THREAT INTELLIGENCE

by VOJAACOM SOC TEAM

GROUP 4

INTRODUCTION

We were having a peaceful and cool saturday at Vojaacom Security Operation centre when we received an alert at 2:15 PM. A trusted cybersecurity partner, Val Agency had sent us 30 file hashes with a critical warning: 'One of these contains an active malware payload.'

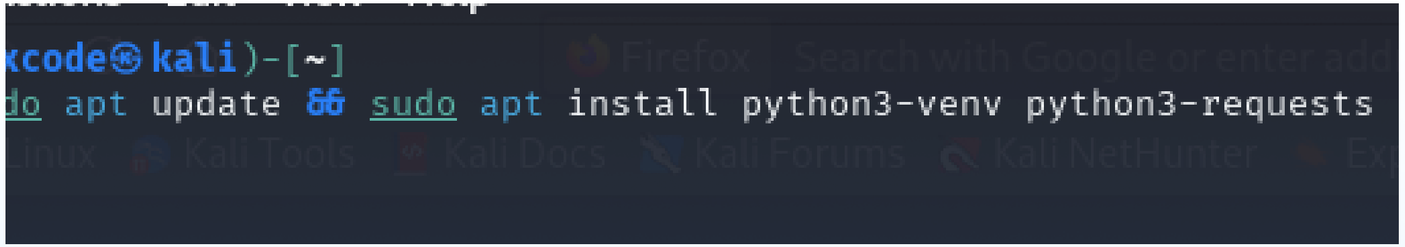
Our mission is to identify the malware type, conduct a thorough threat intelligence analysis, and develop yara rule and recommend solutions to counter the new threat.

LETS SHOW YOU HOW!!!

Tools

- Virustotal API
- Linux Terminal
- python
- Text Editor
- Threat Intelligence

Methodology



Created a python script

Detected the malicious Hash

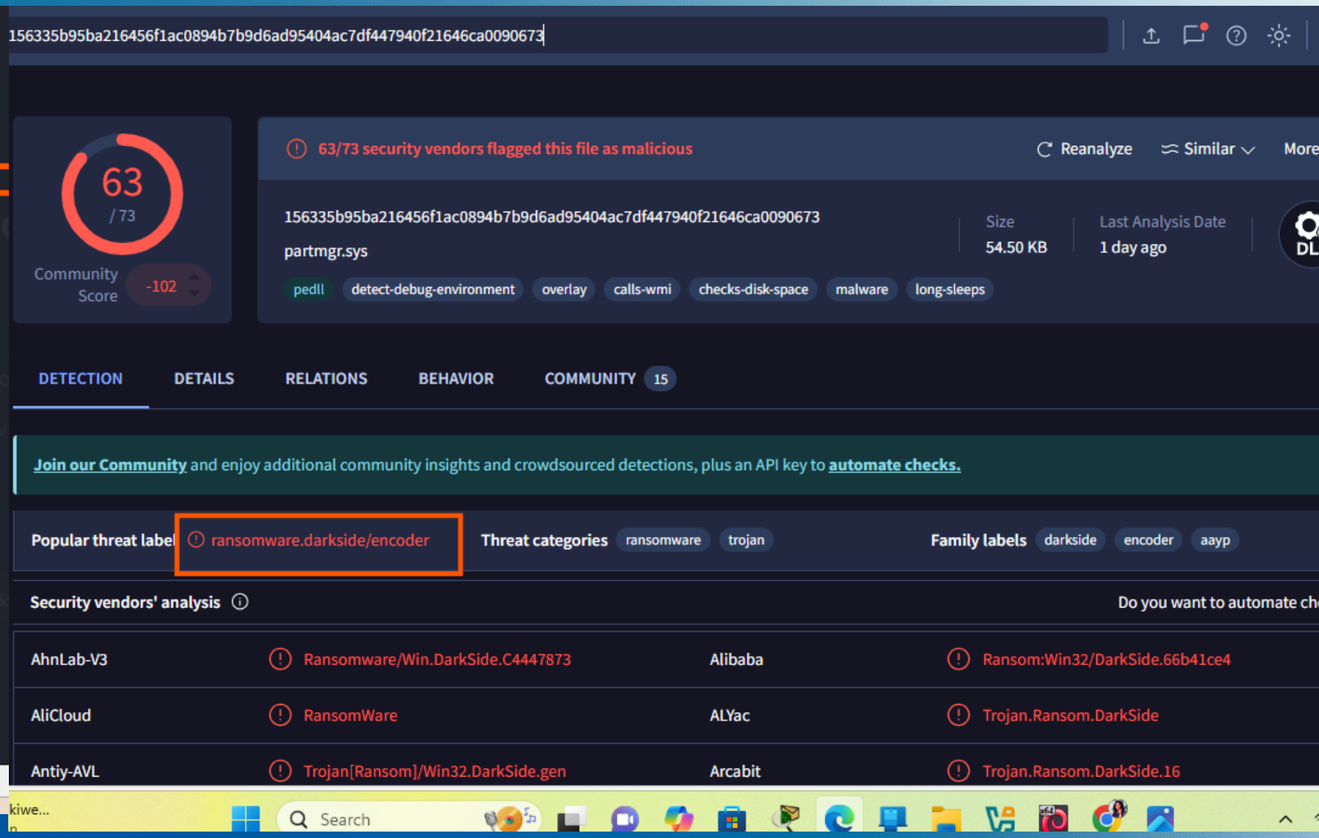
researched about the hash

created a Yara Rule

RESULT

```
┌──(vixcode㉿kali)-[~]
└─$ python3 check_hashes.py

Waiting for 60 seconds to stay within API rate limit...
Waiting for 60 seconds to stay within API rate limit...
Waiting for 60 seconds to stay within API rate limit...
Waiting for 60 seconds to stay within API rate limit...
56335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673 is flagged as malicious by:
- Bkav: W32.AIDetectMalware
- Lionic: Trojan.Win32.Encoder.U!c
- Elastic: Windows.Ransomware.Darkside
- Cynet: Malicious (score: 100)
- CAT-QuickHeal: Ransom.Darkside.S26339594
- Skyhigh: BehavesLike.Win32.Ursnif.qh
- ALYac: Trojan.Ransom.DarkSide
- Cylance: Unsafe
- Zillya: Trojan.Encoder.Win32.2315
- Sangfor: Ransom.Win32.Darkside.Vdw6
- K7AntiVirus: Trojan ( 005795061 )
- Alibaba: Ransom:Win32/DarkSide.66b41ce4
- K7GW: Trojan ( 005795061 )
- CrowdStrike: win/malicious_confidence_100% (W)
- huorong: Ransom/DarkSide.a
- Symantec: Ransom.Darkside
- ESET-NOD32: a variant of Win32/Filecoder.DarkSide.B
- APEX: Malicious
- Paloalto: generic.ml
- ClamAV: Win.Packed.DarkSide-9262656-0
- Kaspersky: Trojan-Ransom.Win32.Gen.aayp
- BitDefender: Gen:Variant.Ransom.DarkSide.16
- NANO-Antivirus: Trojan.Win32.Encoder.komjqz
```



ANALYSIS

Threat Intelligence Research: Darkside Ransomware

1. History: First emerged in 2020 but became prominent in 2021
2. Evolution : They operate as RANSOMWARE AS A SERVICE (RaaS)
3. Current Status: As of 2023, Darkside Ransomware is still active but, rebranded
4. Affiliated with: REvil and BlackMatter from russia
5. Motivation: financial gain
6. Notable Attack: Colonial Pipeline Attack (2021)

DarkSide Ransomware MITRE ATT&CK Mapping

Tactic (ID)	Technique (ID)	DarkSide Ransomware Activity
TA0001: Initial Access	T1566 (Phishing)	Phishing emails for initial entry.
	T1190 (Exploit Public-Facing App)	Exploits VPN/RDP vulnerabilities.
TA0002: Execution	T1059 (Command-Line Interface)	Uses cmd.exe/PowerShell for execution.
	T1204 (User Execution)	Tricks users into running malware.
TA0003: Persistence	T1053 (Scheduled Task)	Creates scheduled tasks for persistence.
	T1547.001 (Registry Run Keys)	Modifies registry for auto-start.
TA0004: Privilege Escalation	T1055 (Process Injection)	Injects code into legitimate processes.
	T1068 (Exploitation for Priv Esc)	Exploits Windows vulnerabilities.
TA0005: Defense Evasion	T1222 (File Permissions Mod)	Disables security tools via permission changes.
	T1027 (Obfuscated Files)	Uses encryption to evade detection.
TA0006: Credential Access	T1003 (OS Credential Dumping)	Uses Mimikatz for credential theft.
	T1110 (Brute Force)	Attacks RDP/VPN with brute force.
TA0007: Discovery	T1046 (Network Scanning)	Scans for vulnerable systems.
	T1083 (File & Directory Discovery)	Enumerates files before encryption.
TA0008: Lateral Movement	T1021 (Remote Services)	Moves via RDP/SMB/PsExec.
	T1550.002 (Pass the Hash)	Uses stolen credentials to spread.
TA0009: Collection	T1039 (Data from Network Shares)	Collects files from shared drives.
	T1560 (Archive Collected Data)	Compresses files before exfiltration.
TA0011: Command & Control	T1573 (Encrypted Channel)	Uses HTTPS/Tor for C2.
	T1043 (Commonly Used Port)	Communicates over ports 443/80.
TA0010: Exfiltration	T1041 (Exfiltration Over C2)	Sends stolen data to C2 servers.
	T1567 (Exfiltration Over Web)	Uses cloud storage for data leaks.
TA0040: Impact	T1486 (Data Encrypted for Impact)	Encrypts files for ransom.
	T1490 (Inhibit System Recovery)	Deletes backups & shadow copies.

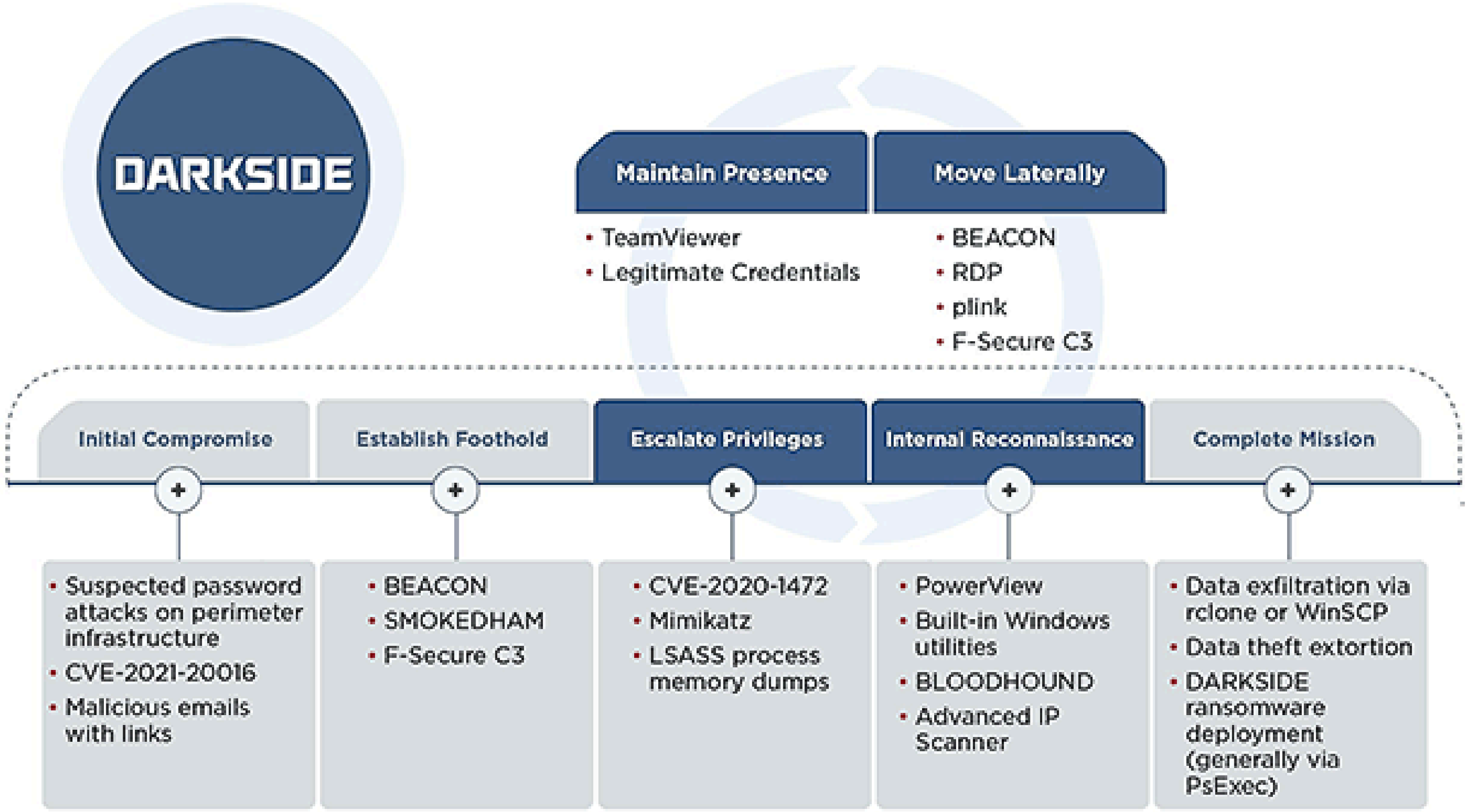
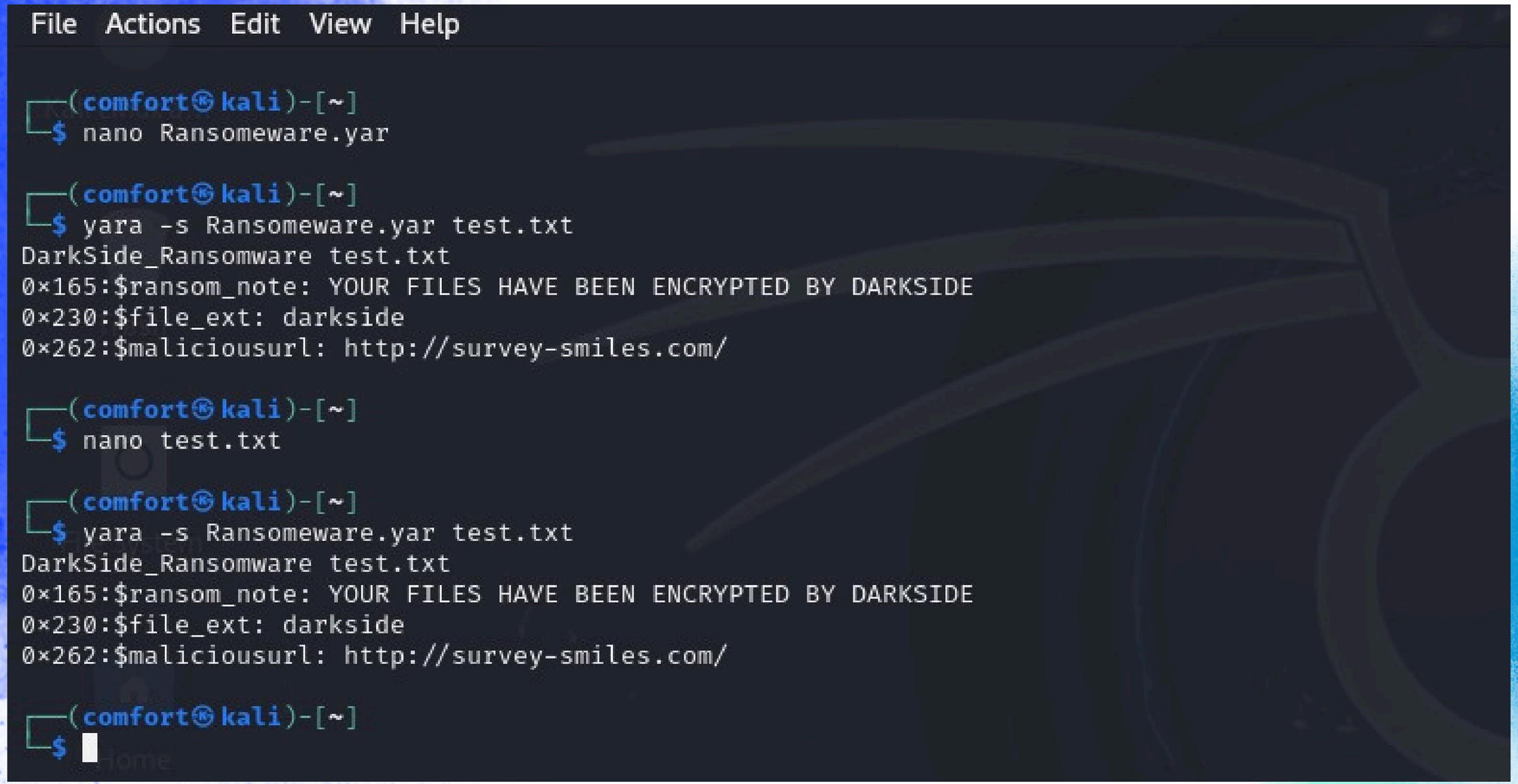


IMAGE SOURCE: HTTPS://WWW.FIREEYE.COM/CONTENT/DAM/FIREEYE-WWW/BLOG/IMAGES/DARKSIDE/FIG3B.PNG



TESTED YARA RULE TO DETECT DARKSIDE RANSOMEWARE

RECOMMENDATION

- **Implement Proactive Monitoring: Use threat intelligence feeds and tools like YARA to detect and respond to malware threats in real-time.**
- **Enhance Email Security: Deploy advanced email filtering solutions to block phishing attempts and malicious attachments.**
- **Regular System Updates: Ensure all systems are regularly updated with the latest security patches to mitigate vulnerabilities.**
- **Employee Training: Conduct regular cybersecurity awareness training to reduce the risk of social engineering attacks.**
- **Incident Response Planning: Develop and test an incident response plan to quickly contain and remediate malware infections.**

THANK YOU

TEAM MEMBERS

- Aderinola Kehinde
- Adebisi Mololuwa
- Nwobodo Chigozie
- Oghenetejiri Brume
- Victoria Simon
- Odunayo Balogun
- Gyekye micaiah Ampofo
- Aleka Moses Ogamodey
- Comfort Ukangwobia