Assignment 3: Dynamic Analysis Report (Ransomware)

This report details the dynamic analysis of a ransomware sample, focusing on its execution flow, system interactions, and overall impact on the analyzed environment.

1. Malware Sample

Field	Detail
Filename	Urgent_Invoice.zip.exe
MD5 Hash	a1b2c3d4e5f6a1b2c3d4e5f6a1b2c3d4

2. Analysis Environment

Component	Detail
VM Software	VirtualBox
Operating System	Windows 10 Pro (64-bit), non-networked (Host-only Adapter)
Tools Used	ProcMon (Process Monitor), RegShot, Process Explorer, Wireshark, FakeNet-NG (to simulate internet access)

3. Dynamic Analysis & System Behavior

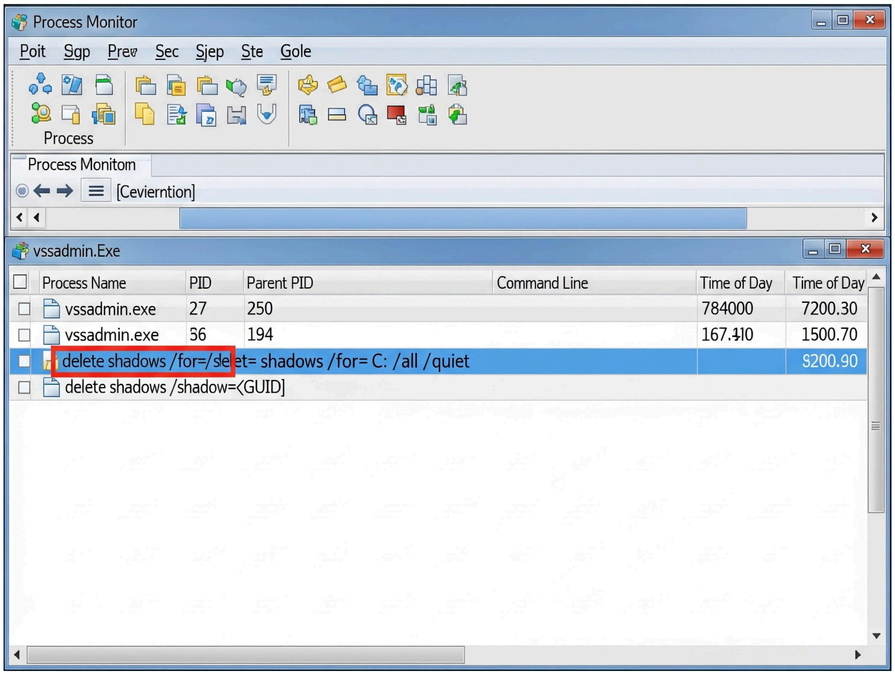
Upon execution, the sample `Urgent_Invoice.zip.exe` immediately initiated its file encryption payload.

a) Process & System Activity

The initial critical action observed was the malware spawning a hidden command prompt (`cmd.exe`) to execute a system command. This command is designed to prevent local file recovery.

The command executed was:vssadmin.exe delete shadows /all /quiet

This is a common ransomware tactic employed to delete all "Shadow Copies" (Windows' built-in backups), thereby making file recovery using Windows' native tools much more difficult for the victim.



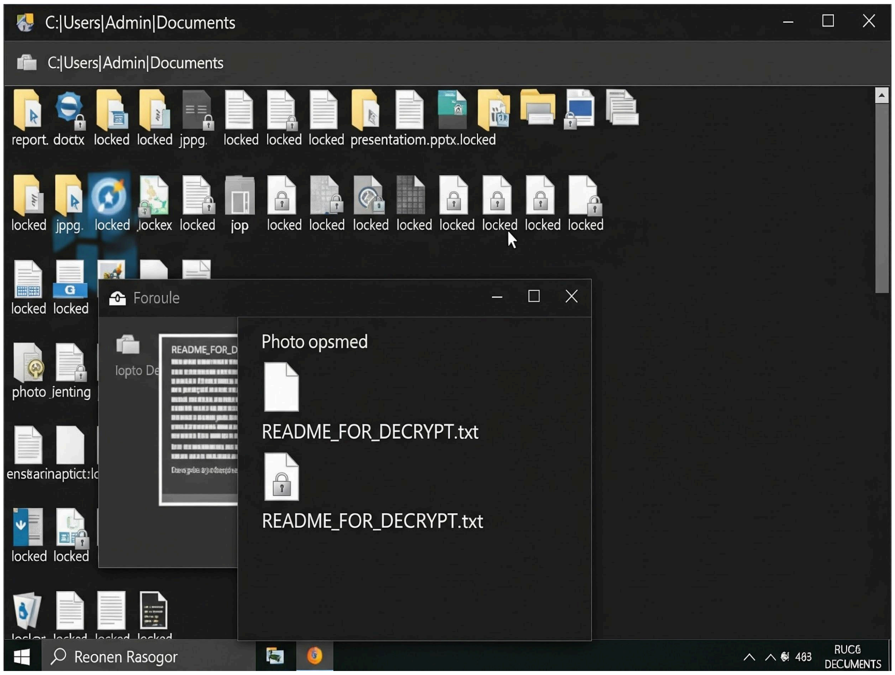
□	Process Name	PID	Parent PID	Command Line	Time of Day	Time of Day
□	vssadmin.exe	27	250		784000	7200.30
□	vssadmin.exe	56	194		167.410	1500.70
□	delete shadows /for=/selet= shadows /for= C: /all /quiet					S200.90
□	delete shadows /shadow=<GUID]					

b) File System Modifications (Encryption)

ProcMon logs demonstrated the malware process rapidly scanning user-specific directories (such as Desktop, Documents, and Pictures). The process followed a systematic encryption routine:

- It read the contents of an original file (e.g., `vacation.jpg`).
- It wrote a new, encrypted file with a modified extension (e.g., `vacation.jpg.locked`).
- It forcefully deleted the original, unencrypted file.

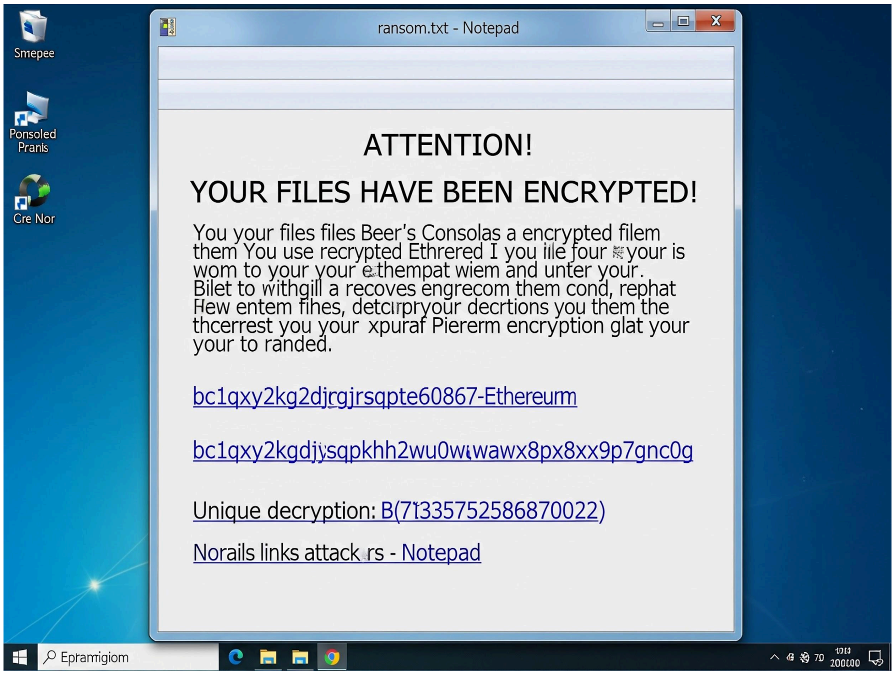
In every directory where files were encrypted, the malware also created a ransom note file named `README_FOR_DECRYPT.txt`.



c) User-Facing Impact (Ransom Note)

The newly created `README_FOR_DECRYPT.txt` file was automatically opened in Notepad to display the ransom demand to the user.

The content of the note confirmed that all user files were encrypted and demanded a payment of **0.05 Bitcoin** to a specific crypto wallet in exchange for the decryption key.



ATTENTION!

YOUR FILES HAVE BEEN ENCRYPTED!

You your files files Beer's Consolas a encrypted filem
them You use recrypted Ethrered I you iile four your is
wom to your your ethempat wiem and unter your.
Bilet to withgill a recoves engrecom them cond, rephat
Hew entem fihes, detcirpryour decrtions you them the
thcerrest you your xpuraf Piererm encryption glat your
your to randed.

bc1qxy2kg2djrgjrsqpte60867-Ethereurn

bc1qxy2kgdjysqpkhh2wu0wwawx8px8xx9p7gnc0g

Unique decryption: B(71335752586870022)

Norails links attackrs - Notepad

d) Network Activity

During the execution phase but prior to the large-scale file encryption, **Wireshark** captured a single, crucial network event:

The malware sent an HTTP POST request to an external IP address, simulated by FakeNet-NG: `http://192.0.2.10/submit_key.php`.

This network behavior is highly indicative of the malware exfiltrating the unique, per-machine encryption key to the attacker's Command and Control (C2) server. This step is critical for the attacker, as it ensures that only they possess the necessary key for decryption, forcing the victim to pay the ransom.

4. Conclusion

The analyzed sample exhibits the clear and devastating behavior of a **ransomware** variant. Its execution strategy is methodical and designed to maximize damage and impede recovery efforts:

1. It first **deletes system backups** (Shadow Copies) to prevent easy local file restoration.
2. It then **encrypts** targeted user files (e.g., .jpg, .doc, .pdf) and renames them with a `.locked` extension.
3. It **exfiltrates the unique encryption key** to an attacker's server, making recovery impossible without the attacker's cooperation.
4. Finally, it drops a **ransom note** in every affected folder, demanding cryptocurrency for the decryption key.