GET TO KNOW

DARKSIDE RANSOMWARE

What is DarkSide Ransomware?

The Darksside 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

Publicly Available Tools

91%

91% of utilized tools by DarkSide threat actors are publicly available and legitimate tools that are using known attack techniques.

34 MITRE ATT&CK Techniques

34 MITRE ATT& CK Techniques used by **DarkSide operators** which are categorized under all 14 tactics of the framework.

Behavior-Based Detection

Signature-based prevention approaches are not effective against these tools. Behavior-based detection is required.

From Reactive to Proactive

Instead of reactive approaches, **proactive approaches** such as **attack simulation** and **security control validation** help finding gaps and improving cyber resilience against emerging threat actors like DarkSide.

DarkSide Timeline

NOVEMBER 2020

- Darkside threat group launched its RaaS (ransomware-as-a-service) model. They invited other criminals to the group's services. Later on, a DarkSide data leak site was identified.

MARCH 2021

- 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

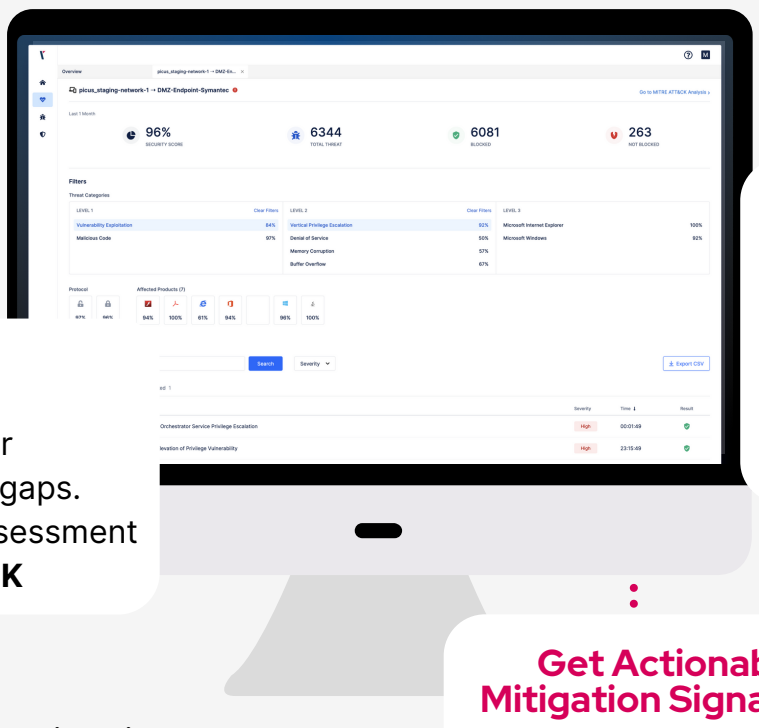
- DarkSide launched the Colonial Pipeline
- Recruitment was published a recruitment advertisement for network penetration testers.

Detect & Prevent Ransomware Threats with Complete Security Control Validation Platform

Use Threat Library

The most up to date real-world threat landscape at the tip of your finger

- **10.000+** total threats
- 100+ adversary group and malware scenarios such as: **DarkSide**, Hafnium, APT38 (Lazarus), Sodinokibi, Ryuk,WastedLocker, and NetWalker.



Run Risk-Free Attack Simulations

Safely and continuously run attack simulations against your network, endpoint, and cloud security controls.

Validate Your Security Controls

Automatically identify your prevention and detection gaps. Get the results of your assessment mapped to **MITRE ATT&CK**

Get Actionable Mitigation Signatures

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

- 60.000+ prevention signatures
- 300+ new signatures in each month
- 2300+ vendor-specific detection rules
- 500+ vendor agnostic detection rules

PICUS

GET YOUR FREE DEMO

www.picussecurity.com