ILLUMINATING DARKSIDE

TTPs, Tools, and the Trend Towards Defense Evasion

Research by

PICUS

ILLUMINATING DARKSIDE:

TTPs, Tools, and the Trend Towards Defense Evasion

EXECUTIVE SUMMARY

The DarkSide ransomware group conducted several high-profile breaches, including the US-based Colonial Pipeline Company incident in May 2021. They have established the Ransomware as a Service (RaaS) model and expanded their operations with the participation of other threat actors. In addition to encrypting files and demanding ransom, the DarkSide threat actors exfiltrate data and threaten the victim by releasing the exfiltrated data, known as the double-extortion tactic.

In this research, we investigated Tactics, Techniques, and Procedures (TTPs) utilized by the DarkSide threat group to understand their attack methods and the impact of their breaches. The results of this investigation show that the DarkSide group used dozens of techniques and utilized all tactics under the MITRE ATT&CK framework.

We also analyzed tools used by DarkSide in breaches, and we found that DarkSide threat actors heavily utilize publicly available and legitimate tools; only 3 of 32 tools used by them are malicious software. Emerging threat actors like DarkSide use native living-off-the-land Windows utilities, legitimate tools and services, and red team tools throughout the attack lifecycle to stay under the radar of security controls and remain undetected.

Since these legitimate tools are also used by the system and network admins or penetration testers and red teamers, it is difficult to distinguish whether these tools were used for legitimate or malicious purposes. Moreover, living-off-the-land utilities already exist in the target environment, and they are whitelisted in most of the signature-based preventive security controls. These findings emphasize the importance of behavior-based detection and proactive approaches such as attack simulation and security control validation.

KEY FINDINGS

- **The most exciting finding was that only 9% of used tools in DarkSide attack campaigns were malware.** These malware are responsible for encryption, data collection, and command and control (C2) communication.

- **91% of utilized tools by DarkSide threat actors are publicly available and legitimate tools that are using known attack techniques,** which include living off the land Windows utilities (19%), open-source tools (19%), free tools (31%) and services (9%), and commercial-off-the-shelf (COTS) tools (13%).

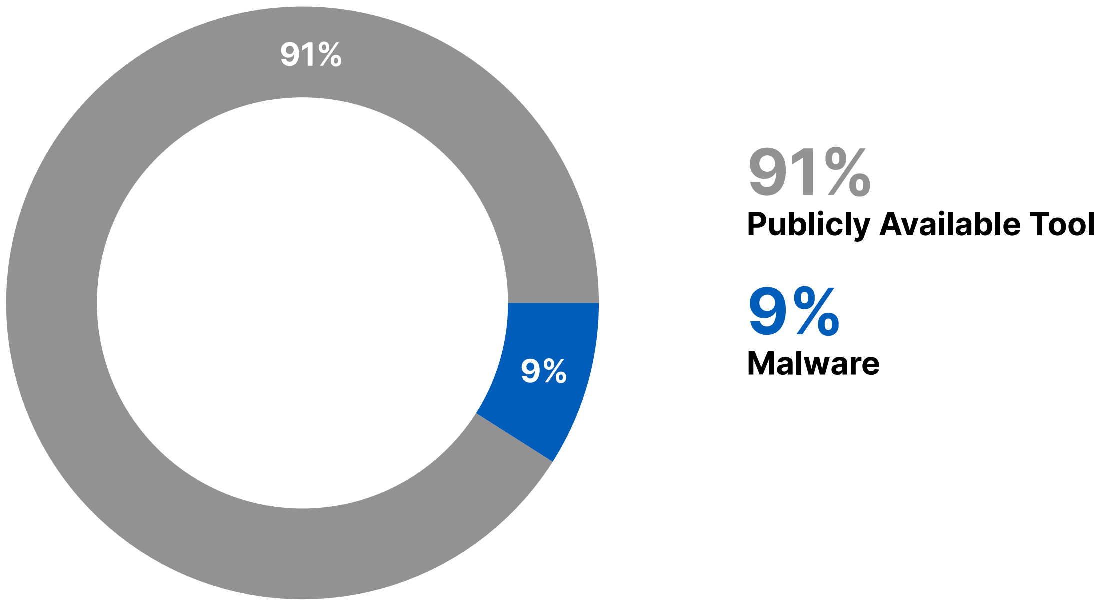
- DarkSide operators use at least **34 MITRE ATT&CK techniques** categorized under all **14 tactics** of the framework.

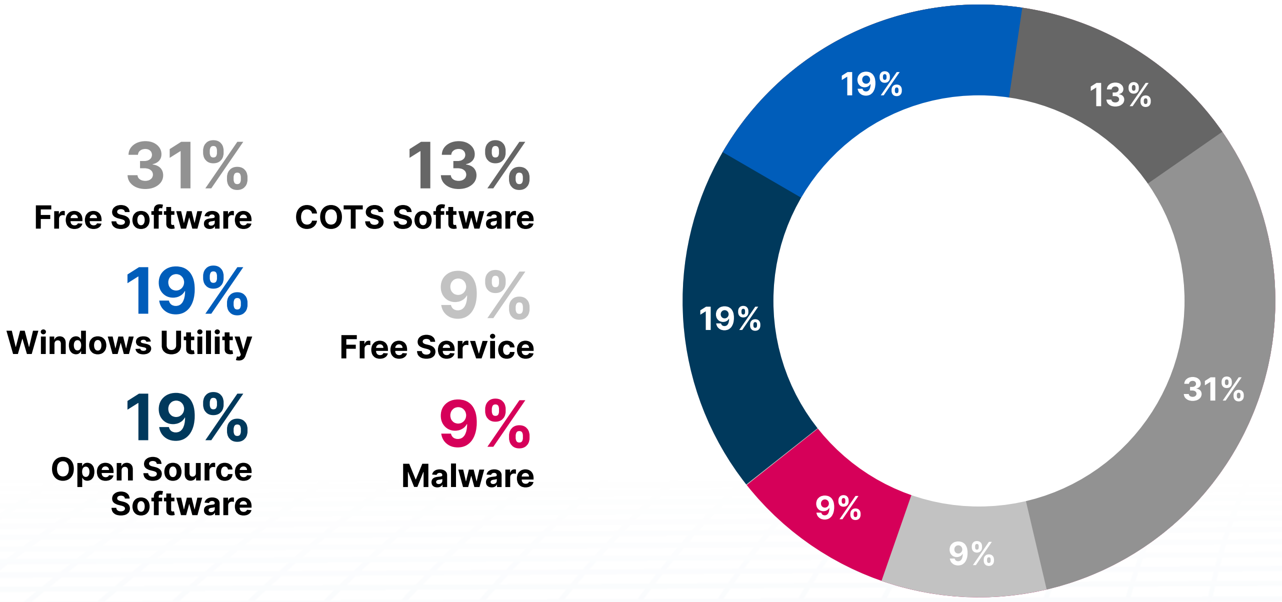
- DarkSide threat actors use **multiple tools to employ a technique.** They adapt their tooling to the victim environment and security controls.

- Signature-based prevention approaches, such as blocking these tools directly using simple IOCs such as their known file hashes, are not effective against these tools. **Behavior-based** detection is required.

- Instead of reactive approaches, proactive approaches such as **attack simulation** and **security control validation** help you to find gaps and improve cyber resilience against emerging threat actors like DarkSide.

DISTRIBUTION OF TOOLS USED BY DARKSIDE THREAT ACTORS





DARKSIDE TIMELINE

AUGUST 2020

- DarkSide threat group announced its ransomware.

NOVEMBER 2020

- DarkSide threat group launched its RaaS (ransomware-as-a-service) model. They invited other criminals to use the group's services. Later on, a DarkSide data leak site was identified.
- DarkSide launched a content delivery network (CDN) to store and distribute exfiltrated data.

MARCH 2021

- DarkSide released version 2.0 of its ransomware.
- DarkSide launched a “call service” allowing the affiliates to directly organize calls pressuring victims into paying ransoms from the management panel.

APRIL 2021

- DarkSide announced its new capability, denial-of-service (DoS) attacks.

MAY 2021

- DarkSide launched the Colonial Pipeline attack.
- To grow their team, the DarkSide ransomware group has published a recruitment advertisement for network penetration testers.

MITRE ATT&CK TECHNIQUES UTILIZED BY THE DARKSIDE RANSOMWARE OPERATORS

RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION
T1592.002 Gather Victim Host Information: Software	T1588.002 Obtain Capabilities: Too	T1190 Exploit Public-Facing Application	T1059.001 Command and Scripting Interpreter: PowerShell	T1053 Scheduled Task/Job	T1055 Process Injection: Dynamic-link Library Injection	T1197 BITS Jobs
		T1566.002 Phishing: Spearphishing Link	T1053 Scheduled Task/Job	T1053 Scheduled Task/Job	T1053 Scheduled Task/Job	T1484.001 Domain Policy Modification: Group Policy Modification
		T1078 Valid Accounts	T1569.002 System Services: Service Execution	T1078 Valid Accounts	T1078.002 Valid Accounts: Domain Accounts	T1562.001 Impair Defenses: Disable or Modify Tools
						T1036.005 Masquerading: Match Legitimate Name or Location
						T1055 Process Injection: Dynamic-link Library Injection

CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXFILTRATION	IMPACT
T1003 OS Credential Dumping	T1087.002 Account Discovery: Domain Account	T1570 Lateral Tool Transfer	T1005 Data from Local System	T1071 Application Layer Protocol	T1048 Exfiltration Over Alternative Protocol	T1486 Data Encrypted for Impact
	T1018 Remote System Discovery	T1021.001 Remote Services: Remote Desktop Protocol	T1560.001 Archive Collected Data: Archive via Utility	T1105 Ingress Tool Transfer	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1490 Inhibit System Recovery
	T1016 System Network Configuration Discovery	T1021.002 Remote Services: SMB/Windows Admin Shares	T1056 Input Capture	T1572 Protocol Tunneling		
		T1021.004 Remote Services: SSH		T1219 Remote Access Software		
				T1102 Web Service		

TOOLS USED BY DARKSIDE RANSOMWARE OPERATORS

Tool	Type	Tactic
AnyDesk	COTS Software	Command and Control
CobaltStrike	COTS Software	Command and Control
Ngrok	COTS Software	Command and Control
TeamViewer	COTS Software	Command and Control
AdFind	Free Software	Discovery
Advanced IP Scanner	Free Software	Discovery
GMER	Free Software	Defense Evasion
Mega Client	Free Software	Exfiltration
NetScan	Free Software	Discovery
PC Hunter	Free Software	Defense Evasion
Plink	Free Software	Command and Control
PowerTool64	Free Software	Defense Evasion
puTTy	Free Software	Exfiltration
WinSCP	Free Software	Exfiltration
Mega	Free Service	Exfiltration
pCloud	Free Service	Command and Control
PrivatLab	Free Service	Exfiltration

Tool	Type	Tactic
power_encryptor	Malware	Impact
SMOKEDHAM	Malware	Collection
SystemBC	Malware	Command And Control
7-zip	Open-Source Software	Collection
AdRecon	Open-Source Software	Discovery
BloodHound	Open-Source Software	Discovery
Mimikatz	Open-Source Software	Exfiltration
Rclone	Open-Source Software	Exfiltration
F-Secure C3	Open-Source Software	Command and Control
BITSAdmin	Windows Utility	Defense Evasion
Group Policy Object (GPO)	Windows Utility	Execution, Persistence, Defense Evasion
PowerShell	Windows Utility	Execution
SQLDumper.exe	Windows Utility	Collection
PsExec	Windows Utility	Execution, Lateral Movement
WMI	Windows Utility	Execution, Impact

INTRODUCTION

The US-based Colonial Pipeline Company became aware of a ransomware incident on Friday, May 7, 2021 [1]. Because of the incident, pipeline operations were proactively suspended, and many systems were taken offline [1].

The DarkSide ransomware group accepted responsibility for the attack [1]. To expand their operations, DarkSide threat actors have established a Ransomware as a Service (RAAS) model and invited other threat actors to use the DarkSide ransomware. They use double extortion tactics; in other words, they exfiltrate critical data before encrypting files and threaten the victim with the release of the exfiltrated data to encourage ransom payment.

Although DarkSide is a relatively new group compared with other well-known ransomware groups like Maze, Sodinokibi (REvil), and NetWalker, they carried out dozens of high-profile breaches in less than a year.

We analyzed Tactics, Techniques, and Procedures (TTPs) and tools utilized by the DarkSide threat group to understand their attack methods and the impact of their breaches.

Our research references the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 9 framework.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

UTILIZED BY DARKSIDE OPERATORS

DarkSide ransomware operators utilize 34 techniques and sub-techniques under all 14 tactics in the MITRE ATT&CK framework. They also use multiple procedures for some techniques.

This section presents:

- Malicious behaviors of DarkSide threat actors by categorizing them under MITRE ATT&CK v9 tactics and techniques.
- Procedures that explain how DarkSide operators implement these techniques.
- Description of tools used in each tactic.

You can create an adversary emulation plan using techniques and sub-techniques given below to validate your security controls against the DarkSide threat group.

DON'T FORGET
While you can manually emulate most of these TTPs, **Picus Threat Library** includes all of the required adversary emulations out of the box, alongside 700+ other attack scenarios and 10000+ network and endpoint attack emulations.

1. RECONNAISSANCE

The Reconnaissance tactic of the MITRE ATT&CK framework includes techniques involving adversaries to collect information actively and passively before compromising a victim [2]. Attackers use this information to use in other phases of the attack lifecycle, such as Initial Access, as used by the DarkSide ransomware operators.

Tactic	Technique	Procedure
Reconnaissance	T1592.002 Gather Victim Host Information: Software	DarkSide threat actors determine whether a SonicWall SMA100 SSL VPN software runs on the machine, if so, which version is running. This information is used for initial access by exploiting **CVE-2021-20016**, a vulnerability in this product.

2. RESOURCE DEVELOPMENT

The Resource Development tactic includes techniques involving adversaries to create, purchase, or compromise resources such as infrastructure, accounts, or capabilities [3]. They develop these resources before compromising the victim and leverage them to utilize in other phases, such as using leased Virtual Private Servers to support Command and Control.

Tactic	Technique	Procedure
Resource Development	T1588.002 Obtain Capabilities: Tool	Adversaries obtain tools in cyberattacks to support their operations [4]. These tools can be free or commercial, open or closed source. The DarkSide ransomware operators use dozens of tools to help its post-compromise behaviors.

3. INITIAL ACCESS

The Initial Access tactic includes techniques used by attackers to gain an initial foothold within a network, such as exploiting vulnerabilities on public-facing web servers [5].

Tactic	Technique	Procedure
Initial Access	T1190 Exploit Public-Facing Application	Adversaries exploit vulnerabilities in Internet-facing software, such as web servers, to gain access to the host [6]. The **DarkSide** threat actors obtained initial access to their victim by exploiting **CVE-2021-20016,** a vulnerability in the SonicWall SMA100 SSL VPN product, which has been patched by SonicWall [1].
	T1566.002 Phishing: Spearphishing Link	**DarkSide** operators use phishing mail with links to collect valid credentials as the initial access method [7].
	T1078 Valid Accounts	Threat actors obtain and abuse credentials of existing accounts to gain Initial Access, Persistence, Privilege Escalation, or Defense Evasion [8]. **DarkSide** ransomware operators get initial access through corporate VPN infrastructure using valid credentials [1].

DON'T FORGET

Picus Security Control Validation Platform can assess the effectiveness of your email security controls against Phishing (Spearphishing Attachment, Spearphishing Link) techniques with thousands of emails that include malicious attachments and links. Picus also simulates software vulnerability exploitation attacks to assess your network and endpoint security controls.

4. EXECUTION

Techniques that result in adversary-controlled code running on a local or remote system are categorized under the Execution tactic in the MITRE ATT&CK Framework. This tactic cannot be detached from others; execution techniques are often paired with techniques from all other tactics. For example, an adversary might use a Remote Access Tool (tactic: Command and Control) to run a PowerShell (tactic: Execution) script that does Remote System Discovery (tactic: Discovery).

- **A Group Policy Object (GPO),** a component of Windows OS, is a virtual collection of policy settings [10]. It can represent policy settings in the file system and Active Directory.
- **PowerShell** is a robust interactive command-line shell and scripting language installed by default on Windows OSs. Since PowerShell has extensive access to Windows internals, system administrators frequently use it to manage and configure the operating system and automate complex tasks. Not only system administrators but also adversaries have realized the potential in incorporating such a powerful tool into their arsenal.
- **PsExec** is a legitimate Microsoft tool and a part of Windows Sysinternals utilities [11]. **PsExec** can execute commands and binaries on remote systems and download or upload files over a network share. Besides **DarkSide,** ransomware gangs like **Nefilim** and **LockerGoga**, and more than 20 threat groups such as **HAFNIUM, OilRig,** and **Turla** utilize **PsExec** for lateral movement [12].
- **WMI** (Windows Management Instrumentation) is the infrastructure for management data and operations on Windows-based operating systems. System admins write WMI scripts or applications to automate administrative tasks on remote computers.

- **ENROLL** in the free “MITRE ATT&CK PowerShell” course in Purple Academy to learn how adversaries operate Windows Command Shell in their attacks and red and blue team exercises.

- **READ** our blog post titled “MITRE ATT&CK PowerShell” to learn more about this technique.

Tactic	Technique	Procedure
Execution	T1059.001 Command and Scripting Interpreter: PowerShell	Since **PowerShell** has extensive access to Windows internals, system administrators frequently use it to manage and configure the operating system and automate complex tasks [13]. DarkSide operators use the **DownloadFile** method of **PowerShell** to download the DarkSide ransomware binary [14]. They also used **PowerShell** to run a **WMI** function that deletes volume shadow copies.
	T1053 Scheduled Task/Job	Adversaries use task scheduling utilities of operating systems to execute malicious payloads on a defined schedule or at system startup [15]. DarkSide uses **Group Policy Object (GPO)** to create a scheduled task to run the ransomware.
	T1569.002 System Services: Service Execution	DarkSide utilizes Microsoft Sysinternals **PsExec** to execute binaries on remote systems using a temporary Windows service.
	T1047 Windows Management Instrumentation	The DarkSide group runs a **PowerShell** command to execute **WMI**’s **Win32_ShadowCopy** class to delete volume shadow copies.

5. PERSISTENCE

The Persistence tactic consists of techniques used by adversaries to maintain their foothold across system restarts, changed credentials, or patched vulnerabilities [16].

Tactic	Technique	Procedure
Persistence	T1053 Scheduled Task/Job	Adversaries use task scheduling utilities of operating systems to execute malicious payloads on a defined schedule or at system startup to achieve persistence [15]. DarkSide uses **Group Policy Object (GPO)** to create a scheduled task to execute the ransomware and stay persistent.

- **ENROLL** in the free "MITRE ATT&CK Scheduled Task/Job" course in Purple Academy to learn how adversaries operate Windows Command Shell in their attacks and red and blue team exercises.
- **READ** our blog post titled "MITRE ATT&CK T1053 Scheduled Task" to learn more about this technique.

6. PRIVILEGE ESCALATION

Adversaries typically enter and explore a network with unprivileged access, but they need elevated permissions to pursue their goals. In order to gain higher-level permissions, adversaries use Privilege Escalation techniques.

Tactic	Technique	Procedure
Privilege Escalation	T1055 Process Injection: Dynamic-link Library Injection	The **DarkSide** ransomware injects its code into the existing process and dynamically loads its libraries.
	T1078.002 Valid Accounts: Domain Accounts	**DarkSide** threat actors create and use domain accounts.

- **ENROLL** in the free "MITRE ATT&CK Process Injection" course in Purple Academy" to learn how adversaries operate Windows Command Shell in their attacks and red and blue team exercises.
- **READ** the blog post titled "MITRE ATT&CK Process Injection" to learn more about this technique.

7. DEFENSE EVASION

Defense evasion consists of techniques that adversaries use to avoid detection by security controls.

- **BITSAdmin** is a command-line tool used for creating and managing **BITS Jobs** [17].
- **GMER** is designed as a rootkit detector and remover [18]. Likewise, it is also used by threat actors, such as **DarkSide** [8], **Dharma** [19], and **Deadmin Locker** [20], to disable security protections on the system.
- **PC Hunter** is an application designed as a security utility. It enables users to access the system processes, kernel modes, hooks, registry, and startup information and closing and removing processes to spot and remove rootkits and other malware types [21]. However, **PC Hunter** is also used by threat actors, such as **DarkSide** [8], **Dharma** [19], and **Nefilim** [22] ransomware groups to disable security tools as a defense evasion tool. It can be detected as **pchunter.exe, pchunter64.exe**, or **pchunter32.exe** in the process list. **PC Hunter** is also used by threat actors, such as **DarkSide** [8], **Dharma** [19], and **Nefilim** [22] ransomware groups to disable security tools.
- **DarkSide** ransomware group uses **PowerTool64** to disable active antivirus protection. This tool is also used by **Dharma** [19] and **Deadmin Locker** [20] ransomware families.

Tactic	Technique	Procedure
Defense Evasion	T1197 BITS Jobs	**DarkSide** threat actors utilize **Bitsadmin** to download malware binary.
	T1484.001 Domain Policy Modification: Group Policy Modification	**DarkSide** uses **Group Policy Object (GPO)** to create a scheduled task to execute the ransomware.
	T1562.001 Impair Defenses: Disable or Modify Tools	The **DarkSide** ransomware group utilizes **PC Hunter, GMER**, and **PowerTool64** to disable security tools.
	T1036.005 Masquerading: Match Legitimate Name or Location	Adversaries may masquerade names/locations of their artifacts as identical or similar names/locations of legitimate files to evade monitoring and detection. DarkSide operators download the ransomware binary as “update.exe” to masquerade its name [14].

- **ENROLL** in the free “MITRE ATT&CK Impair Defenses” course in Purple Academy to learn how adversaries operate Windows Command Shell in their attacks and red and blue team exercises.
- **READ** our blog post titled “MITRE ATT&CK T1562 Impair Defenses” to learn more about this technique.

- **ENROLL** in the free “MITRE ATT&CK Masquerading” course in Purple Academy to learn how adversaries operate Windows Command Shell in their attacks and red and blue team exercises.
- **READ** our blog post titled “MITRE ATT&CK T1036 Masquerading” to learn more about this technique.

8. CREDENTIAL ACCESS

Adversaries use the techniques in the Credential Access tactic to steal credentials such as account names and passwords. They use valid credentials to access systems without detection. Brute force attacks, exploiting software vulnerabilities, keylogging, man-in-the-middle attacks, network sniffing, and dumping credentials from operating systems are some of the techniques used for credential access.

• **Mimikatz** is one of the most frequently used tools for credential dumping [23]. It can extract plaintext passwords, password hashes, and Kerberos tickets from memory. Including the Lazarus group, Turla, MuddyWater, APT29, APT41, and APT29, more than 30 APT (Advanced Persistent Threat) groups use Mimikatz in their attacks.

Tactic	Technique	Procedure
Credential Access	T1003 OS Credential Dumping	**DarkSide** ransomware operators have employed **Mimikatz** credential dumping to escalate privileges in the victim network [7].

• **ENROLL** in the free "MITRE ATT&CK OS Credential Dumping" course in Purple Academy to learn how adversaries operate Windows Command Shell in their attacks and red and blue team exercises.

• **READ** our blog post titled "MITRE ATT&CK T1003 Credential Dumping" to learn more about this technique.

9. DISCOVERY

Adversaries use the techniques in the Discovery tactic to obtain information about your environment, such as services, processes, network, files, software, system, accounts, domain, and registry.

• **ADFind** is a command-line Active Directory reconnaissance tool [24]. This AD query tool is also used by other threat groups, such as FIN6, menuPass (APT10), APT29, and Wizard Spider [25].

• **ADRecon** is an Active Directory (AD) reconnaissance tool [26]. It extracts and combines various artifacts, such as forest, domain, DCs, SPNs, domain accounts, LAPS passwords, and ACLs, out of an AD environment. DarkSide uses this tool to gather information from Active Directory.

• **Advanced IP Scanner** is a network scanner that can show all network devices, allows you access to shared folders, and provides remote control of computers (via RDP and Radmin) [27]. Although it is developed for network administrators, it is also used by threat actors like DarkSide for malicious activities.

• **BloodHound** is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment [28]. Threat groups, such as **Chimera, Wizard Spider,** and **Operation Wocao** utilize **BloodHound** for the account, domain trust, password policy, permission groups, and remote system discovery [28].

• **NetScan** is a network reconnaissance tool used to discover open ports, running services, and live hosts.

Tactic	Technique	Procedure
Discovery	T1087.002 Account Discovery: Domain Account	DarkSide utilizes **ADRecon** and **ADFind** tools to enumerate domain accounts.
	T1018 Remote System Discovery	DarkSide utilizes **ADRecon, ADFind** and **BloodHound** tools for discovering computers listed in the Active Directory by querying AD for computers.
	T1016 System Network Configuration Discovery	DarkSide uses **NetScan** for network service discovery, such as scanning ports and listening services. It also utilizes **Advanced IP Scanner** to discover network devices and shared folders.

10. LATERAL MOVEMENT

The Lateral Movement tactic includes techniques that are used by adversaries to access and control remote systems (lateral movement) on the target network [29]. To accomplish Lateral Movement, adversaries may use legitimate tools with valid accounts as well as their remote access tools.

- **PsExec** is a legitimate Microsoft tool and a part of Windows Sysinternals utilities [11]. **PsExec** can execute commands and binaries on remote systems and download or upload files over a network share. Besides **DarkSide,** ransomware gangs like **Nefilim** and **LockerGoga,** and more than 20 threat groups such as **HAFNIUM, OilRig,** and **Turla** utilize **PsExec** for lateral movement [12].

Tactic	Technique	Procedure
Lateral Movement	T1570 Lateral Tool Transfer	DarkSide ransomware operators deploy ransomware encryptors using PsExec [7].
	T1021.001 Remote Services: Remote Desktop Protocol	DarkSide uses valid accounts collected via phishing to log in to target Windows systems using the Remote Desktop Protocol (RDP).
	T1021.002 Remote Services: SMB/Windows Admin Shares	The DarkSide threat actors utilize PsExec to execute commands on remote systems. DarkSide also uses SMB BEACON of Cobalt Strike to move laterally in target environments.
	T1021.004 Remote Services: SSH	DarkSide uses valid accounts collected via phishing to log in to target Linux-based systems using Secure Shell (SSH).

11. COLLECTION

Adversaries use the techniques in the Collection tactic to gather information relevant to their objectives. Various data types such as text, audio, and video are collected from multiple sources such as local system cloud, network drive, removable media, and clipboard. The next goal after data collection is often to exfiltrate the data.

- **7-zip** is an archiving utility that is used to manage compressed files.
- **SQLDumper.exe** is a debugging utility included with Microsoft SQL Server.
- **SMOKEDHAM** is a .NET backdoor that can log keystrokes, take screenshots, and execute arbitrary .NET commands.

Tactic	Technique	Procedure
Collection	T1005 Data from Local System	Adversaries may search local system sources, such as file systems or local databases to collect critical data. The DarkSide threat actors use SQLDumper.exe to generate a dump file in the SQL server.
	T1560.001 Archive Collected Data: Archive via Utility	Adversaries may use several utilities such as 7-Zip, WinRAR, and WinZip to compress or encrypt data before exfiltration [30]. Among these utilities, **DarkSide** operators use **7-Zip** to compress data to be exfiltrated like the Hafnium threat group [31].
	T1056 Input Capture	**DarkSide** threat actors use **SMOKEDHAM** backdoor for keylogging (T1056.001 Keylogging) and taking screenshots (T1056.002 GUI Input Capture).

12. COMMAND AND CONTROL

The Command and Control (C&C or C2) tactic includes techniques that adversaries may use to communicate with compromised systems within a victim network. In order to avoid detection, adversaries try to mimic legitimate traffic. They also use various channels, ports, and protocols for communication.

Certutil:

Certutil is a command-line Windows utility designed to obtain certificate authority information and configure Certificate Services [32]. Adversaries use certutil to download files from a given URL.

F-Secure Custom Command and Control (C3):

F-Secure Custom Command and Control (C3) is a tool that allows Red Teams to rapidly develop and utilize esoteric command and control channels (C2) [34]. However, this tool is also used by adversaries to create C2 channels.

AnyDesk:

AnyDesk is a remote desktop control software.

Plink (PuTTy Link):

Plink (PuTTY Link) is a command-line connection tool similar to UNIX ssh. Plink utility is frequently used by adversaries to create SSH tunnels, such as OilRig, Cobalt Group, and Fin6 [35].

Ngrok:

Ngrok is a desktop application that exposes local servers behind NATs and firewalls to the public internet over secure tunnels.

Team Viewer:

TeamViewer is a remote desktop control software.

Cobalt Strike:

Cobalt Strike is a commercial remote access tool that is designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors [33]. Cobalt Strike's interactive post-exploit capabilities cover a wide-range of MITRE ATT&CK techniques.

SystemBC:

SystemBC is a Remote Access Tool (RAT) that is used by ransomware operators as an off-the-shelf backdoor. In addition to the DarkSide threat actors, Ryuk and Egregor ransomware operators also used SystemBC in their cyberattacks [36].

Tactic	Technique	Procedure
Command and Control	T1071 Application Layer Protocol	The **DarkSide** threat actors use **SMB** and **HTTPS BEACON** payloads of **Cobalt Strike** for Command and Control.
	T1105 Ingress Tool Transfer	**DarkSide** operators use **Certutil,** a built-in Windows utility, to download ransomware binary [13].
	T1572 Protocol Tunneling	**DarkSide** operators utilize the Plink tool to open a reverse SSH tunnel from the compromised system to the Command and Control (C2) system. They also use **Ngrok** software to open secure tunnels for C2 communications.
	T1219 Remote Access Software	Adversaries frequently utilize legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, and AmmyyAdmin, to create a C2 channel to target systems within networks [36]. The **DarkSide** threat actors use **AnyDesk** to establish an interactive command and control channel to compromised systems.
	T1102 Web Service	**DarkSide** utilizes the F-Secure **C3 framework** to establish a C2 channel by deploying relays configured to proxy C2 communications through the Slack API [1].

13. EXFILTRATION

Adversaries use techniques in the Exfiltration tactic to steal data from your network. They encrypt or compress the data to be exfiltrated and use different channels and protocols to avoid detection.

Data loss protection is one of the top priority issues for CISOs today. Organizations utilize DLP solutions to protect and secure their data and comply with regulations. Picus simulates the exfiltration of a wide range of data over different channels to test the effectiveness of both network and endpoint-based data loss prevention (DLP) solutions.

- **Mega[.]nz, pCloud,** and **PrivatLab** are free cloud storage services where you can store and share your files. Threat actors use these services to manually or automatically exfiltrate data. For example, **HAFNIUM** has exfiltrated data to file sharing sites, including MEGA [31].
- **Mega Client** is an application used to upload files to Mega cloud storage.
- **puTTy** is a free SSH and telnet client for Windows.
- **Rclone** is a command-line program to manage files on cloud storage [38]. It supports over 40 cloud storage products.
- **WinSCP** is a free SFTP, SCP, Amazon S3, WebDAV, and FTP client for Windows.

Tactic	Technique	Procedure
Exfiltration	T1048 Exfiltration Over Alternative Protocol	DarkSide threat actors utilize puTTy to exfiltrate files over SSH protocol.
	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	Adversaries may exfiltrate data to a cloud storage that allows upload, modify and retrieve files. DarkSide operators manually exfiltrate collected data to free cloud storage providers, such as Mega[.]nz, pCloud, and PrivatLab. They also use client applications to upload files to these services, such as Mega client. Moreover, DarkSide operators exfiltrate data over SFTP and SMB protocols using Rclone and WinSCP to systems in cloud storage environments.

i

DON'T FORGET

Picus Threat Library includes hundreds of data files consisting of different types of information mapped to standards and regulations, including PII, PCI DSS, PHI, GDPR, HIPAA, PIPEDA, confidential files such as password files of OSs, and Intellectual Property (IP) data.

14. IMPACT

The Impact tactic covers techniques that manipulate, interrupt, or destroy your systems to disrupt availability, compromise integrity, or cover a confidentiality breach.

- **power_encryptor** is a malware that is used by DarkSide to encrypt files and create ransom notes.

Tactic	Technique	Procedure
Lateral Movement	T1486 Data Encrypted for Impact	DarkSide threat actors deploy the file power_encryptor.exe in a compromised environment to encrypt files and create ransom notes.
	T1490 Inhibit System Recovery	DarkSide ransomware operators navigate to ESXi administration interfaces and disable snapshot features prior to the ransomware encryptor deployment [7]. They also used PowerShell and WMI to delete volume shadow copies, as explained in the Execution tactic.

- **READ** our blog post titled "An Underrated Technique to Delete Volume Shadow Copies - DeviceIoControl" to learn more about four methods used by ransomware threat groups to prevent the recovery of encrypted files from volume shadow copies.

CONCLUSION

The main goal of the current study was to determine attack methods used by DarkSide threat actors and the impact of their cyber attacks by examining Tactics, Techniques, and Procedures (TTPs) and tools utilized in DarkSide attack campaigns.

The most obvious finding to emerge from this study is that only 9% of used tools are malware, and the remaining 91% of tools are publicly available legitimate tools, such as built-in Windows utilities like WMI, PowerShell, and BITSAdmin.

This finding shows that IoC and signature-based approaches would not work against emerging threats like DarkSide. Most of the tools used by the DarkSide group are in whitelists of security controls since they are also used by legitimate users, such as system and network administrators. Therefore, blocking these tools directly using their known file hashes may result in false positives. Besides, 19% of these tools are open-source software, so attackers can easily modify them and easily change their hashes.

Reasonable approaches to tackle these threats are behavior-based detection and proactive defense approach with attack simulation and security control validation. The DarkSide ransomware group and most of the other threat actors use known TTPs, so simulating these TTPs to identify gaps in security controls and closing these gaps is the most effective and efficient way to defend against these attacks.

Picus Security Control Validation Platform simulates hundreds of TTPs in its Threat Library and gives actionable mitigation information, such as ready-to-use vendor-specific or vendor-agnostic detection rules, for each TTP for building a proactive defense against adversaries.

HOW PICUS HELPS?

DETECT AND PREVENT RANSOMWARE THREATS

Picus Security Control Validation Platform offers a threat-centric security control validation and mitigation that allows security teams to proactively identify gaps in the network, endpoint, and cloud security controls.

Picus is not just a Breach and Attack Simulation (BAS) tool; it also provides actionable vendor-specific and vendor-agnostic detection rules and prevention signatures to enable you quickly fix your security gaps.

Threat Library

Mobilize thousands of threats and hundreds of TTPs in your environment with a few clicks in minutes.

Attack Simulation

Run attack simulations against your network, endpoint, and cloud security controls.

Security Control Validation

Identify your gaps in detection and prevention automatically.

Fast Mitigation

Get detection rules and prevention signatures to fix your gaps in your security controls.

- **Picus Threat Library** includes 10.000+ threats. It includes 100+ adversary group and malware scenarios, such as DarkSide, Hafnium, Nobelium (UNC2452), APT7, APT38 (Lazarus), Sodinokibi, Ryuk, TrickBot, WastedLocker, and NetWalker. It also includes 700+ atomic attack scenarios to assess your defenses against MITRE ATT&CK techniques.
- Picus provides **risk-free adversary emulation.** You can simulate these attacks to test your network, endpoint, and cloud security controls.
- Then, you can **validate your security controls** against these attack scenarios, such as DarkSide. Picus identifies your gaps in both detection and prevention. Picus' Detection Analytics feature shows log collection, detection, and alerting status about adversary techniques and visualizes on the MITRE ATT&CK Framework.
- Picus also provides **actionable mitigation content.** Picus provides prevention signatures to address gaps in preventive security controls, log sources and log validation to address gaps in log generation and collection, detection rules and detection validation to address detection and alerting gaps. So, you can collect required logs, write detection rules, generate alerts using the mitigation content provided by Picus.
- Picus also provides search queries for **threat hunting.** So, you can use these queries to hunt for adversary TTPs, such as the DarkSide TTPs listed in this document, in your SIEM or EDR.

Picus Threat Library

- 10.000+ total threats
800+ endpoint attacks
  - 100+ adversary group scenarios
  - 700+ atomic attacks
- 6000+ malware attacks
- 2000+ web application attacks
- 700+ vulnerability exploitation attacks
- 200+ data exfiltration attacks

Picus Mitigation Library

- 12 prevention technologies (NGFW, WAF, IPS, etc.)
- 60.000+ prevention signatures
- 300+ new signatures in each month
- 2300+ vendor-specific detection rules
- 500+ vendor-agnostic detection rules

REFERENCES

[1] “What We Know About Darkside Ransomware and the US Pipeline Attack,” 14-May-2021. Available: https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us -pipeline-attac.html. [Accessed: 07-Jun-2021]

[2] “Reconnaissance.” Available: https://attack.mitre.org/tactics/TA0043/.

[3] “Resource Development.” Available: https://attack.mitre.org/tactics/TA0042/.

[4] “Obtain Capabilities: Tool.” Available: https://attack.mitre.org/techniques/T1588/002/.

[5] “Initial Access.” Available: https://attack.mitre.org/tactics/TA0001/.

[6] “Exploit Public-Facing Application.” Available: https://attack.mitre.org/techniques/T1190/.

[7] J. Nuce, “Shining a Light on DARKSIDE Ransomware Operations.” Available: https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html.

[8] S. Gallagher, M. Loman, P. Mackenzie, and Y. Polat, “A defender’s view inside a DarkSide ransomware attack,” 11-May-2021. Available: https://news.sophos.com/en-us/2021/05/11/a-defenders-view-inside-a-darkside-ransomware-attack/.

[9] “Valid Accounts.” Available: https://attack.mitre.org/techniques/T1078/.

[10] REDMOND\\markl, “Group Policy Objects.” Available: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects.

[11] markruss, “PsExec - Windows Sysinternals.” Available: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec.

[12] “PsExec.” Available: https://attack.mitre.org/software/S0029/.

[13] S. Özarslan, “MITRE ATT&CK T1086 PowerShell.” Available: https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1086-powershell.

[14] C. Nocturnus, “Cybereason vs. DarkSide Ransomware.” Available: https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware.

[15] S. Özarslan, “MITRE ATT&CK T1053 Scheduled Task.” Available: https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-1053-scheduled-task.

[16] “Persistence.” Available: https://attack.mitre.org/tactics/TA0003/.

[17] “BITSAdmin.” Available: https://attack.mitre.org/software/S0190/.

[18] “GMER - Rootkit Detector and Remover.” Available: http://gmer.net.

[19] Eric Loui-Karl Scheuerman - Aaron Pickett - Brendon Feeley, “Dharma Ransomware Intrusions Exhibit Consistent Techniques,” 16-Apr-2020. Available: https://www.crowdstrike.com/blog/targeted-dharma-ransomware-intrusions-exhibit-consistent-techniques/.

[20] “Alert: New version of DEADMIN LOCKER Ransomware.” Available: https://www.sangfor.com/en/info-center/blog-center/cyber-security/alert-new-version-of-deadmin-locker-ransomware.

[21] “PC Hunter.” Available: https://www.softpedia.com/get/Security/Security-Related/PC-Hunter.shtml.

[22] “Nefilim ransomware analysis.” Available: https://www.maldefense.com/nefilim-ransomware-analysis.html.

[23] S. Özarslan, “MITRE ATT&CK T1003 Credential Dumping.” Available: https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1003-credential-dumping.

[24] “AdFind.” Available: http://www.joeware.net/freetools/tools/adfind/.

[25] “AdFind.” Available: https://attack.mitre.org/software/S0552/.

[26] sense-of-security, “sense-of-security/ADRecon.” Available: https://github.com/sense-of-security/ADRecon.

[27] “Advanced IP Scanner - Download Free Network Scanner.” Available: https://www.advanced-ip-scanner.com.

[28] “BloodHound.” Available: https://attack.mitre.org/software/S0521/.

[29] “Lateral Movement.” Available: https://attack.mitre.org/tactics/TA0008/.

[30] “Archive Collected Data: Archive via Utility.” Available: https://attack.mitre.org/techniques/T1560/001/.

[31] S. Özarslan, “Tactics, Techniques, and Procedures (TTPs) Used by HAFNIUM to Target Microsoft Exchange Servers.” Available: https://www.picussecurity.com/resource/blog/ttps-hafnium-microsoft-exchange-servers.

[32] “certutil.” Available: https://attack.mitre.org/software/S0160/.

[33] “Cobalt Strike.” Available: https://attack.mitre.org/software/S0154/.

[34] “C3.” Available: https://labs.f-secure.com/tools/c3/.

[35] “Protocol Tunneling.” Available: https://attack.mitre.org/techniques/T1572/.

[36] S. Gn and S. Gallagher, “Ransomware operators use SystemBC RAT as off-the-shelf Tor backdoor,” 16-Dec-2020. Available: https://news.sophos.com/en-us/2020/12/16/systembc/.

[37] “Remote Access Software.” Available: https://attack.mitre.org/techniques/T1219/.

[38] N. Craig-Wood, “Rclone.” Available: https://rclone.org.

ABOUT PICUS

In 2013, Picus Security pioneered Breach and Attack Simulation (BAS) technology and has helped companies improve their cyber resilience since then.

Established by cybersecurity veterans with academic backgrounds and extensive hands-on experience, Picus Security developed a transformative Security Validation solution for end-to-end attack readiness visibility and effortless mitigation to pre-empt cyber attacks across all cyber defense layers.

Picus' "The Complete Security Validation Platform" provides granular and actionable insights for operational and executive teams, helps build proactive capabilities, maximizes technology utilization, and thus optimizes return on investment and keeps the risk of getting breached consistently low.

ACCREDITED BY FROST & SULLIVAN AS A MARKET LEADER

"Picus Security is one of the early proponents of applying threat-centric validation to cyber-defense operations. The company offers its customers proactive SOC capabilities, granular visibility, and multi-tenancy. For instance, with its recent Detection Analytics & Mitigation solution, Picus Security has empowered SOC teams with mitigation recommendations."

Frost Radar: Global BAS Market, 2020 Research Report

RECOGNIZED AS A COOL VENDOR BY GARTNER

"Picus Security is cool because it offers a breach and attack simulation platform that covers multiple threat vectors (network, endpoint, email, and lateral movement). This coverage identifies the security gaps as well as underutilized security investments along with mitigation recommendations to reduce the attack surface."

Cool Vendors in Security and Risk Management, 2H19, Prateek Bhajanka, Sr. Principal Analyst at Gartner

picussecurity

www.picussecurity.com