DarkSide Ransomware Gang: An Overview

By Ramarcus Baylor

Published: 2021-05-12 · Archived: 2026-04-05 13:07:21 UTC

Executive Summary

It took an attack on a major U.S. pipeline company, and the possibility of disruption in the delivery of gasoline and jet fuel supplies to a large part of the country, to show the world that ransomware attackers are not going to rest on their laurels after shaking down municipal governments, school districts and hospitals.

DarkSide became one of the world's most well-known hacking groups after the FBI confirmed it is responsible for the highly publicized attack. When a shadowy group can sit halfway across the world and, with a few keystrokes, threaten fuel supplies on the U.S. Eastern Seaboard, then people do begin to take notice.

The impact of this attack is a reflection of the fact that ransomware operators are always on the move – improving, automating and becoming more effective at targeting larger and larger organizations. And they're getting a lot more money for their efforts. The average cyber ransom paid more than doubled in 2020 – to $312,493 – compared to 2019, according to the 2021 Unit 42 Ransomware Threat Report. So far in 2021, the average payment has nearly tripled compared to the previous year – to about $850,000.

DarkSide has helped boost those averages by constantly focusing on ways to optimize its business model in the short time it's been active (we first encountered the group about a year ago). Like other leading ransomware gangs, DarkSide recently embraced the Ransomware-as-a-Service (RaaS) model. It outsourced code development, infrastructure and operations and turned to the dark web to recruit new staff. As a result, the group can now better focus on getting to know victims and targeting the most valuable types of data at each organization, so it can extract the largest-possible ransom and boost the return on investment in its criminal businesses.

The group started getting the attention of Unit 42 responders around October 2020. Since then, we've been finding its fingerprints in a growing number of cases. What makes DarkSide stand out is that the group has shown discipline we've traditionally only seen with nation-state actors – once the threat actors are in, they really dig in. That said, researchers have noted DarkSide is likely a criminal network operating out of Russia; no one has yet directly connected this to the Russian government.

It is interesting to note that back in November, one ransomware negotiation firm placed the DarkSide operation on an internal restricted list after it announced plans to host infrastructure in Iran – because Iran is under U.S. sanctions, facilitating payments to that location might run afoul of the law.

Wherever they may be, there are indications that DarkSide attackers are highly experienced and accomplished in mounting ransomware attacks. They clearly operate at the high end of the ransomware ecosystem, focusing on a smaller pool of victims from whom they can extract steep ransoms.

Palo Alto Networks customers are protected from this threat by:

- WildFire: All known samples are identified as malware.
- Cortex XDR with:
    - indicators for DarkSide.
    - Anti-Ransomware Module to detect DarkSide encryption behaviors.
    - Local Analysis detection to detect DarkSide binaries.
- Cortex XSOAR: Cortex XSOAR's **ransomware content pack** can immediately help incident response, threat intelligence and SecOps teams to standardize and speed-up post-intrusion response processes. This content pack automates most of the ransomware response steps, allowing the incident response and SecOps teams to add their guidance and input.
- Next-Generation Firewalls: DNS Signatures detect the known command and control (C2) domains, which are also categorized as malware in URL Filtering.
- AutoFocus: Tracking related activity using the DarkSide tag.

If you think you may have been impacted, please email unit42-investigations@paloaltonetworks.com or call (855) 875-4631 to get in touch with the Unit 42 Incident Response team.

Doubling and Tripling Their Pressure

The DarkSide group is aggressive in pressuring victims to pay. The threat actors don't like to be ignored. If victims don't respond within two or three days, they send threatening emails to employees. If that doesn't work, they start calling senior executives on mobile phones. And then they might threaten to start contacting customers or the press. And if that doesn't work, they might launch DDoS to take down external websites.

DarkSide is one of a growing number of ransomware operators that we have seen push the boundaries of their trade to include these tactics, which we refer to as double and triple extortion (others include Maze, Sodin, Clop, NetWalker and Conti).

These aggressive techniques build on the pattern of a typical ransomware attack, in which files are encrypted and a ransom is demanded to decrypt them and restore access. Some victims have backed up their data and do not see a need to pay for decryption keys to restore access to corrupted systems. To prepare for that scenario, attackers also exfiltrate sensitive information and study the victim's network so they can up the ante if a target refuses to pay. Then they threaten to release the data or launch a DDoS attack.

DarkSide even purports to operate under a "code of conduct," seeking to position the group as a trustworthy security "partner." When victims pay, the threat actors will do things to demonstrate good will including providing decryption keys or presenting evidence that appears to show they have deleted stolen data. When asked, they will sometimes even tell victims how they got in so security gaps can be closed.

DarkSide Ransomware: Tactics, Techniques and Procedures

We have seen the following software and tools leveraged by the DarkSide group to gain access to the victims' data:

- Legitimate **remote monitoring and management (RMM)** tools to maintain access into a victim's network, such as AnyDesk and TeamViewer.

- **Reconnaissance tools (ADRecon)** to gather information about victims' Active Directory prior to ransomware encryption.
- A **credential harvesting utility**, Mimikatz, to dump password credentials.
- **PowerShell** to carry out objectives, such as to apply GPO to create a scheduled task to execute the ransomware.
- **Password management utilities** such as Dashlane and LastPass to gain access to additional credentials.
- **Utilities such as SQLDumper.exe** to target SQL Server.
- Victims' **internal messaging software** to contact members of the IT staff.
- **File transferring software** Rclone to exfiltrate data to cloud sharing websites (such as PCloud and MegaSync).

Not many groups target non-Windows based systems, but in early 2021, DarkSide introduced an ESXI version of their ransomware that targets VMware virtual machines (VMs), which many organizations use to leverage server virtualization to reduce operating costs and increase IT productivity.

Why does this matter? While we found that in many cases the client's endpoint security did its job protecting Windows PCs from being encrypted, because the servers were heavily virtualized through VMware's ESXI, the ESXI version of the ransomware made it possible for the DarkSide group to encrypt the virtual infrastructure. The threat actors then essentially shut down applications and services, such as file shares, DNS and email, leaving the victims' networks in a deteriorated state or, worse, not functional.

What Can We Learn From This?

We've been noting for some time that ransomware attackers are becoming increasingly professionalized, outsourcing code development, infrastructure and C2 operations, as well as operating RaaS. Many of them are organized enough to respond to media inquiries and operate victim hotlines.

As these threat actors continue to up their game, organizations need to follow best practices to safeguard their data and protect against groups such as the DarkSide ransomware gang.

Organizations should also make sure to have an incident response plan in place in case of an attack. Unit 42 offers a Ransomware Readiness Assessment to help organizations get started on bolstering defenses.

Palo Alto Networks customers are protected from this threat by:

- WildFire: All known samples are identified as malware.
- Cortex XDR with:
    - indicators for DarkSide.
    - Anti-Ransomware Module to detect DarkSide encryption behaviors.
    - Local Analysis detection to detect DarkSide binaries.
- Cortex XSOAR: Cortex XSOAR's **ransomware content pack** can immediately help incident response, threat intelligence and SecOps teams to standardize and speed-up post-intrusion response processes. This content pack automates most of the ransomware response steps, allowing the incident response and SecOps teams to add their guidance and input.

- Next-Generation Firewalls: DNS Signatures detect the known command and control (C2) domains, which are also categorized as malware in URL Filtering.
- AutoFocus: Tracking related activity using the DarkSide tag.

IOCs

Indicators associated with Darkside are available on GitHub, have been published to the Unit 42 TAXII feed and are viewable via the ATOM Viewer.

Courses of Action

This section documents relevant tactics, techniques and procedures (TTPs) used with DarkSide and maps them directly to Palo Alto Networks product(s) and service(s). It also further instructs customers on how to ensure their devices are configured correctly.

Product / Service	Course of Action
Initial Access, Lateral Movement, Command and Control, Execution, Exfiltration, Persistence, Collection, Privilege Escalation, Discovery, Defense Evasion	
Exploit Public-Facing Application [T1190], External Remote Services [T1133], Remote Desktop Protocol [T1021.001], Web Protocols [T1071.001], Multi-hop Proxy [T1090.003], Valid Accounts [T1078], Phishing [T1566], PowerShell [T1059.001], Automated Exfiltration [T1020], Scheduled Task [T1053.005], Archive Collected Data [T1560], Automated Collection [T1119], Bypass User Account Control [T1548.002], Account Discovery [T1087] Modify Registry [T1112]	
NGFW	Ensure application security policies exist when allowing traffic from an untrusted zone to a more trusted zone
	Ensure 'Service setting of ANY' in a security policy allowing traffic does not exist
	Ensure 'Security Policy' denying any/all traffic to/from IP addresses on Trusted Threat Intelligence Sources Exists
	Ensure that User-ID is only enabled for internal trusted interfaces
	Ensure that 'Include/Exclude Networks' is used if User-ID is enabled
	Ensure that the User-ID Agent has minimal permissions if User-ID is enabled
	Ensure that the User-ID service account does not have interactive logon rights
	Ensure remote access capabilities for the User-ID service account are forbidden
	Ensure that security policies restrict User-ID Agent traffic from crossing into untrusted zones
	Set up File Blocking

	Ensure 'SSL Forward Proxy Policy' for traffic destined to the Internet is configured
	Ensure 'SSL Inbound Inspection' is required for all untrusted traffic destined for servers using SSL or TLS
	Ensure that the Certificate used for Decryption is Trusted
Threat Prevention †	Ensure a Vulnerability Protection Profile is set to block attacks against critical and high vulnerabilities, and set to default on medium, low and informational vulnerabilities
	Ensure a secure Vulnerability Protection Profile is applied to all security rules allowing traffic
	Ensure that antivirus profiles are set to block on all decoders except 'imap' and 'pop3'
	Ensure a secure antivirus profile is applied to all relevant security policies
	Ensure an anti-spyware profile is configured to block on all spyware severity levels, categories, and threats
	Ensure DNS sinkholing is configured on all anti-spyware profiles in use
	Ensure passive DNS monitoring is set to enabled on all anti-spyware profiles in use
	Ensure a secure Anti-Spyware profile is applied to all security policies permitting traffic to the Internet
	Ensure that all zones have Zone Protection Profiles with all Reconnaissance Protection settings enabled, tuned and set to appropriate actions
	Ensure that User Credential Submission uses the action of ‘block’ or ‘continue’ on the URL categories
DNS Security †	Enable DNS Security in Anti-Spyware profile
URL Filtering †	Ensure that URL Filtering is used
	Ensure that URL Filtering uses the action of ‘block’ or ‘override’ on the <enterprise approved value> URL categories
	Ensure that access to every URL is logged
	Ensure all HTTP Header Logging options are enabled
	Ensure secure URL Filtering is enabled for all security policies allowing traffic to the internet
WildFire †	Ensure that WildFire file size upload limits are maximized

	Ensure forwarding is enabled for all applications and file types in WildFire file blocking profiles
	Ensure a WildFire Analysis profile is enabled for all security policies
	Ensure forwarding of decrypted content to WildFire is enabled
	Ensure all WildFire session information settings are enabled
	Ensure alerts are enabled for malicious files detected by WildFire
	Ensure 'WildFire Update Schedule' is set to download and install updates every minute
Cortex XSOAR	Deploy XSOAR Playbook Cortex XDR - Isolate Endpoint
	Deploy XSOAR Playbook - Access Investigation Playbook
	Deploy XSOAR Playbook - Impossible Traveler
	Deploy XSOAR Playbook - Block Account Generic
	Deploy XSOAR Playbook - Block URL
	Deploy XSOAR Playbook - Palo Alto Networks - Hunting And Threat Detection
	Deploy XSOAR Playbook - PAN-OS Query Logs for Indicators
	Deploy XSOAR Playbook - Phishing Investigation - Generic V2
	Deploy XSOAR Playbook - Endpoint Malware Investigation
Cortex XDR	Configure Host Firewall Profile
	Enable Anti-Exploit Protection
	Enable Anti-Malware Protection
	Look for the following BIOCs alerts to detect activity*: Cortex XDR Analytics - Possible LSASS memory dump Cortex XDR Analytics - Unsigned process executed as a scheduled task Cortex XDR Analytics - Connection to a TOR anonymization proxy Cortex XDR Analytics - Dumping Registry hives with passwords
Discovery	
File and Directory Discovery [T1083], Process Discovery [T1057]	

Cortex XDR	Look for the following BIOCs alerts to detect activity*: Cortex XDR Analytics - Multiple Discovery Commands
Impact	
Service Stop [T1489], Inhibit System Recovery [T1490], Data Encrypted for Impact [T1486]	
Cortex XDR	Look for the following BIOCs alerts to detect activity*: Manipulation of Volume Shadow Copy configuration
Cortex XSOAR	Deploy XSOAR Playbook - Ransomware Manual

Table 1. Courses of Action for Darkside ransomware.
†These capabilities are part of the NGFW security subscriptions service.
** These analytic detectors will trigger automatically for Cortex XDR Pro customers.*

Table of Contents

Related Articles

- Unit 42 Ransomware and Extortion Report Highlights: Multi-Extortion Tactics Continue to Rise
- Understanding REvil: REvil Threat Actors May Have Returned (Updated)
- 2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner