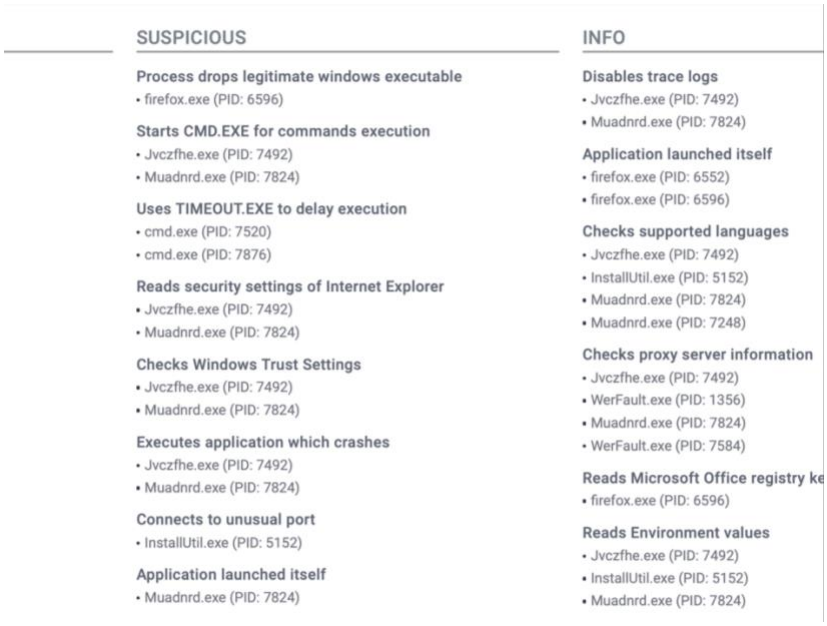
ESERCIZIO SETTIMANALE 2, S11L5:

Studiare questo link di anyrun e spiegare queste minacce in un piccolo report:
https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

SVOLGIMENTO:

Per eseguire questo esercizio, oltre ad analizzare il link, ho scaricato il report di anyrun per visualizzare informazioni dettagliate riguardo le potenziali minacce rilevate:



SUSPICIOUS

Process drops legitimate windows executable
• firefox.exe (PID: 6596)

Starts CMD.EXE for commands execution
• Jvczfhe.exe (PID: 7492)
• Muadnrd.exe (PID: 7824)

Uses TIMEOUT.EXE to delay execution
• cmd.exe (PID: 7520)
• cmd.exe (PID: 7876)

Reads security settings of Internet Explorer
• Jvczfhe.exe (PID: 7492)
• Muadnrd.exe (PID: 7824)

Checks Windows Trust Settings
• Jvczfhe.exe (PID: 7492)
• Muadnrd.exe (PID: 7824)

Executes application which crashes
• Jvczfhe.exe (PID: 7492)
• Muadnrd.exe (PID: 7824)

Connects to unusual port
• InstallUtil.exe (PID: 5152)

Application launched itself
• Muadnrd.exe (PID: 7824)

INFO

Disables trace logs
• Jvczfhe.exe (PID: 7492)
• Muadnrd.exe (PID: 7824)

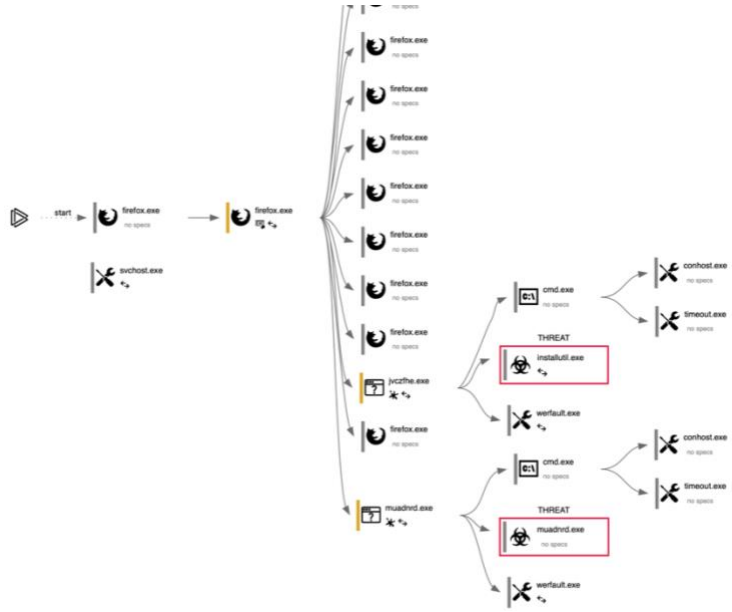
Application launched itself
• firefox.exe (PID: 6552)
• firefox.exe (PID: 6596)

Checks supported languages
• Jvczfhe.exe (PID: 7492)
• InstallUtil.exe (PID: 5152)
• Muadnrd.exe (PID: 7824)
• Muadnrd.exe (PID: 7248)

Checks proxy server information
• Jvczfhe.exe (PID: 7492)
• WerFault.exe (PID: 1356)
• Muadnrd.exe (PID: 7824)
• WerFault.exe (PID: 7584)

Reads Microsoft Office registry ke
• firefox.exe (PID: 6596)

Reads Environment values
• Jvczfhe.exe (PID: 7492)
• InstallUtil.exe (PID: 5152)
• Muadnrd.exe (PID: 7824)



Di seguito le informazioni generali, comportamento e minacce rilevate:

Informazioni Generali:

- **Nome del file:** Jvczfhe.exe
- **Sistema operativo analizzato:** Windows 10 Pro (64-bit)
- **Verdetto:** Attività dannosa rilevata
- **Origine:** GitHub

Comportamento e Minacce Rilevate:

Processi sospetti:

- Jvczfhe.exe (PID: 7492) e Muadnrd.exe (PID: 7824)
- Modifica chiavi di registro sensibili, incluse impostazioni di sicurezza e proxy.
- Lettura di dati di sistema, inclusi GUID macchina e impostazioni proxy.
- Esecuzione di comandi tramite CMD.exe, con utilizzo di time-out per ritardare operazioni (tecnica di evasione).
- Creazione di file o cartelle nella directory dell'utente.

Persistenza e Manomissione del Sistema:

- **Modifica delle impostazioni di Windows Trust** per potenziale bypass dei controlli di sicurezza.
- **Disabilitazione dei log di traccia**, nascondendo le attività dannose.
- **Lettura di chiavi di registro di Microsoft Office e Internet Explorer**, possibile tentativo di furto di credenziali o informazioni utente.

Attività di Rete e Connessioni:

- **InstallUtil.exe (PID: 5152) ha effettuato connessioni su porte inusuali**.
- **Possibile utilizzo di TOR** per offuscare il traffico e nascondere la comunicazione con server remoti.

Tecniche di Evasione:

- **Auto-esecuzione dei processi malevoli**, suggerendo un meccanismo di autorigenerazione.

Value: 0000000000805C4000000002011096A40000000C0BB3D8F400000000400189140

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing
Operation: write **Name:** EnableConsoleTracing
Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write **Name:** EnableFileTracing
Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write **Name:** EnableAutoFileTracing
Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write **Name:** EnableConsoleTracing
Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write **Name:** FileTracingMask
Value:

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write **Name:** ConsoleTracingMask
Value:

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** EnableFileTracing
Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** EnableAutoFileTracing
Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** EnableConsoleTracing
Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** FileTracingMask
Value:

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** ConsoleTracingMask
Value:

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** MaxFileSize
Value: 1048576

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** FileDirectory
Value: %windir%\tracing

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

Operation: write **Name:** ApplicationFlags
Value: 1

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** EnableFileTracing
Value: 0

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** EnableAutoFileTracing
Value: 0

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** EnableConsoleTracing
Value: 0

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** FileTracingMask
Value:

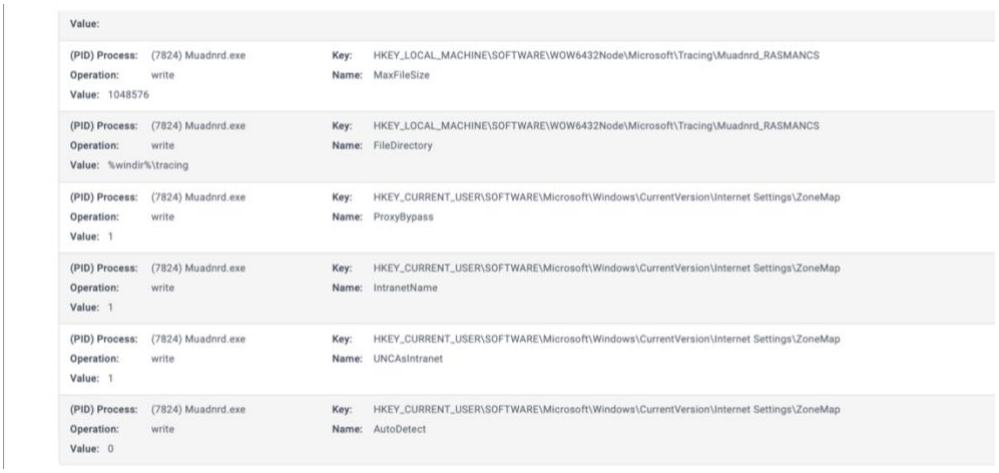
(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** ConsoleTracingMask
Value:

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** MaxFileSize
Value: 1048576

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** FileDirectory
Value: %windir%\tracing

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write **Name:** EnableFileTracing
Value: 0

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation: write **Name:** EnableAutoFileTracing



Questa breve analisi suggerisce che **Jvczfhe.exe è un malware con capacità avanzate di persistenza ed evasione**.

Le attività osservate suggeriscono che il file potrebbe essere:

- **Trojan** → Raccoglie informazioni di sistema e credenziali.
- **Downloader** → Scarica ed esegue ulteriori payload dannosi.
- **RAT (Remote Access Trojan)** → Potenzialmente utilizzabile per il controllo remoto del sistema compromesso.

Raccomandazioni di Sicurezza:

- **Isolare immediatamente il sistema infetto** per prevenire la diffusione del malware.
- **Eseguire una scansione completa con un antivirus aggiornato**.
- **Controllare eventuali modifiche alle chiavi di registro** e ripristinare i valori predefiniti.
- **Monitorare il traffico di rete per attività sospette**, specialmente connessioni a porte non standard.
- **Bloccare eventuali domini o IP sospetti associati all'attività di rete del malware**.