Esercizio 2: Studio IoC

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

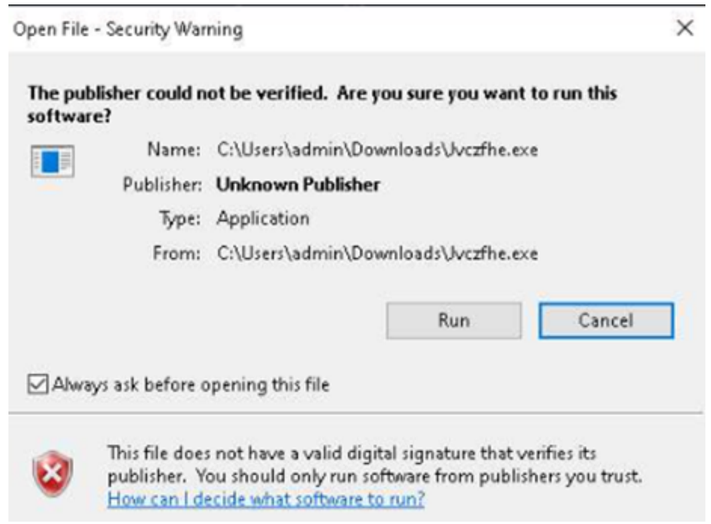
Indice

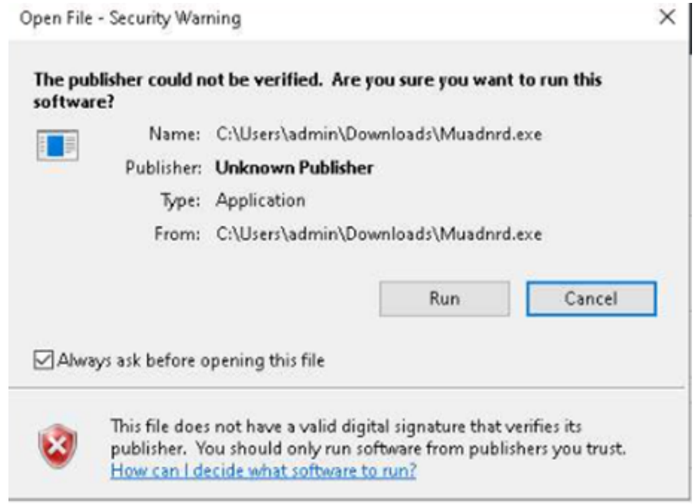
Descrizione dello scenario

Aperto il link appare subito l'azione intrapresa dall'utente della sandbox anyrun.

L'azione messa in atto prevedere il download da Github e l'installazione di due file eseguibili:

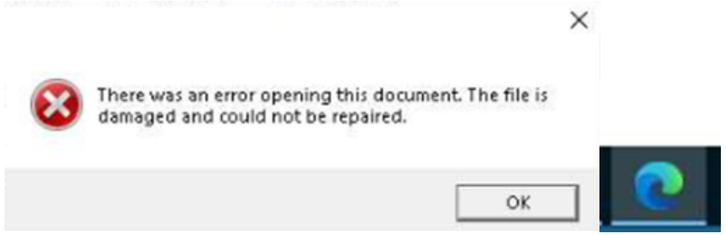
- Jvczfhe.exe;
- Muadnrd.exe.





Esecuzione Jvczfhe.exe

Una volta cliccato su run, appare sia l'icona di MicrosoftEdge sia un pop up di errore come a far intendere all'utente che il file è danneggiato e non è stato possibile eseguirlo.

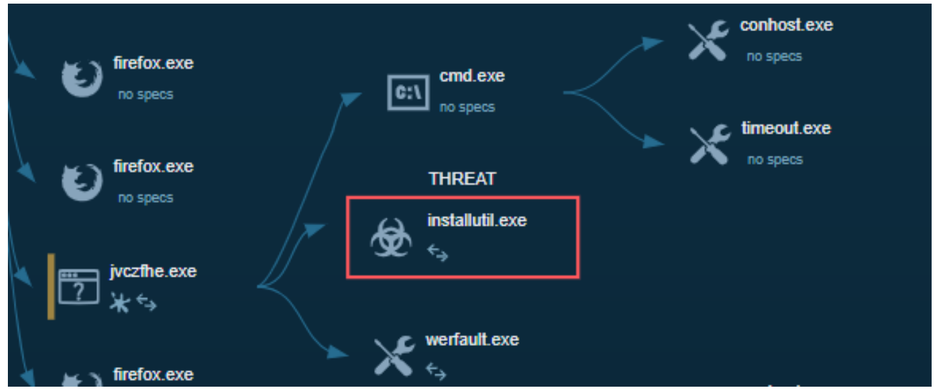


Ma sarà veramente così?

Parte 2

Esecuzione Jvczfhe.exe

In verità **Jvczfhe.exe** ha fatto diverse azioni e alcune abbastanza sospette:



- ·Esegue un processo che si blocca → Attività non usuale:
  Image: C:\Windows\SysWOW64\WerFault.exe
  Cmdline: C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676

- Legge le impostazioni di sicurezza → Warning System Security:
  Key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security
  Typevalue: REG_SZ

- Controlla le impostazioni di Sicurezza di Windows → Warning general:
  Value 146432
  key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\TrustProviders\SoftwarePublishing
  Typevalue: REG_DWORD

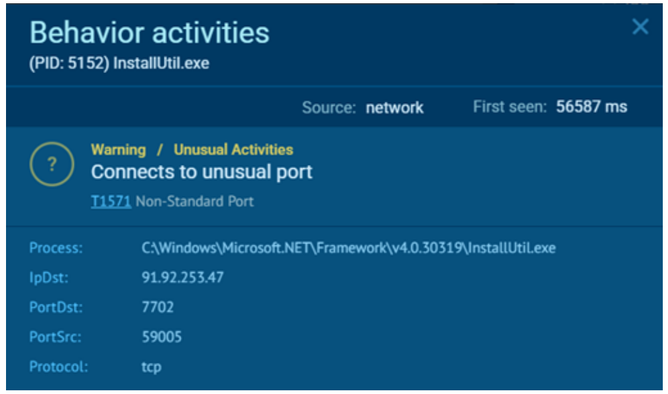
- Attiva CMD.exe per l'esecuzione dei comandi (Command Execution) → Warning general.
  Image: C:\Windows\SysWOW64\cmd.exe
  Cmdline: "cmd" /c timeout 21 & exit

- Crea un processo figlio conhost.exe

- Esegue un timeout 21.

- Il processo (PID: 5152) InstallUtil.exe si connette ad una porta non usuale → Unusual Activity

- ·Si rintraccia l'azione di .Net Reactor usato per prevenire la reverse engeneering e viene avviato il processo WerFault.exe un modulo di report errori di Windows

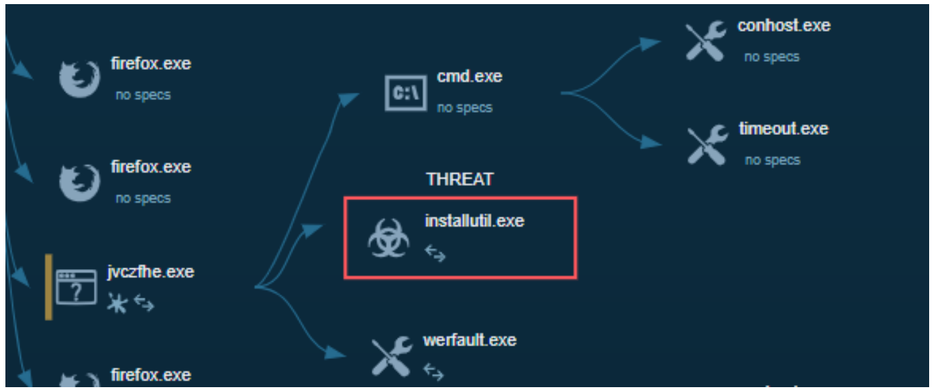


Giulia Campagna

Esecuzione Jvczfhe.exe

Indicatori di compromissione (IoC):

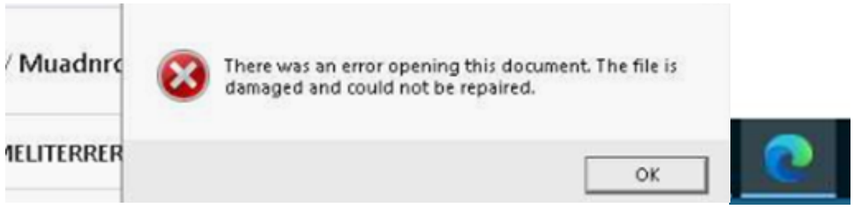
- La connessione alla rete avviata.
- Processo si è bloccato.
- Il certificato non è valido.
- Lettura delle chiavi di registro di windows.
- Attivazione CMD.exe per l'esecuzione dei comandi.
- Connessione del processo a porta non standard.
- Il punteggio assegnato da VirusTotal dopo l'analisi



Giulia Campagna

Esecuzione Muadnrd.exe

Anche il file eseguibile **Muadnrd.exe** pone in atto visivamente un comportamento simile facendo apparire un pop up di errore e una connessione a MicrosoftEdge.

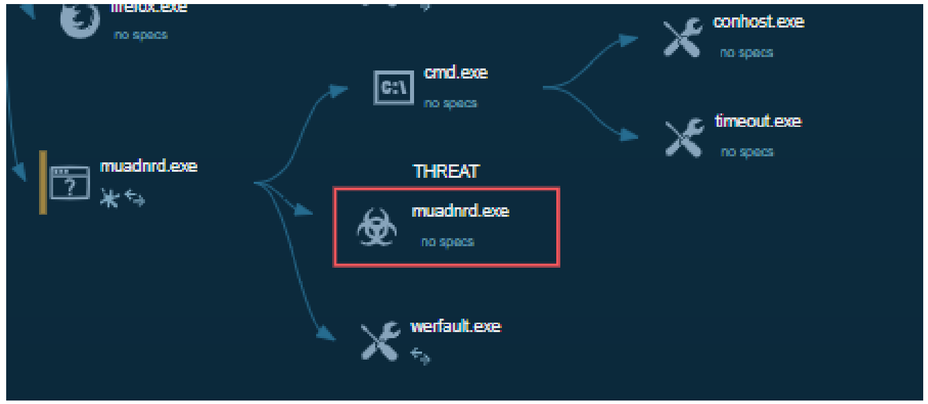


Avrà attuato altre azioni?
Saranno uguali o diverse rispetto all'altro file?

Parte 3

Esecuzione Muadnrd.exe

In verità anche **Muadnrd.exe** ha fatto diverse azioni.



- Esegue un processo che si blocca → Attività non usuale:
  Image: C:\Windows\SysWOW64\WerFault.exe
  Cmdline: C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7824 -s 2888

- Il programma si lancia da solo → Azione sospetta:
  image: C:\Users\admin\Downloads\Muadnrd.exe
  cmdChild: "C:\Users\admin\Downloads\Muadnrd.exe"
  cmdParent: "C:\Users\admin\Downloads\Muadnrd.exe"

- Controlla le impostazioni di Sicurezza di Windows → Warning general:
  Value 146432
  key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\TrustProviders\SoftwarePublishing
  Typevalue: REG_DWORD

- Legge le impostazioni di sicurezza → Warning System Security:
  Key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security
  Typevalue: REG_SZ

- Attiva CMD.exe per l'esecuzione dei comandi (Command Execution) → Warning general.
  Image: C:\Windows\SysWOW64\cmd.exe
  Cmdline: "cmd" /c timeout 21 & exit

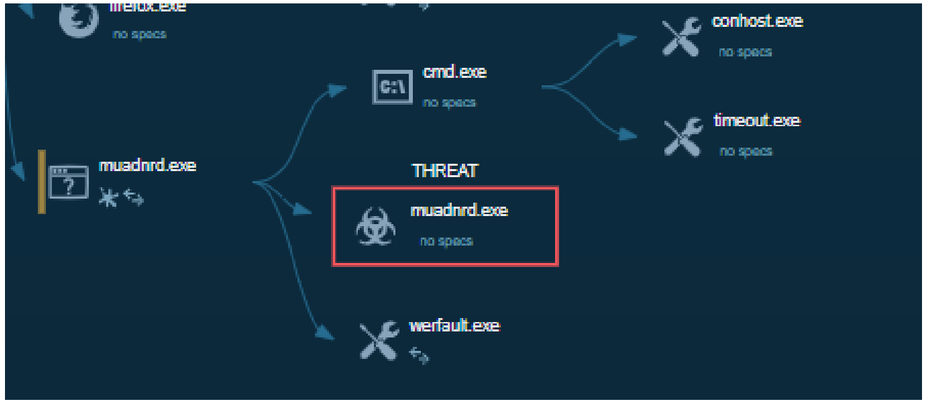
- ·Si rintraccia l'azione di .Net Reactor usato per prevenire la reverse engeneering e viene avviato il processo WerFault.exe un modulo di report errori di Windows

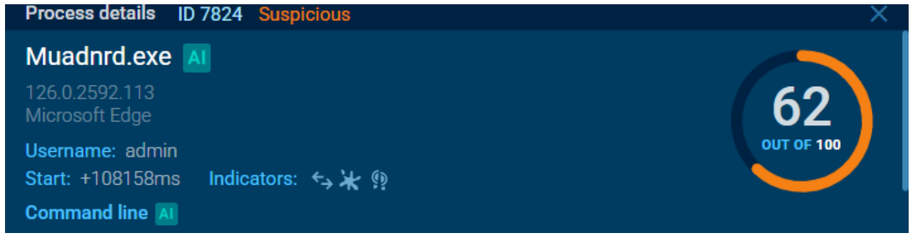
Giulia Campagna

Esecuzione Muadnrd.exe

Indicatori di compromissione (IoC):

- La connessione alla rete avviata.
- Il programma si avvia da solo.
- Processo si è bloccato.
- Il certificato non è valido.
- Lettura delle chiavi di registro di Windows.
- Attivazione CMD.exe per l'esecuzione dei comandi.
- Il punteggio assegnato da VirusTotal dopo l'analisi





Giulia Campagna

L’esercizio ha dimostrato quanto sia importante seguire le seguenti best practise:

- Non scaricare ed eseguire programmi e applicazioni che hanno una provenienza dubbia e autore sconosciuto e il certificato digitale scaduto o non valido.
- Prima di scaricare un file è sempre bene farlo esaminare da scanner di virus (come VirusTotal) per rilevare la presenza di malware e altri tipi di minacce.
- Se possibile eseguire, aprire e scaricare file di dubbia provenienza in un ambiente controllato come una sandbox come Cuckoo o VMFlare per evitare di compromettere il sistema.
- Aggiornare il Sistema Operativo con le ultime patch di sicurezza e mantenerlo sempre aggiornato.
- Installare un buon antivirus e mantenerlo sempre aggiornato.
- Implementare regole Firewall per vietare le connessioni su porte non usuali.

N.B: noto anche delle incongruenze nella sezione DNS Request ma non so interpretarle del tutto.