'analisi del file sospetto `Jvczfhe.exe`, identificato come malware tramite piattaforma di sandbox online (ANY.RUN). L’analisi rivela comportamenti sospetti che includono manipolazione dei registri, tentativi di elusione dei sistemi di rilevamento, e connessioni a porte non usuali.



Comportamenti Sospetti Osservati

⚜️ **Tag:** #comportamenti_sospetti #rilevamento

1. **Modifica delle impostazioni di sicurezza:** Il malware accede e altera le impostazioni di sicurezza del browser Internet Explorer e del

registro di sistema di Windows, con l'obiettivo di ottenere un controllo più profondo sul sistema infettato.

2. **Esecuzione di comandi e manipolazione del sistema:** Avvia comandi tramite il prompt dei comandi di Windows (`cmd.exe`), utilizzando anche `timeout.exe` per ritardare operazioni, tecnica usata per eludere il rilevamento automatico.
3. **Connessioni a porte inusuali:** `InstallUtil.exe` ha stabilito connessioni tramite porte non usuali, comportamento tipico di tentativi di esfiltrazione o download di componenti malevoli.

Modifiche ai Registri - Registry Modifications

⚜️ **Tag:** #registri #modifiche

Il malware esegue modifiche a chiavi di registro critiche per l'ambiente di sistema:

- **Chiavi Modificate:** `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing`
- **Attività:** Disabilita funzionalità di tracciamento (`EnableFileTracing`, `EnableAutoFileTracing`), configura bypass del proxy in `Internet Settings\ZoneMap`.

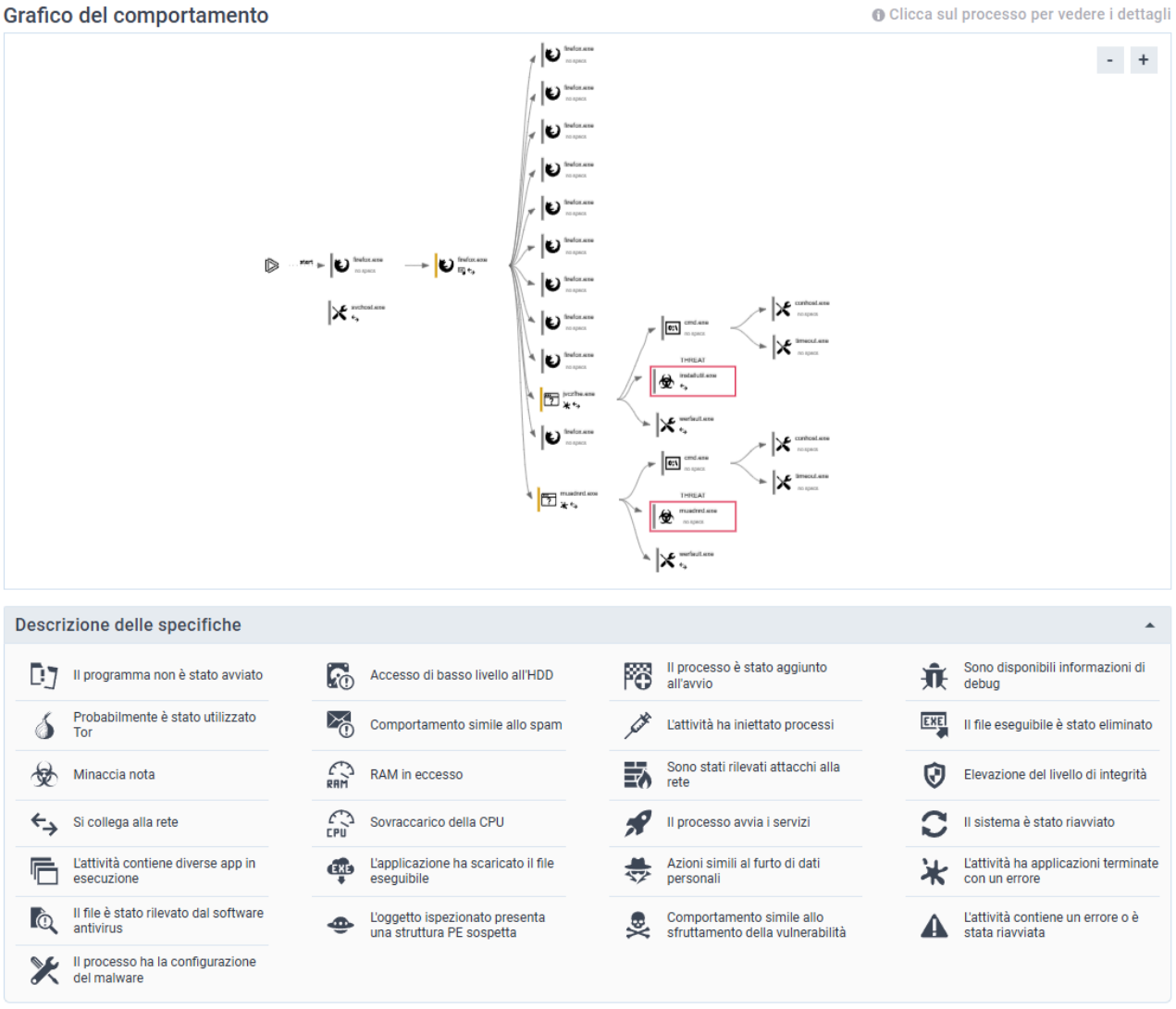
Processi Coinvolti

⚜️ **Tag:** #processi #auto_lancio

Il malware coinvolge diversi processi, tra cui:

- **`Muadnrd.exe` e `Jvczfhe.exe`:** Processi auto-lanciati e usati per avviare comandi tramite `cmd.exe`.

- `InstallUtil.exe`: Strumento di .NET Framework usato per stabilire connessioni sospette e modificare i registri.



Evasione dei Sistemi di Rilevamento - Evasion Techniques

⚜️ **Tag:** #evasione #sistemi #uac

1. **Disabilitazione dei log di traccia:** `Jvczfhe.exe` disabilita log fondamentali per il monitoraggio delle attività sospette, come `EnableConsoleTracing` e `EnableFileTracing`, occultando le proprie azioni.

2. **Autoconferma dei ANY.RUN es.2.2.pdfpermessi di amministratore (UAC):** Il malware utilizza funzionalità di autoconferma UAC per ottenere permessi senza notificare l'utente, ampliando la possibilità di modifiche a livello di sistema.

Remediation Consigliata

⚜️ **Tag:** #remediation #prevenzione

1. **Eliminazione immediata:** Il file deve essere rimosso dal sistema per prevenire danni ulteriori.
2. **Messa in quarantena:** Se l'eliminazione immediata non è possibile, è consigliata la quarantena del file per evitare che continui a essere eseguito o infetti altre parti del sistema.
3. **Blacklist dei vettori d'infezione:** Aggiungere `Jvczfhe.exe` e URL associati a una blacklist per evitare future infezioni.
4. **Conferma di malware vero:** Dati i comportamenti osservati, il file è confermato come malware (vero positivo).

🔑 **Chiavi:**
[malware, evasione, registri, connessioni_sospette, esfiltrazione, criptazione, processi, UAC, rilevamento, remediation]

Per ulteriori informazioni consultare il report

in allegato: Report Anyrun Malware Jvczfhe.pdf

ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

URL:	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe
Full analysis:	https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package