Threat Intelligence Report

Darkside Ransomware

prepared by: Group 4

Date: March 25, 2025

Cyblack Soc Academy, 3’rd Cohort

This Report is a collective work compiled by all of the members of the cyblack soc academy 3'rd cohort, group 4

Group Members

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

Executive Summary

DarkSide ransomware poses a significant threat to modern organizations due to its sophisticated tactics, targeted attacks, and Ransomware-as-a-Service (RaaS) model. Since its emergence in mid-2020, DarkSide has continually evolved, adapting its operational methods despite increased law enforcement efforts and cybersecurity countermeasures.

Key Insights for Leadership:

- Threat Evolution: DarkSide has refined its tactics over time, emphasizing both data encryption and exfiltration.
- High-Profile Incidents: The attack on Colonial Pipeline and subsequent incidents underscore the potential for large-scale disruption and financial loss.
- Operational Complexity: The decentralized structure and RaaS model complicate attribution and containment, requiring a layered security approach.
- Mitigation Necessity: Proactive measures such as advanced endpoint detection, robust network segmentation, continuous monitoring of IOCs, and a well-practiced incident response plan are critical.

Key Findings

Historical Context & Notable Attacks

DarkSide ransomware first emerged in mid-2020 and quickly gained notoriety for its sophisticated tactics. One of the most high-profile incidents was the Colonial Pipeline attack in May 2021, which disrupted fuel supply chains across the United States, demonstrating the ransomware's ability to cripple essential services. Since its inception, DarkSide has evolved rapidly, refining its encryption techniques and data exfiltration methods to make detection and mitigation more challenging.

Threat Actor Profile

DarkSide operates under a Ransomware-as-a-Service (RaaS) model, allowing affiliates to deploy attacks while sharing ransom proceeds with the developers. This decentralized structure makes attribution difficult, as different groups can leverage the ransomware for their own attacks. The group employs advanced obfuscation and anonymization techniques to evade detection. There is also evidence suggesting potential affiliations with larger cybercriminal networks, as DarkSide shares infrastructure and attack methodologies with other ransomware groups.

Attack Lifecycle & Tactics

DarkSide typically gains initial access by exploiting vulnerabilities such as weaknesses in Remote Desktop Protocol (RDP) or through phishing attacks. Once inside a network, the ransomware moves laterally, leveraging built-in system tools to escalate privileges and gain control over critical assets. The attack process involves both data exfiltration and encryption, ensuring that victims face not only operational disruption but also the threat of sensitive information being leaked. Ransom notes are tailored to the target, outlining payment demands and the consequences of non-compliance.

Detection and Prevention Strategies

Effective defense against DarkSide requires a multi-layered security approach. Implementing advanced Endpoint Detection and Response (EDR) solutions can help identify and flag suspicious behaviors early. Network segmentation plays a critical role in preventing lateral movement, limiting the ability of attackers to compromise an entire infrastructure. Continuous monitoring using threat intelligence feeds and automated Indicator of Compromise (IOC) correlation through platforms like VirusTotal enhances proactive detection capabilities.

User awareness and training remain key components in reducing the risk of phishing and social engineering attacks, which are often the initial entry points for ransomware. Additionally, maintaining secure offline backups is essential for ensuring business continuity and rapid recovery in the event of an attack.

Report Overview

This report documents the analysis of a dataset containing Thirty SHA-256 hash values to identify a malicious sample associated with a resurfaced malware strain. Using the VirusTotal API, a Python script was developed to automate the analysis of each hash. A malicious hash was identified, and thorough threat intelligence research was conducted to understand the malware's history, tactics, and impact. Based on the findings, a YARA rule was created to detect the malware in future attacks. The report concludes with recommendations for proactive cybersecurity measures to mitigate similar threats.

Lab Objectives

The primary objectives of this lab were:

Identify the Malicious Hash: Use the VirusTotal API to analyze 50 SHA-256 hash values and identify a malicious sample.

Conduct Threat Intelligence Research: Investigate the malware's history, tactics, and impact.

Create a YARA Rule: Develop a YARA rule to detect the malware based on its hash, strings, file characteristics, and behavioral indicators.

Prepare a Comprehensive Report: Document the analysis, findings, and recommendations for executive leadership.

Tools and Resources Used

VirusTotal API: Used to analyze hash values and identify malicious samples.

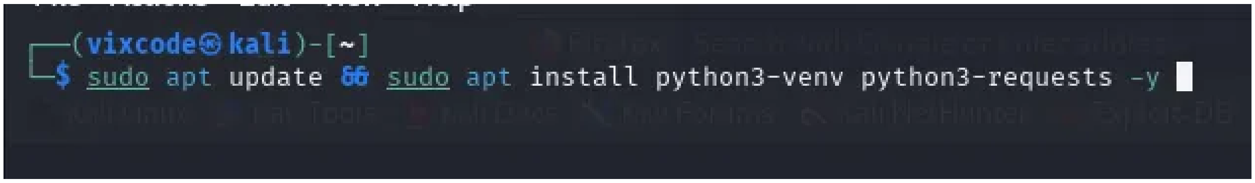
Python: Used to automate the hash analysis process with the requests library.
YARA: Used to create a detection rule for the identified malware.
Text Editor: Used to write and edit the Python script and YARA rule.
Threat Intelligence Sources: Used to research the malware's history, tactics, and impact.

Methodology

The lab was conducted in the following steps:

Install Required Packages
Installed the requests library in Python to interact with the VirusTotal API.

```
sudo apt update && sudo apt install python3-venv python3-requests -y
```

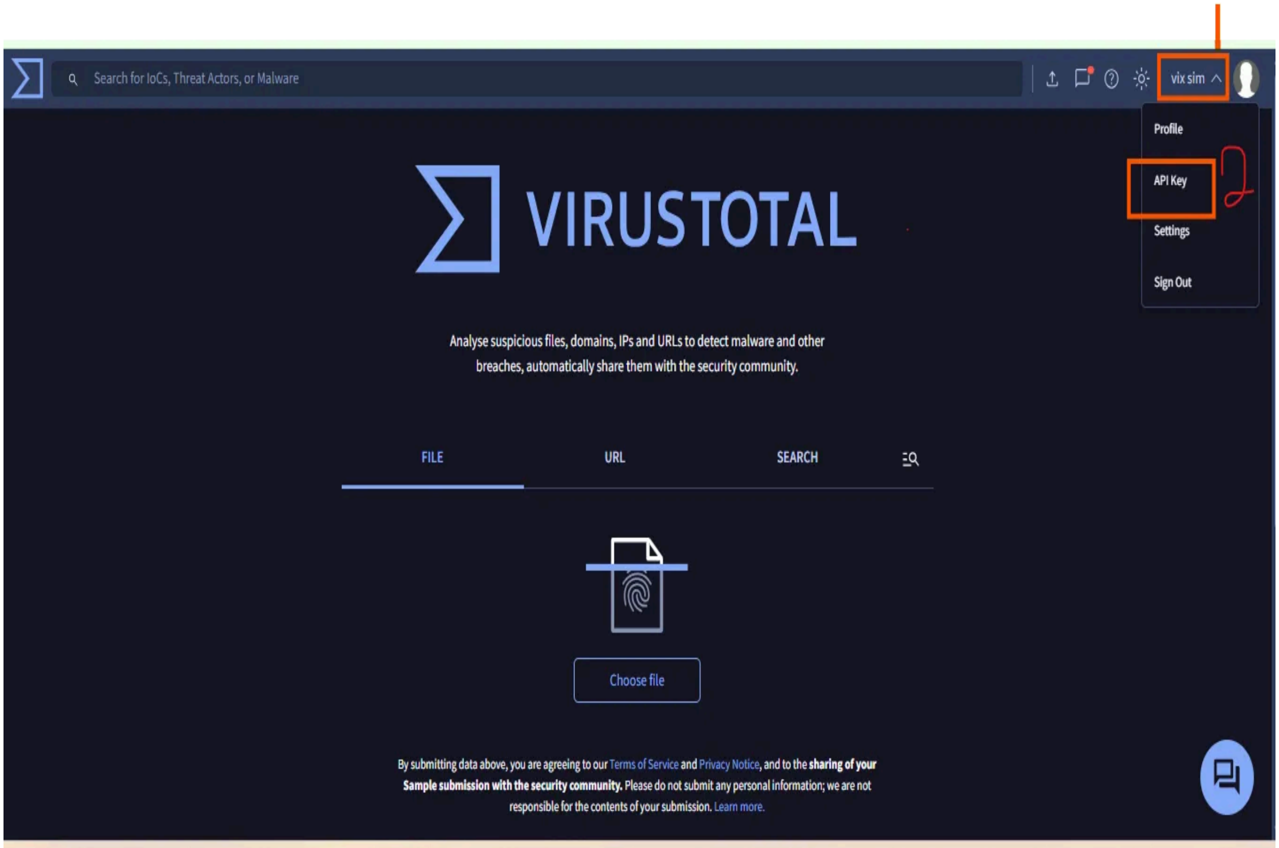


```
┌──(vixcode㉿kali)-[~]
└─$ sudo apt update && sudo apt install python3-venv python3-requests -y
```

Bash shell running the python3-request command

Obtain VirusTotal API Key

Signed up for a VirusTotal account and obtained an API key.



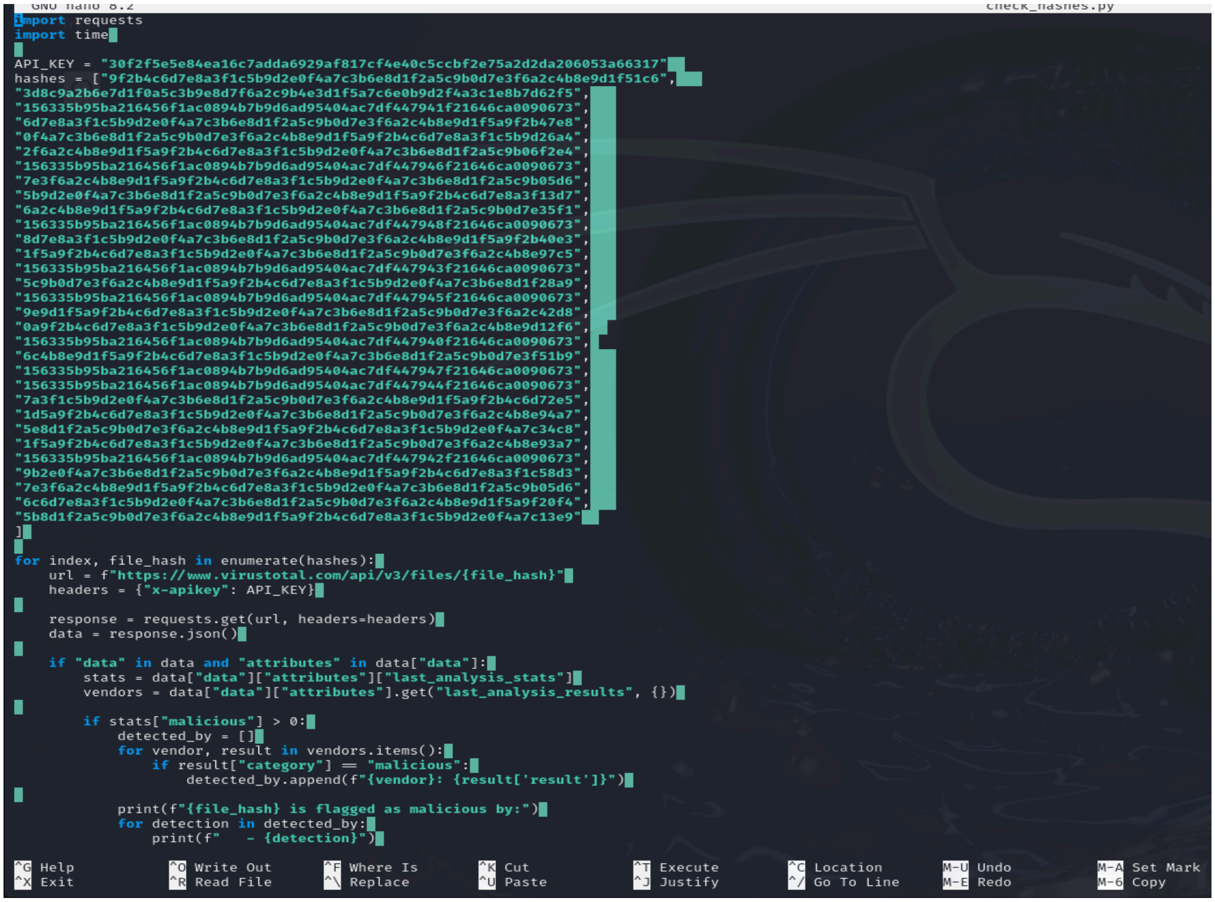
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

VirusTotal API

Create Python Script

Developed a Python script (check_hashes.py) to automate the analysis of 50 SHA-256 hash values using the VirusTotal API.

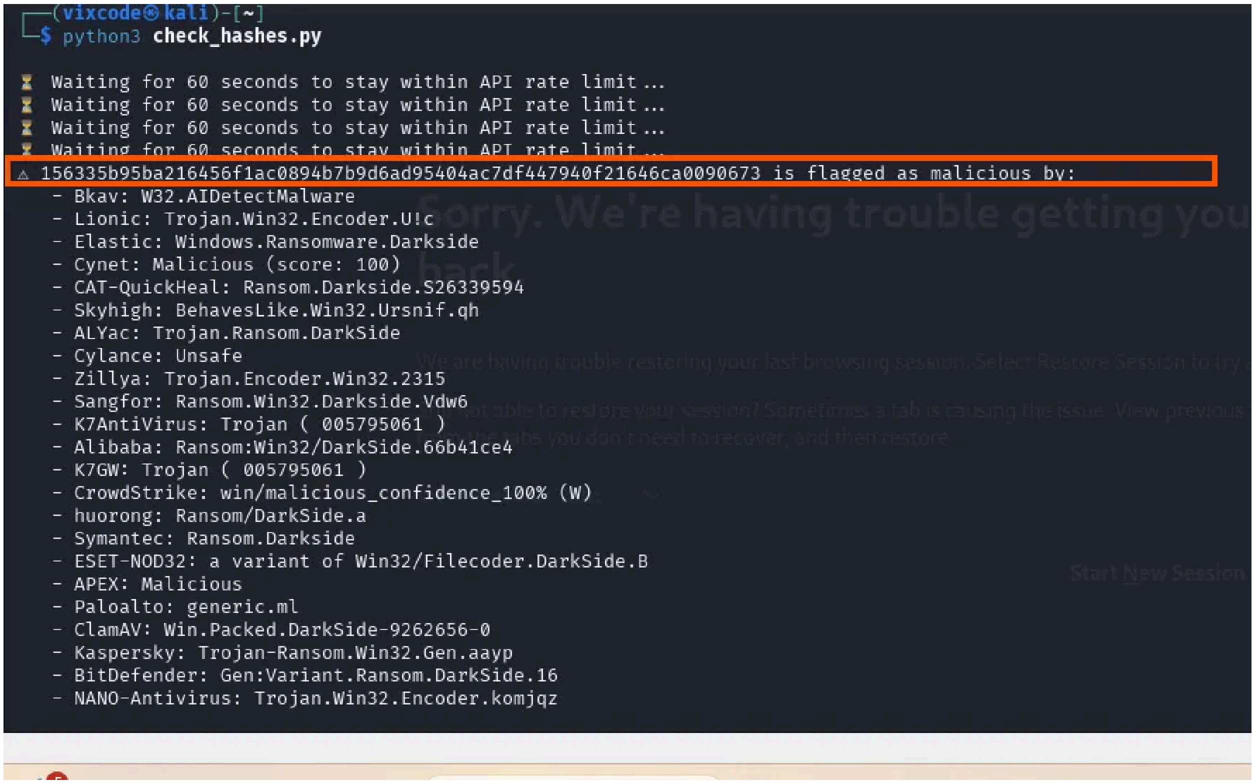


```
import requests
import time

API_KEY = "30f2f5e5e84ea16c7adda6929af817cf4e40c5ccbf2e75a2d2da206053a66317"
hashes = ["9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f51c6",
"3d8c9a2b6e7d1f0a5c3b9e8d7f6a2c9b4e3d1f5a7c6e0b9d2f4a3c1e8b7d62f5",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447941f21646ca0090673",
"6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b47e8",
"0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d26a4",
"2f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b06f2e4",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447946f21646ca0090673",
"7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b05d6",
"5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f13d7",
"6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e35f1",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447948f21646ca0090673",
"8d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b40e3",
"1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e97c5",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447943f21646ca0090673",
"5c9b0d7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f28a9",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447945f21646ca0090673",
"9e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c42d8",
"0a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d12f6",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673",
"6c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f51b9",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447947f21646ca0090673",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447944f21646ca0090673",
"7a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b4c6d72e5",
"1d5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e94a7",
"5e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c34c8",
"1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e93a7",
"156335b95ba216456f1ac0894b7b9d6ad95404ac7df447942f21646ca0090673",
"9b2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c58d3",
"7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b05d6",
"6c6d7e8a3f1c5b9d2e0f4a7c3b6e8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f20f4",
"5b8d1f2a5c9b0d7e3f6a2c4b8e9d1f5a9f2b4c6d7e8a3f1c5b9d2e0f4a7c13e9"
]

for index, file_hash in enumerate(hashes):
    url = f"https://www.virustotal.com/api/v3/files/{file_hash}"
    headers = {"x-apikey": API_KEY}

    response = requests.get(url, headers=headers)
    data = response.json()

    if "data" in data and "attributes" in data["data"]:
        stats = data["data"]["attributes"]["last_analysis_stats"]
        vendors = data["data"]["attributes"].get("last_analysis_results", {})

        if stats["malicious"] > 0:
            detected_by = []
            for vendor, result in vendors.items():
                if result["category"] == "malicious":
                    detected_by.append(f"{vendor}: {result['result']}")

            print(f"{file_hash} is flagged as malicious by:")
            for detection in detected_by:
                print(f"    - {detection}")
```

Python Script for Detecting Malicious Hash

Run the Script

Executed the script to identify the malicious hash and extract relevant details from VirusTotal's response.

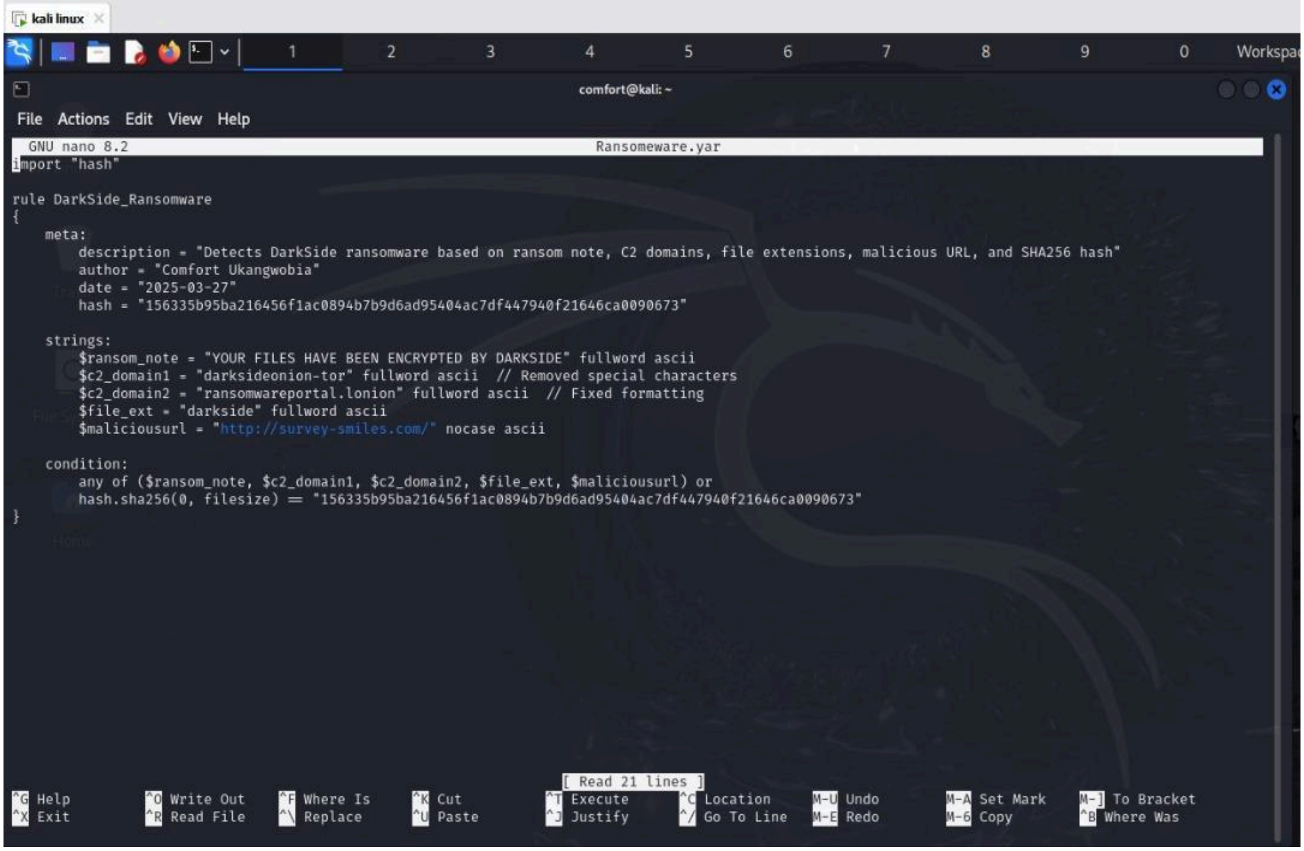


```
┌──(vixcode㉿kali)-[~]
└─$ python3 check_hashes.py

⌛ 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 ...
⚠ 156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673 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
```

Flagged Malicious Hash

Conduct Threat Intelligence Research
Researched the malware's history, notable attacks, threat actors, motivation, tactics, attack lifecycle, current status, and detection strategies.

Create YARA Rule
Developed a yara rule to detect the ransomware based on the hash, strings, URL and ransom note

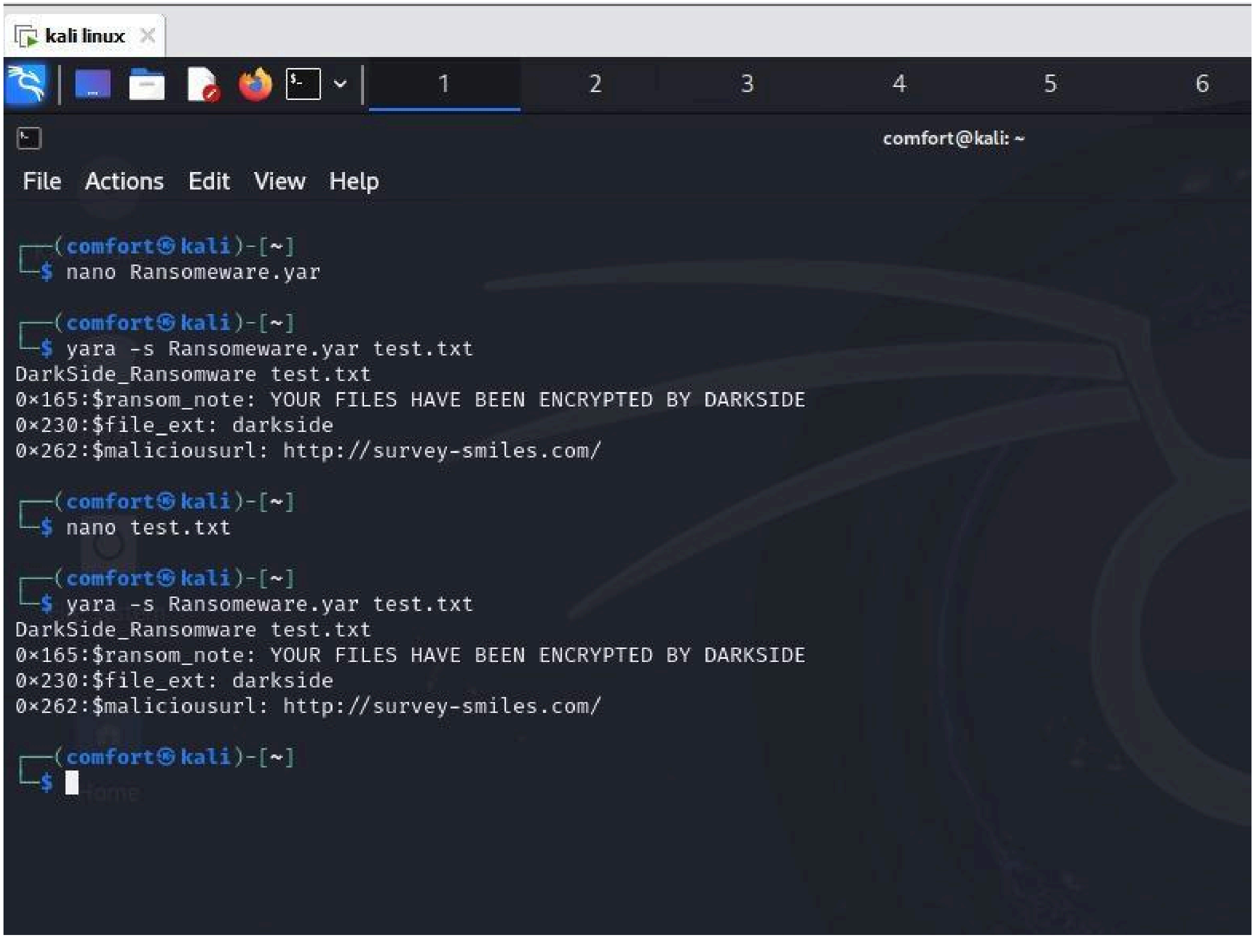


```
import "hash"

rule DarkSide_Ransomware
{
    meta:
        description = "Detects DarkSide ransomware based on ransom note, C2 domains, file extensions, malicious URL, and SHA256 hash"
        author = "Comfort Ukangwobia"
        date = "2025-03-27"
        hash = "156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673"

    strings:
        $ransom_note = "YOUR FILES HAVE BEEN ENCRYPTED BY DARKSIDE" fullword ascii
        $c2_domain1 = "darksideonion-tor" fullword ascii  // Removed special characters
        $c2_domain2 = "ransomwareportal.lonion" fullword ascii  // Fixed formatting
        $file_ext = "darkside" fullword ascii
        $maliciousurl = "http://survey-smiles.com/" nocase ascii

    condition:
        any of ($ransom_note, $c2_domain1, $c2_domain2, $file_ext, $maliciousurl) or
        hash.sha256(0, filesize) == "156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673"
}
```

```
[ Read 21 lines ]
```

Test the YARA Rule

Tested the YARA rule on the identified malicious sample to ensure accurate detection.

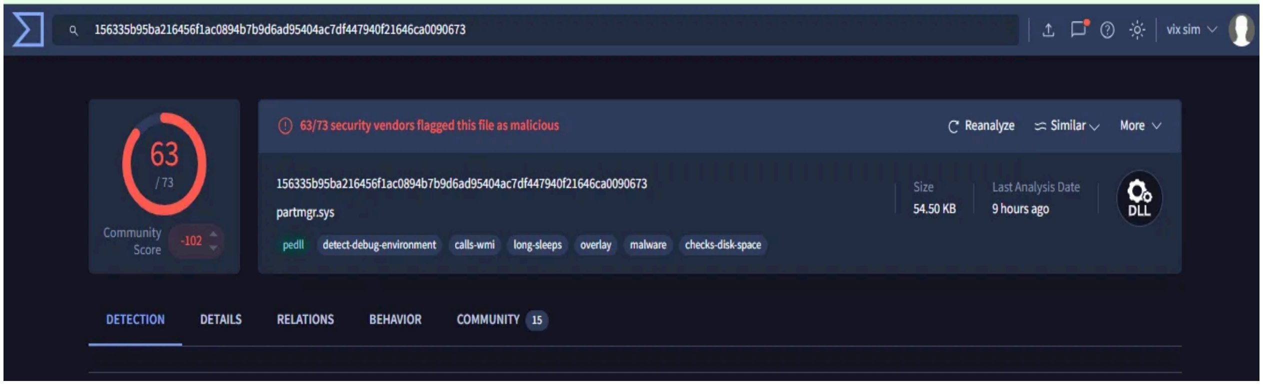


```
┌──(comfort㉿kali)-[~]
└─$ nano Ransomeware.yar

┌──(comfort㉿kali)-[~]
└─$ yara -s Ransomeware.yar test.txt
DarkSide_Ransomware test.txt
0x165:$ransom_note: YOUR FILES HAVE BEEN ENCRYPTED BY DARKSIDE
0x230:$file_ext: darkside
0x262:$maliciousurl: http://survey-smiles.com/

┌──(comfort㉿kali)-[~]
└─$ nano test.txt

┌──(comfort㉿kali)-[~]
└─$ yara -s Ransomeware.yar test.txt
DarkSide_Ransomware test.txt
0x165:$ransom_note: YOUR FILES HAVE BEEN ENCRYPTED BY DARKSIDE
0x230:$file_ext: darkside
0x262:$maliciousurl: http://survey-smiles.com/

┌──(comfort㉿kali)-[~]
└─$ 
```

Analysis and Findings

Malicious Hash Identification:

The hash “**156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673**” was flagged as malicious by multiple antivirus vendors on VirusTotal with a community score of 63/72 as at the 22nd of March, 2025.



156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673

63 / 73

Community Score -102

63/73 security vendors flagged this file as malicious

156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673

partmgr.sys

pedll detect-debug-environment calls-wmi long-sleeps overlay malware checks-disk-space

Size 54.50 KB

Last Analysis Date 9 hours ago

Threat Intelligence Research: Darkside Ransomware

History of the Malware

Emergence: Darkside Ransomware first emerged in 2020. It gained significant attention in 2021-06-02 09:45:36 UTC due to its involvement in high-profile attacks, including the Colonial Pipeline attack in the United States.

Evolution: The malware is believed to be a product of a ransomware-as-a-service (RaaS) model, where the developers lease the ransomware to affiliates who carry out the attacks.

Current Status: As of 2023, Darkside Ransomware is still active, although its operations have been disrupted by law enforcement and cybersecurity firms. The group behind Darkside has rebranded and continues to operate under different names.

Notable Attacks

Colonial Pipeline Attack (2021): One of the most infamous attacks attributed to Darkside Ransomware. The attack caused a temporary shutdown of the Colonial Pipeline, leading to fuel shortages across the U.S. East Coast.

Targeted Industries: Darkside primarily targets critical infrastructure sectors, including energy, healthcare, and manufacturing. The group focuses on organizations that can afford to pay large ransoms.

Geographic Focus: While the group has targeted organizations globally, the majority of its attacks have been concentrated in North America and Europe.

Threat Actor

Group Name: The group behind Darkside Ransomware is known as Darkside or DarkSide. They operate as a Ransomware-as-a-Service (RaaS) group.

Affiliation: Darkside is believed to have ties to other cybercriminal groups, including REvil and BlackMatter. These groups share infrastructure, tools, and tactics.

Motivation: The primary motivation is financial gain. The group demands ransom payments in cryptocurrency (usually Bitcoin) and has been known to exfiltrate data before encrypting files, using the threat of data leakage to pressure victims into paying.

Motivation & Tactics

Motivation

The group is financially motivated, targeting organizations that can pay large ransoms. They also engage in double extortion, where they not only encrypt files but also threaten to leak stolen data if the ransom is not paid.

Tactics

Initial Access: Darkside typically gains access to victim networks through phishing emails, exploiting vulnerabilities in Remote Desktop Protocol (RDP), or purchasing access from initial access brokers.

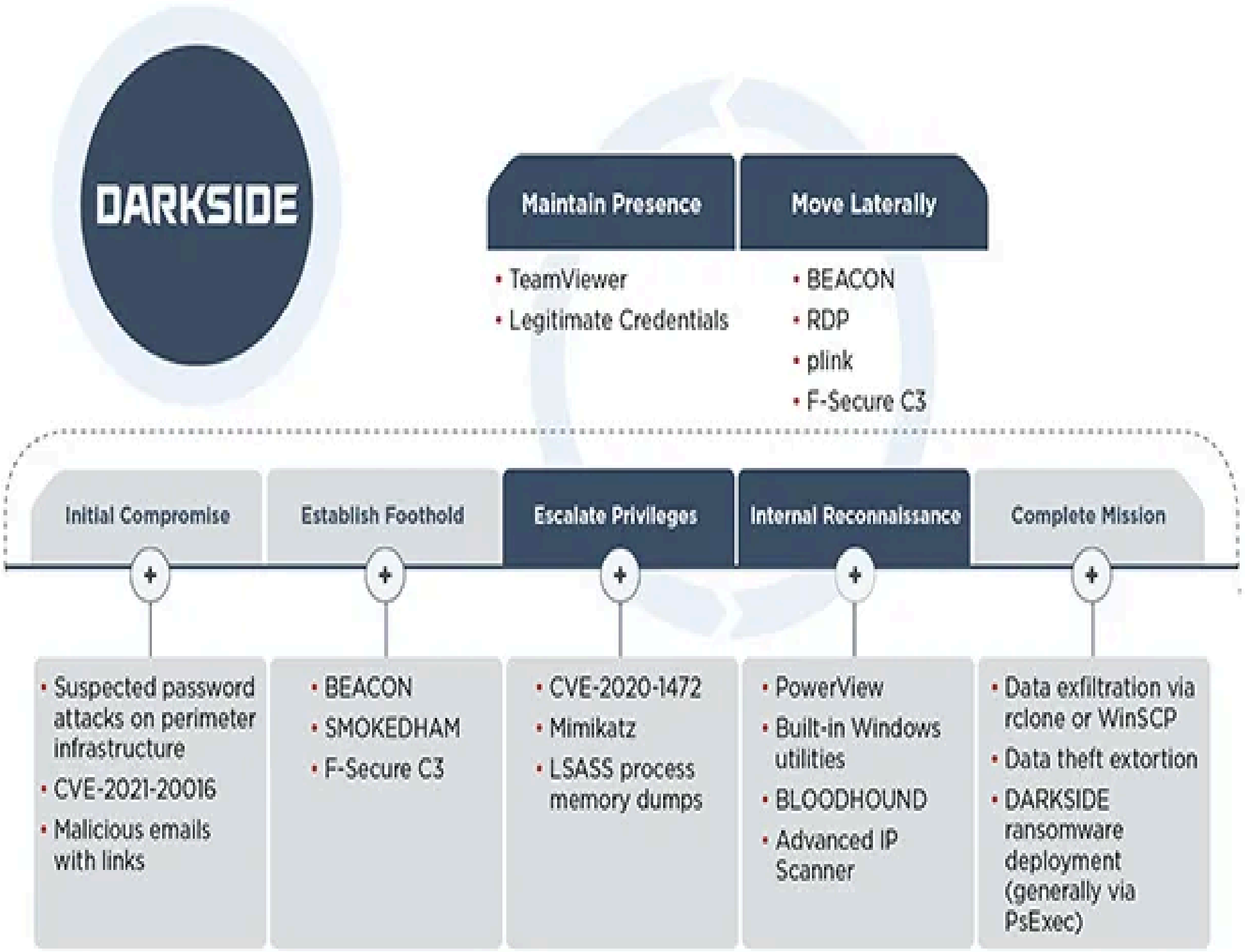
Lateral Movement: Once inside the network, the group uses tools like Mimikatz to escalate privileges and move laterally across the network.

Data Exfiltration: Before encrypting files, the group exfiltrates sensitive data to use as leverage in ransom negotiations.

Encryption: Darkside uses strong encryption algorithms to lock files and demands payment for the decryption key.

Attack Lifecycle

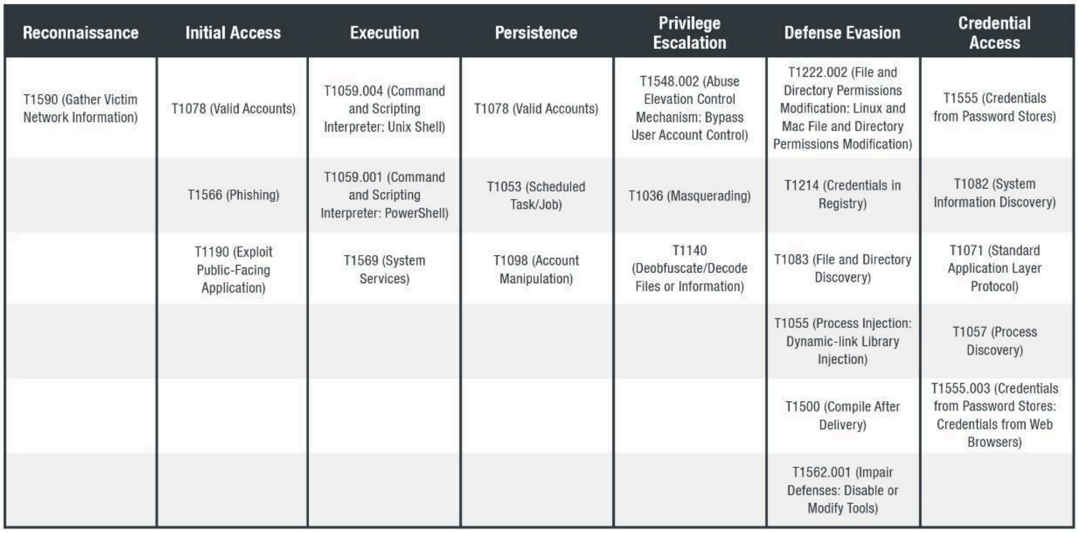
In the figure below



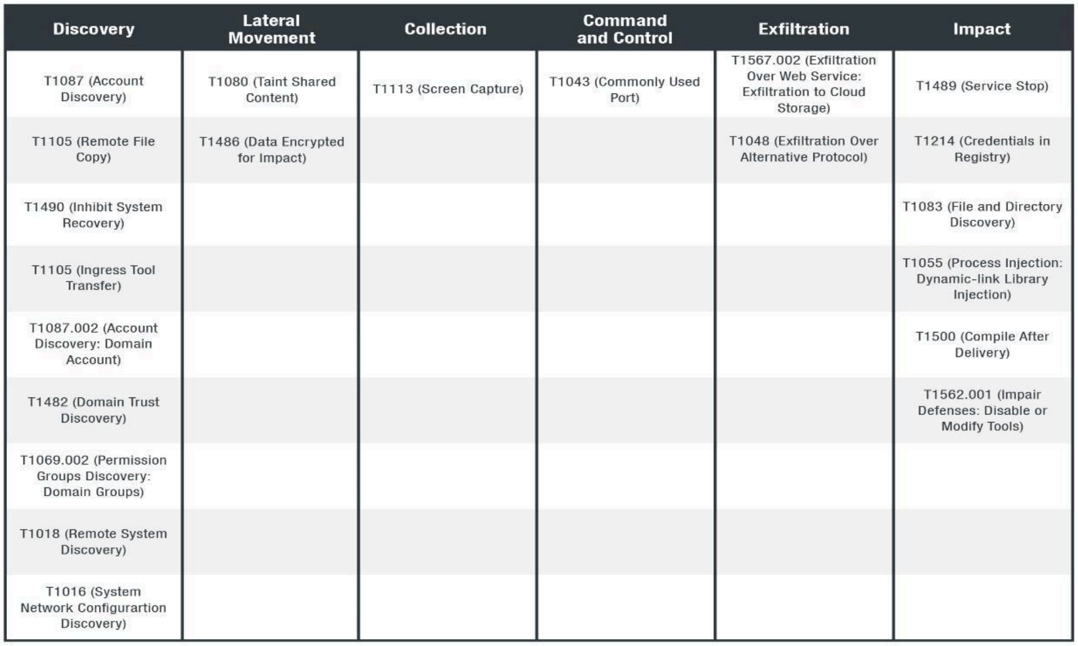
Darkside Attack Lifecycle

MITRE ATT&CK Tactics and Techniques

Below are the MITRE ATT&CK tactics and techniques associated with DarkSide Ransomware.



Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
T1590 (Gather Victim Network Information)	T1078 (Valid Accounts)	T1059.004 (Command and Scripting Interpreter: Unix Shell)	T1078 (Valid Accounts)	T1548.002 (Abuse Elevation Control Mechanism: Bypass User Account Control)	T1222.002 (File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification)	T1555 (Credentials from Password Stores)
	T1566 (Phishing)	T1059.001 (Command and Scripting Interpreter: PowerShell)	T1053 (Scheduled Task/Job)	T1036 (Masquerading)	T1214 (Credentials in Registry)	T1082 (System Information Discovery)
	T1190 (Exploit Public-Facing Application)	T1569 (System Services)	T1098 (Account Manipulation)	T1140 (Deobfuscate/Decode Files or Information)	T1083 (File and Directory Discovery)	T1071 (Standard Application Layer Protocol)
					T1055 (Process Injection: Dynamic-link Library Injection)	T1057 (Process Discovery)
					T1500 (Compile After Delivery)	T1555.003 (Credentials from Password Stores: Credentials from Web Browsers)
					T1562.001 (Impair Defenses: Disable or Modify Tools)	



Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1087 (Account Discovery)	T1080 (Taint Shared Content)	T1113 (Screen Capture)	T1043 (Commonly Used Port)	T1567.002 (Exfiltration Over Web Service: Exfiltration to Cloud Storage)	T1489 (Service Stop)
T1105 (Remote File Copy)	T1486 (Data Encrypted for Impact)			T1048 (Exfiltration Over Alternative Protocol)	T1214 (Credentials in Registry)
T1490 (Inhibit System Recovery)					T1083 (File and Directory Discovery)
T1105 (Ingress Tool Transfer)					T1055 (Process Injection: Dynamic-link Library Injection)
T1087.002 (Account Discovery: Domain Account)					T1500 (Compile After Delivery)
T1482 (Domain Trust Discovery)					T1562.001 (Impair Defenses: Disable or Modify Tools)
T1069.002 (Permission Groups Discovery: Domain Groups)					
T1018 (Remote System Discovery)					
T1016 (System Network Configurartion Discovery)					

Tactics and Techniques Associated with Darkside Ransomware

Initial Access

The various analyzed samples of DarkSide ransomware show that phishing, remote desktop protocol (RDP) abuse, and exploiting known vulnerabilities are the commonly used tactics by the group to gain initial access. DarkSide group also uses legitimate tools throughout the attack chain to remain obfuscate its attack and to remain undetected.

Below is the comprehensive list of legitimate tools used by the group throughout the reconnaissance and gaining-entry phases of the attack.

PowerShell: for reconnaissance and persistence

Metasploit Framework: for reconnaissance

Mimikatz: for reconnaissance

BloodHound: for reconnaissance

Cobalt Strike: for installation

For a modern ransomware attack like the DarkSide, gaining initial access no longer immediately leads to ransomware being dropped onto the victim's machine. There are now several steps that follow in between that are often manually executed by the threat actor.

Lateral Movement and Privilege Escalation

Lateral movement is one of the key discovery phases in any modern ransomware process. The end goal is to identify all the critical data within the victim's network, which includes the target files and locations to facilitate the upcoming exfiltration and encryption steps.

In the case of DarkSide, the goal of lateral movement activity is to gain Domain Controller (DC) or Active Directory access, which will be further used to steal credentials, escalate privileges, and acquire other valuable assets for data exfiltration. The group laterally moves through the systems, eventually using the DC network share to deploy the ransomware to connected machines. As per the observation, the DarkSide group deployed PSExec and RDP.

Exfiltration

The critical files are exfiltrated before the ransomware is being launched. This is the riskiest step in the DarkSide ransomware execution process, as data exfiltration is more likely to be noticed by the victim organization's cybersecurity team. It is the last step before any ransomware is dropped, and the attack often speeds up at this point to complete the process before it is detected and stopped.

For exfiltration, these were the tools being used:

7-Zip: a utility used for archiving files to prepare for exfiltration of critical data

Rclone and Mega client: tools used for exfiltrating files to the cloud storage

PuTTy: an alternative application used for network file transfer

DarkSide uses several Tor-based leak sites to host victim's stolen data. The file-sharing services used by the DarkSide group for data exfiltration include Mega and PrivatLab.

Execution and Impact

The execution of the actual ransomware follows next. It is to be noted that the DarkSide ransomware shares many similarities with REvil in this step of the process, which includes the structure of ransom notes and the use of PowerShell to execute a command which eventually deletes shadow copies from the network. On code analysis, it was found that the same code checks were used by this ransomware to check whether the victim is located in a commonwealth of Independent States (CIS) country or not.

The PowerShell is used to install and operate the malware itself, while Certutil and Bitsadmin were used to download the ransomware. Two encryption methods were used, depending on whether the target operating system is Windows or Linux: A ChaCha20 stream cipher with RSA-4096 is used on Linux, whereas Salsa20 with RSA-1024 is used on Windows.

Current Status

Active Status: Darkside Ransomware is still active, although its operations have been disrupted by law enforcement and cybersecurity firms. The group has rebranded and continues to operate under different names.

Mitigation Efforts: Many organizations have implemented endpoint detection and response (EDR) solutions, network segmentation, and regular backups to mitigate the impact of Darkside attacks. Law enforcement agencies have also taken down some of the group's infrastructure.

Relationship Summary

156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673	Connected_To	baroquetees.com
156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673	Connected_To	rumahsia.com
156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673	Dropped	3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a
156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673	Dropped	f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e
baroquetees.com	Resolved_To	176.103.62.217
baroquetees.com	Connected_From	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
176.103.62.217	Resolved_To	baroquetees.com
rumahsia.com	Resolved_To	99.83.154.118
rumahsia.com	Connected_From	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
99.83.154.118	Resolved_To	rumahsia.com
3ba456cafcb31e0710626170c3565aae305bc7c32a948a54f0331d0939e0fe8a	Dropped_By	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
f6fba207c71d1f53f82d96a87c25c4fa3c020dca58d9b8a266137f33597a0b0e	Dropped_By	156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673

Challenges and Solutions

Challenge: Rate limiting by the VirusTotal API.
Solution: Implemented a 60-second delay after every four API requests to stay within the rate limit.

Challenge: Identifying unique byte patterns in the malware.
Solution: Leveraged YARA rules from VirusTotal to detect distinct byte sequences associated with the malware.

Challenge: Testing the YARA rule.
Solution: Since the actual DarkSide malicious file was unavailable, a test.txt file was created containing the string “Your file has been encrypted by DarkSide” to test the rule’s effectiveness.

Recommendations

Strengthening Cyber Defense Posture

To effectively mitigate ransomware threats like DarkSide, organizations must invest in advanced cybersecurity solutions. Deploying Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), and robust network segmentation can help detect and contain threats early. Proactive threat hunting using automated tools, YARA rules, and real-time threat intelligence feeds will enhance the ability to detect and respond to malware threats before they escalate.

Additionally, organizations should enhance email security by implementing advanced filtering solutions to block phishing attempts and malicious attachments, which remain a primary entry point for ransomware. Regular system updates and security patching should be enforced across all endpoints to mitigate vulnerabilities.

Policy and Governance

A strong cybersecurity governance framework is essential for maintaining resilience. Organizations should conduct regular security audits to identify vulnerabilities and ensure compliance with best practices. Establishing a cybersecurity task force at the executive level will help align security initiatives with business objectives and ensure ongoing risk management oversight.

Investment in staff training and cybersecurity awareness programs is also critical. Employees should receive ongoing training on the latest adversarial tactics, including social engineering and phishing schemes, to minimize human-related security risks.

Collaboration and Information Sharing

Given the evolving nature of ransomware threats, collaboration with industry peers, government agencies, and threat intelligence platforms is essential. Engaging with cybersecurity Information Sharing and Analysis Centers (ISACs) allows organizations to stay informed about emerging threats and mitigation strategies.

Furthermore, maintaining active communication channels with law enforcement and cybersecurity agencies, such as CISA and INTERPOL, ensures that organizations receive timely threat advisories and best practice guidelines to strengthen their security posture.

Incident Response and Recovery Readiness

A comprehensive and well-tested incident response plan is essential for mitigating ransomware incidents. Organizations should regularly conduct simulation exercises and tabletop drills to evaluate their readiness in handling ransomware attacks.

Maintaining resilient backup and recovery solutions, including secure offline backups, is crucial for minimizing downtime and ensuring rapid recovery in case of an attack.

Conclusion

Our in-depth analysis of DarkSide ransomware highlights the ever-evolving nature of cyber threats and the critical need for a proactive, multi-layered defense strategy. While law enforcement efforts have disrupted some of its operations, the rise of successor groups like BlackMatter demonstrates that threat actors continuously adapt, refine their tactics, and exploit new vulnerabilities.

Cybersecurity is no longer just an IT issue it is an enterprise-wide responsibility that demands strategic investments, robust governance, and a culture of security awareness. Executive leadership must prioritize cybersecurity by fostering cross-functional collaboration, engaging with external threat intelligence partners, and aligning security initiatives with business objectives.

By implementing strong access controls, advanced threat detection, incident response planning, and continuous monitoring, organizations can not only mitigate the immediate risk posed by ransomware but also strengthen their long-term cyber resilience. Staying ahead of sophisticated cyber adversaries requires continuous vigilance, innovation, and a commitment to proactive defense strategies, ensuring the protection of critical assets, sensitive data, and overall business continuity in an ever-evolving threat environment.

References

Blackpanda. (2023). *What is DarkSide ransomware?* Retrieved from https://www.blackpanda.com/blog/what-is-darkside-ransomware

International Cybersecurity and Digital Forensics Academy. (2023). *Lab assignment template guide.* Retrieved from https://www.sisainfosec.com/blogs/darkside-ransomware-operations/

Trend Micro. (2023). *What we know about DarkSide ransomware and the U.S. pipeline attack.* Retrieved from https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

VirusTotal. (2023). *VirusTotal API documentation.* Retrieved from https://developers.virustotal.com/

YARA Documentation. (2023). *Writing YARA rules.* Retrieved from https://yara.readthedocs.io/