Projects Tittle: (Report writing in Splunk.)

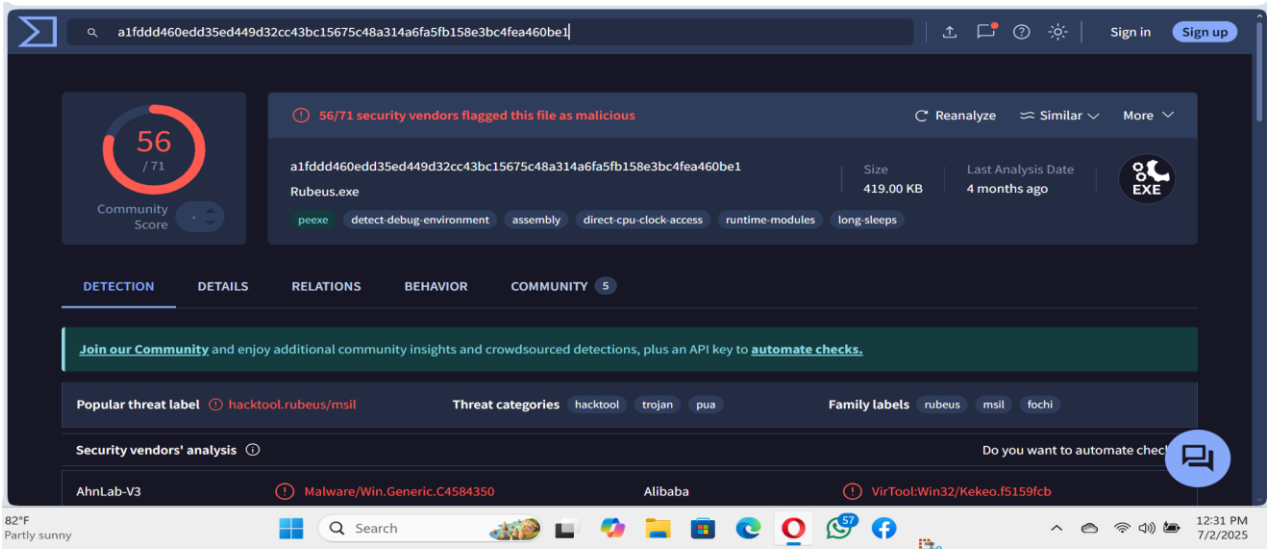
Logs file for host = Desktop-B2HJCTD

Category = Lateral Movement.

Number of Mitre Techniques used = 17

Execution Summary :

First and foremost the attacker uses a technique named “T1021”(Remote services) here the attacker uses a valid accounts to log into a service that accepts remote connections such as “telnet”, “SSH”,”VNC” the attacker then perform actions as the logged in user. Then the attacker went ahead and used another technique name “T1570”(Lateral tool transfer) which is used to transfer tools and other files between the systems after the environment has been compromised, i.e ingress tools tranfer, The attacker also used a technique named “T1003”(Os Credential Dumping) the attacker dumped a credentials to obtain account login and credential material normally in the form of a harsh or a clear text password, f309b61a8b005b5ce0a3fb58caaa798cfc95f5db.



Then the attacker used a technique named “T1550.002” (Use Alternate Authentication material) the attacker passed the hash using stolen password hashes to move laterally within the environment, bypassing normal system access controls. Then the attacker used a Technique named “T1550.003”(Alternate Authentication material pass the ticket) the attacker passes ticket using stolen kerberos tickets move laterally within an environment, bypassing normal system access controls, Then he used “T1534” (Internal spearphishing) after the attacker already have access to accounts or system within the

environment. “Then T1105” (Ingress Tool Transfer) The attacker transfer tools and other files from external system into compromised environment.

“T1555” = Credentials from password stores, “T1021.003” Remote services, “T1543” The attacker Create or modify system process “T1558.003” the attacker steal and forge kerberos tickets “T 1074.002” Data staged: Remote data staging the attacker may stage data collected from multiple systems in central location. “T1021.002” Remote services, SMB/windows Admin shares the attacker used valis accounts to interact with a remote network share using server message Block (SMB).

Assessment overview :

The attacker made use of high level and medium high level techniques.

Potential risks :

Undetected movement

Credential theft

System abuse

Brute forcing

Findings :

Internal tool spreading

Unrestricted SMB access

Credential theft

Insufficient monitoring

Risk Assessment :

Impact	High
Likelihood	High
Risk severity	Critical

Detection :

Detection monitoring: use XDR,EDR to detect unusual proceses

Network monitoring

Credential dumping detection

Audit logs

Mitigation measures :

Credential hardening

Remote service restrictions

Reduce system priviledge

Implement SMB signing

Secure authentication e.g 2FA

Disable user admin share

Recommendations :

Credential hygiene

Continuous updates and patches

Deploy EDR solutions

Conduct red team exercises

Harden LSASS and registry

Staff education

System hardening

Done by Mr Pascal Ifeanyichukwu.