CYBERGANG US PIPELINE ATTACK IDENTIFIED AS DARKSIDE

What is Darkside:

DarkSide is among ransomware gangs that have "professionalized" a criminal industry that has cost Western nations billions of dollars in losses.

The cyberextortion attempt that has forced the shutdown of a vital U.S. pipeline was carried out by a criminal gang known as DarkSide that cultivates a Robin Hood image of stealing from corporations and giving a cut to charity.

The shutdown, meanwhile, stretched into its third day, with the Biden administration saying an "all-hands-on-deck" effort is underway to restore operations and avoid disruptions in the fuel supply.

Experts said that gasoline prices are unlikely to be affected if the pipeline is back to normal in the next few days but that the incident - the worst cyberattack to date on critical U.S. infrastructure.

Finding IOC's

IOC	MD5	SHA1
Darksz2_edrExe.exe	6a7fdab1c7f6c5a5482749be5c4bf1a4	4e6d303d96621769b491777209c237b4061e3285
Darksz1_edrExe.exe	9d418ecc0f3bf45029263b0944236884	eeb28144f39b275ee1ec008859e80f215710dc57
Darksz2_browsingExe.exe	6a7fdab1c7f6c5a5482749be5c4bf1a4	4e6d303d96621769b491777209c237b4061e3285
Darksz1_browsingExe.exe	9d418ecc0f3bf45029263b0944236884	eeb28144f39b275ee1ec008859e80f215710dc57
185.105.109.19		
185.234.247.85		
securebestapp20.com		
temisleyes.com		
isrg.trustid.ocsp.identrust.com		

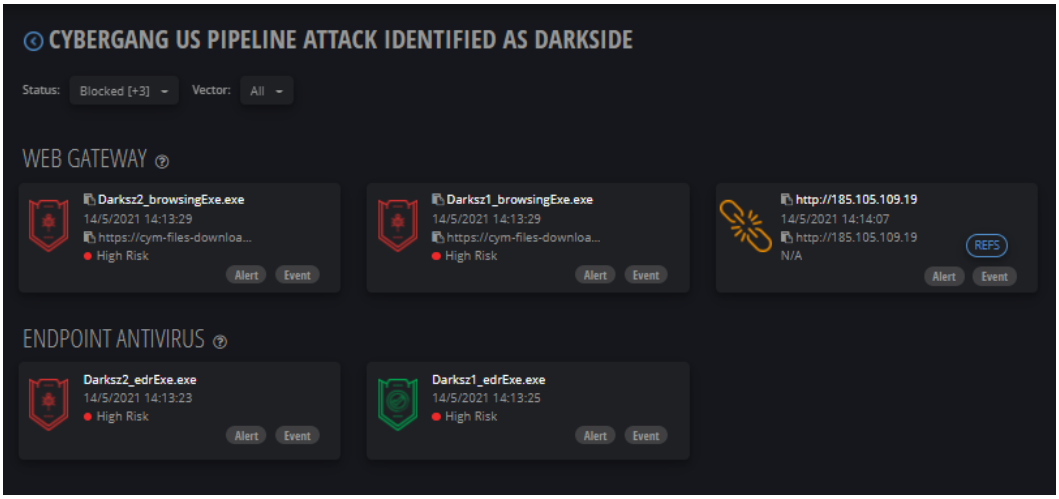
Tools Used:

Sr. No	Tools
1	Cymulate
2	Maltego
3	XDR
4	Qradar

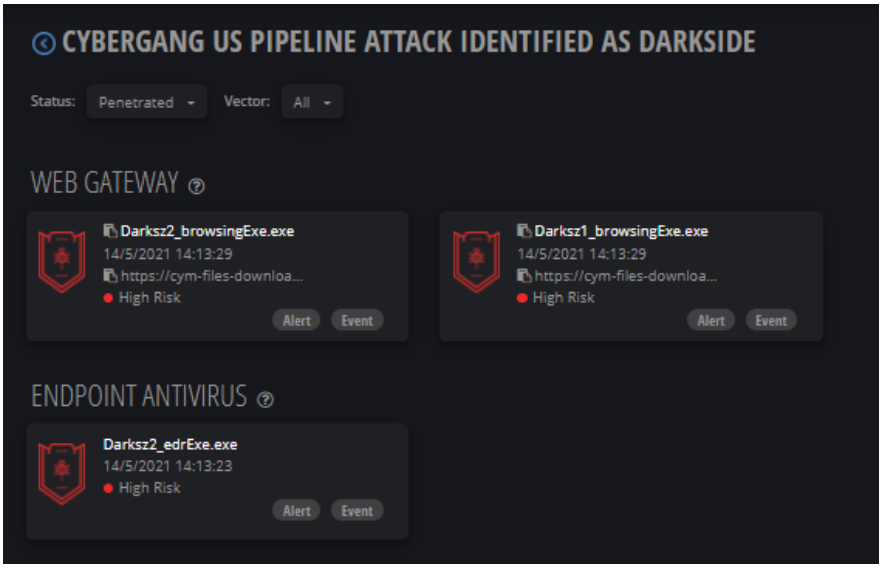
Cymulate Investigation:

- Using IMMEDIATE THREATS INTELLIGENCE Simulation Module, we have tested our environment for Darkside Ransomware.
- We have tested this on Web Gateway and Endpoint Security to understand the risk in our environment.
- Where we have run 5 Vectors for DarkSide Ransomware, among which 3 were easily bypassed in our environment.

5 Vectors

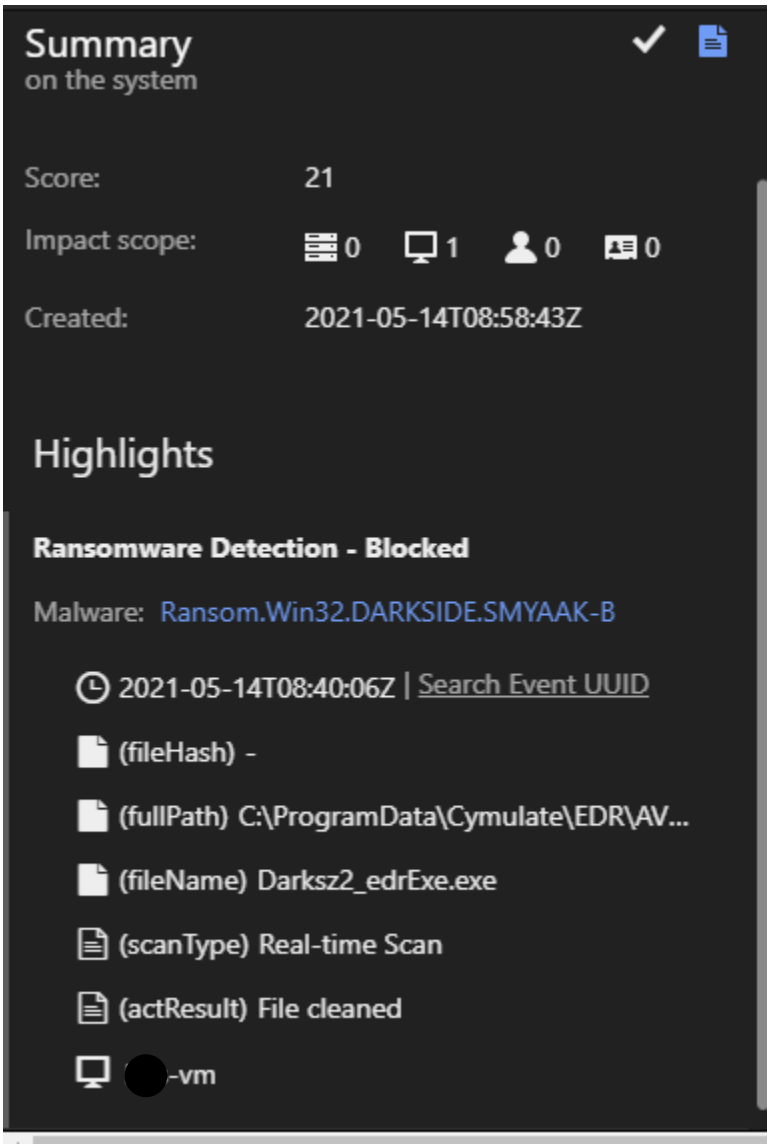


3 Vectors Bypassed



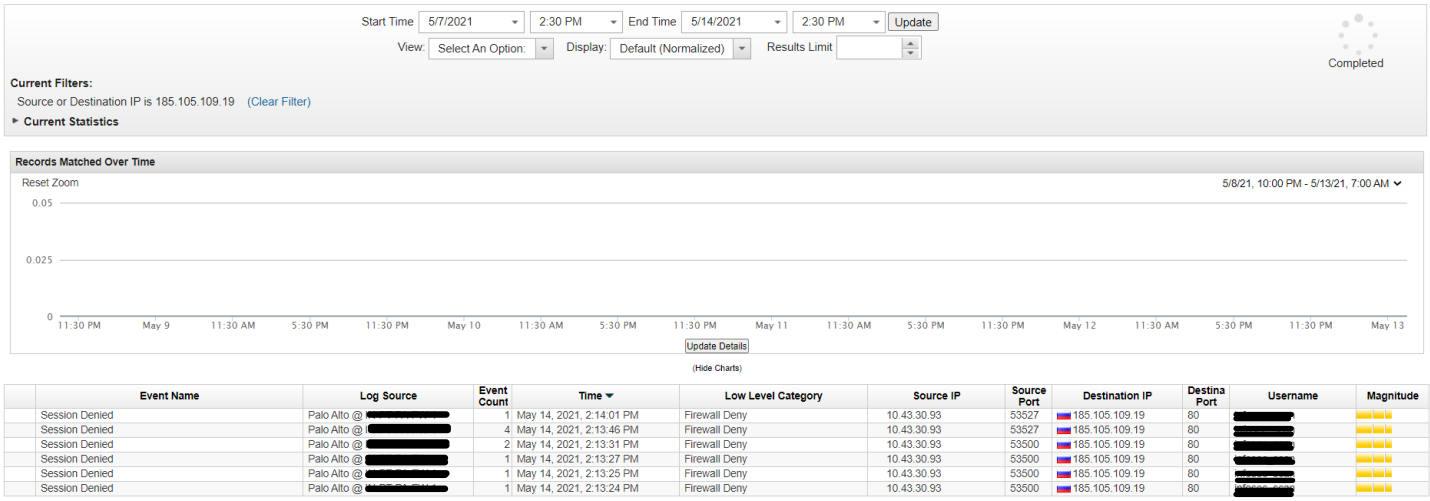
XDR Investigation

- We identified that the file has been blocked and cleaned by TM under the ransomware detection.
- This file was a part of Cymulate simulation which was showing as bypassed on Endpoint Security.



QRadar Investigation

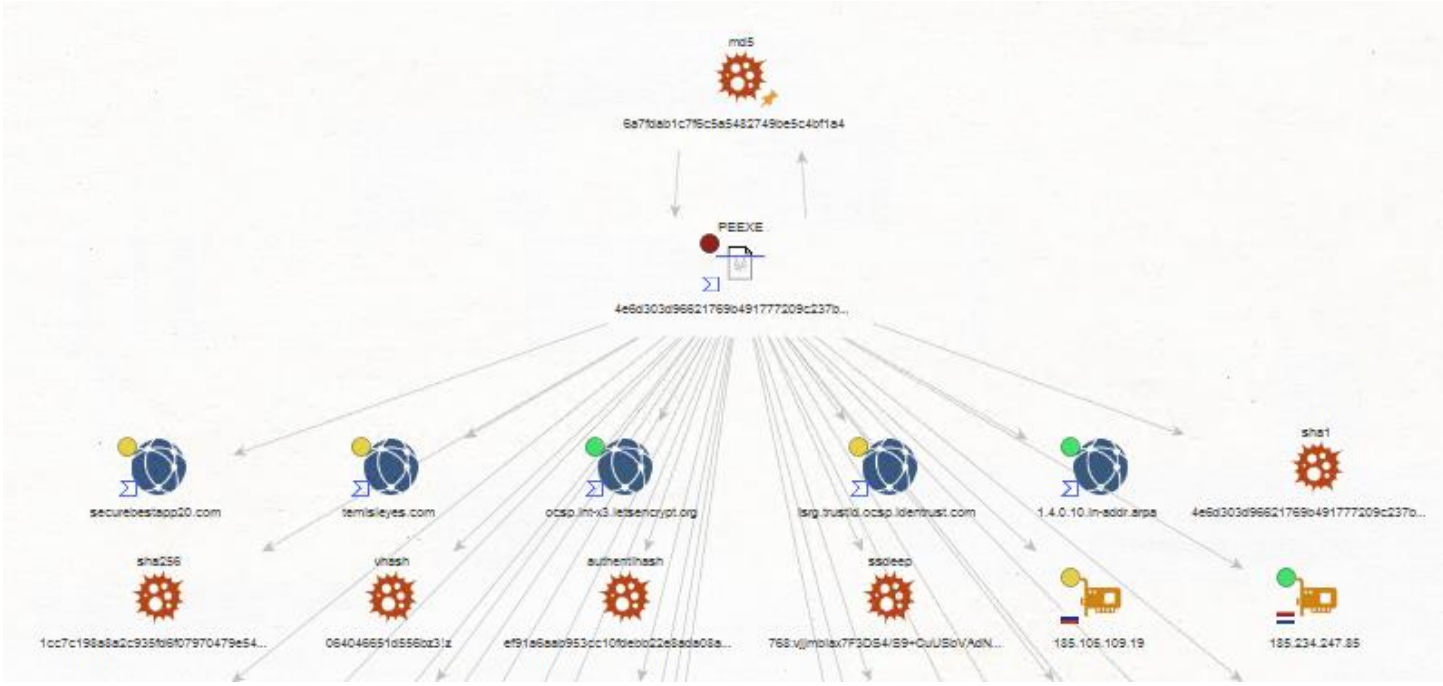
- We have investigated alerts regarding DarkSide Ransomware and communication was blocked on QRadar.



Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
Session Denied	Palo Alto @ [redacted]	1	May 14, 2021, 2:14:01 PM	Firewall Deny	10.43.30.93	53527	185.105.109.19	80	[redacted]	
Session Denied	Palo Alto @ [redacted]	4	May 14, 2021, 2:13:46 PM	Firewall Deny	10.43.30.93	53527	185.105.109.19	80	[redacted]	
Session Denied	Palo Alto @ [redacted]	2	May 14, 2021, 2:13:31 PM	Firewall Deny	10.43.30.93	53500	185.105.109.19	80	[redacted]	
Session Denied	Palo Alto @ [redacted]	1	May 14, 2021, 2:13:27 PM	Firewall Deny	10.43.30.93	53500	185.105.109.19	80	[redacted]	
Session Denied	Palo Alto @ [redacted]	1	May 14, 2021, 2:13:25 PM	Firewall Deny	10.43.30.93	53500	185.105.109.19	80	[redacted]	
Session Denied	Palo Alto @ [redacted]	1	May 14, 2021, 2:13:24 PM	Firewall Deny	10.43.30.93	53500	185.105.109.19	80	[redacted]	

Maltego Investigation

- After finding hashes of the ransomware, we started investigating on Maltego to find all the relevant data mapping to these hashes.
- We have found multiple domain and IP's mapped with this ransomware.



Action Taken

- We have blocked IOC's IP on QRadar found on different console while investigation.
- We have checked URL and Domains on Palo alto and raised a request for change of category for URL "**isrg.trustid.ocsp.identrust.com**" while other were categorized in Malware category.
- Checked on XDR for the ransomware detection executed by cymulate and it was blocked and cleaned by XDR.