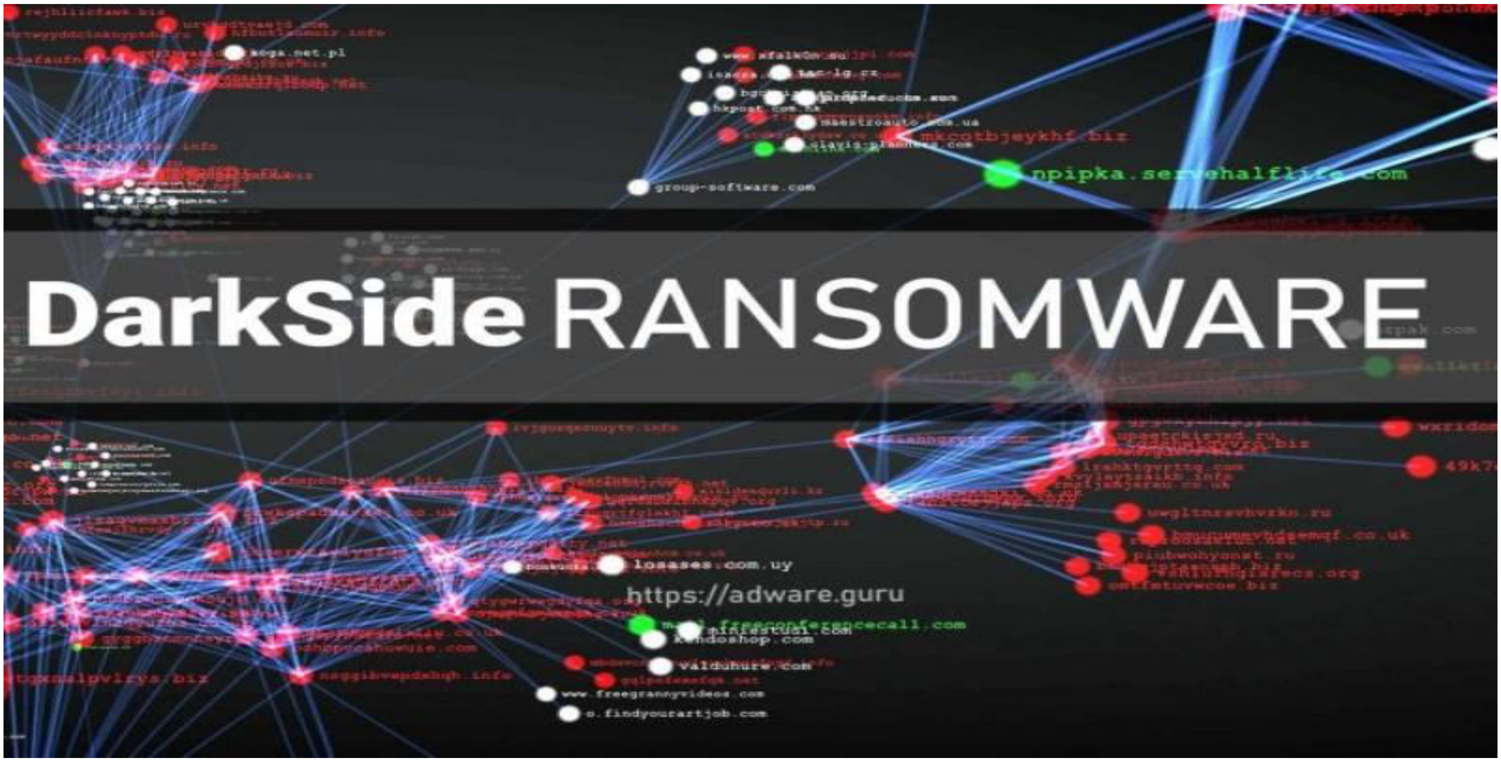


In August 2020, the threat actor group Carbon Spider associated with the ReVil group introduced a new ransomware called Darkside Ransomware . It was later offered as a RaaS (Ransomware as a Service) in November 2020 It uses a variety of methods to gain initial access to its target system specifically through phishing, Remote Desktop Protocol (RDP) exploitation, Cobalt Strike, and other exploits it gains a foothold, it moves to the Domain Controller (DC), where it proceeds to steal credentials as well as other valuable assets for data exfiltration It then continues its lateral movement through the system, eventually using the DC network share to deploy the ransomware to connected machines (Network spreading in terms).

Capabilities :

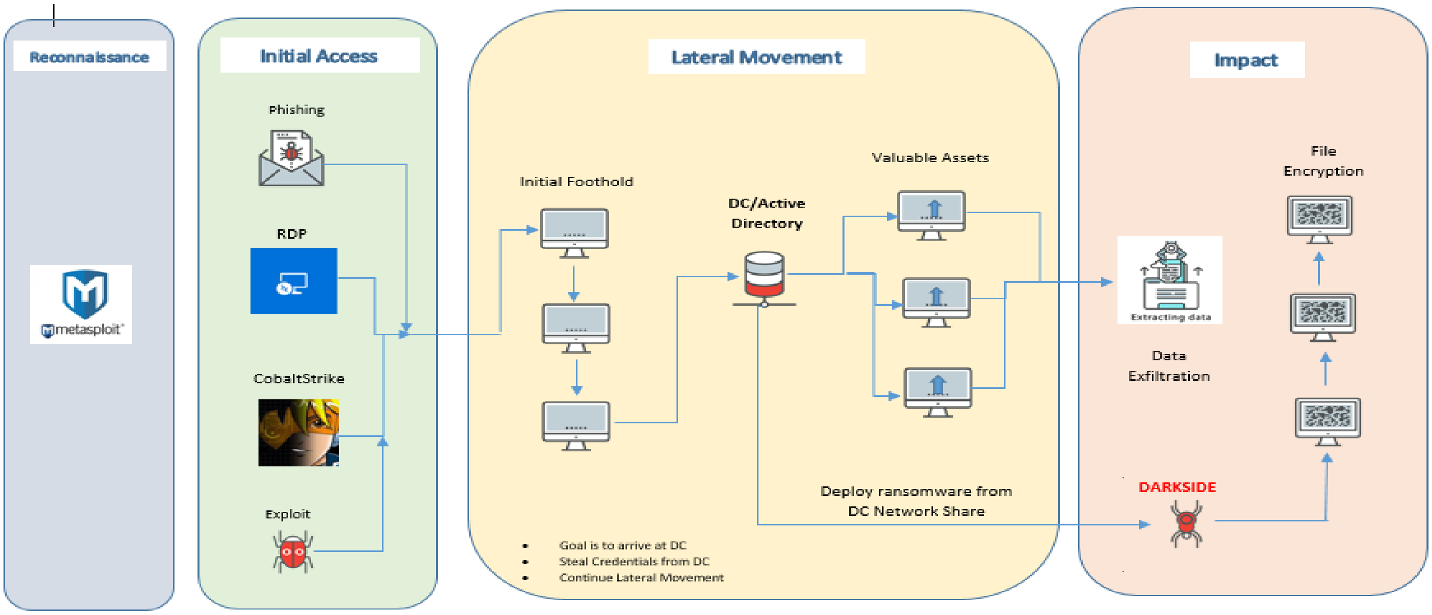
- **File encryption**
- **Credentials Stealing**
- **Data Exfiltration**
- **Lateral Movement**
- **Privilege Escalation**

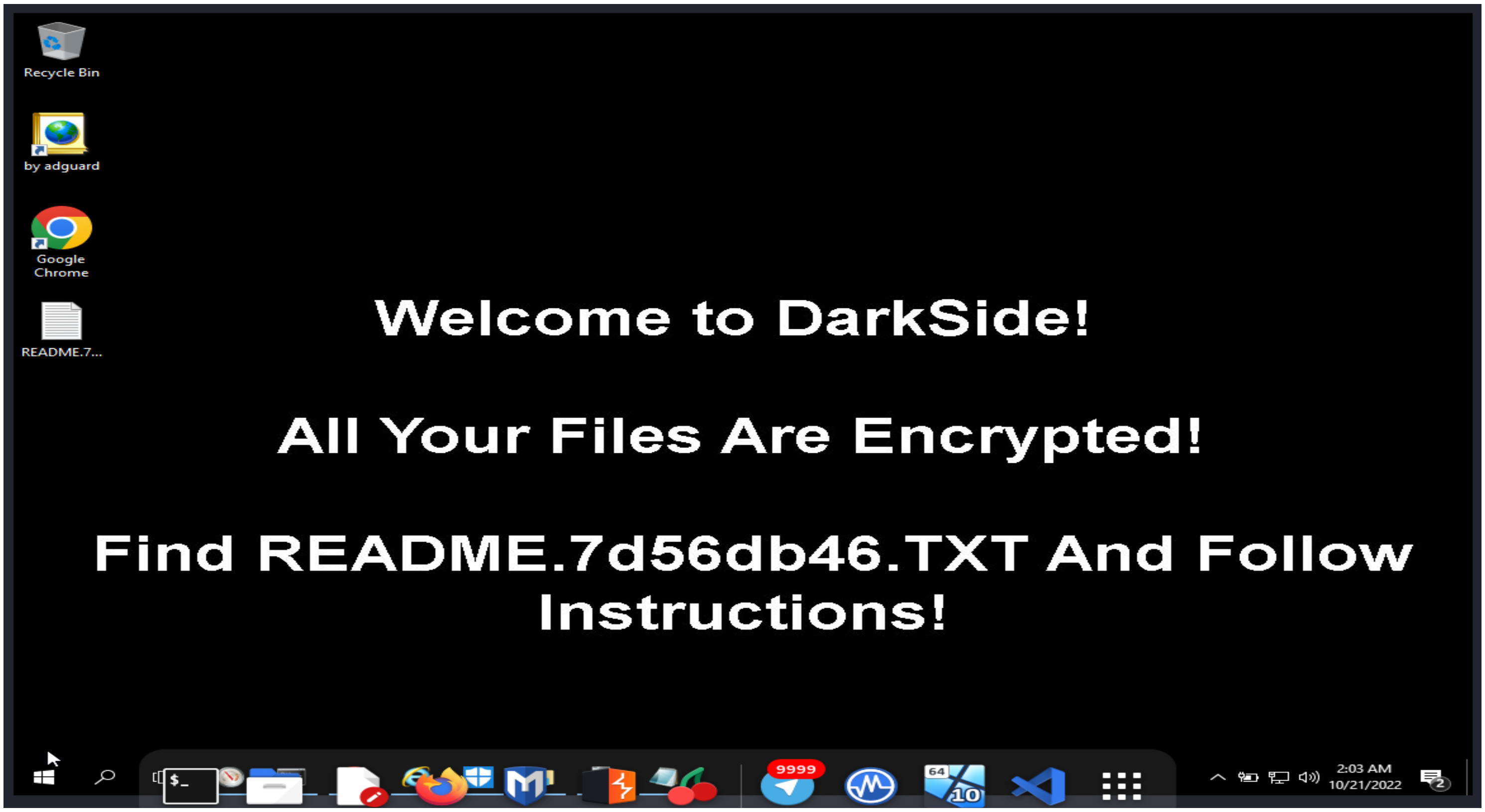
Impact :

- **Data loss –** loosing of important files , documents , due to encryption
- **Money loss –** attackers ask to pay in order to decrypt files that were affected

File Signature:

MD5	979692cd7fc638beea6e9d68c752f360
SHA-1	c511ae4d80aaa281c610190aa13630de61ca714c
SHA-256	0a0c225f0e5ee941a79f2b7701f1285e4975a2859eb4d025d96d9e366e81abb9



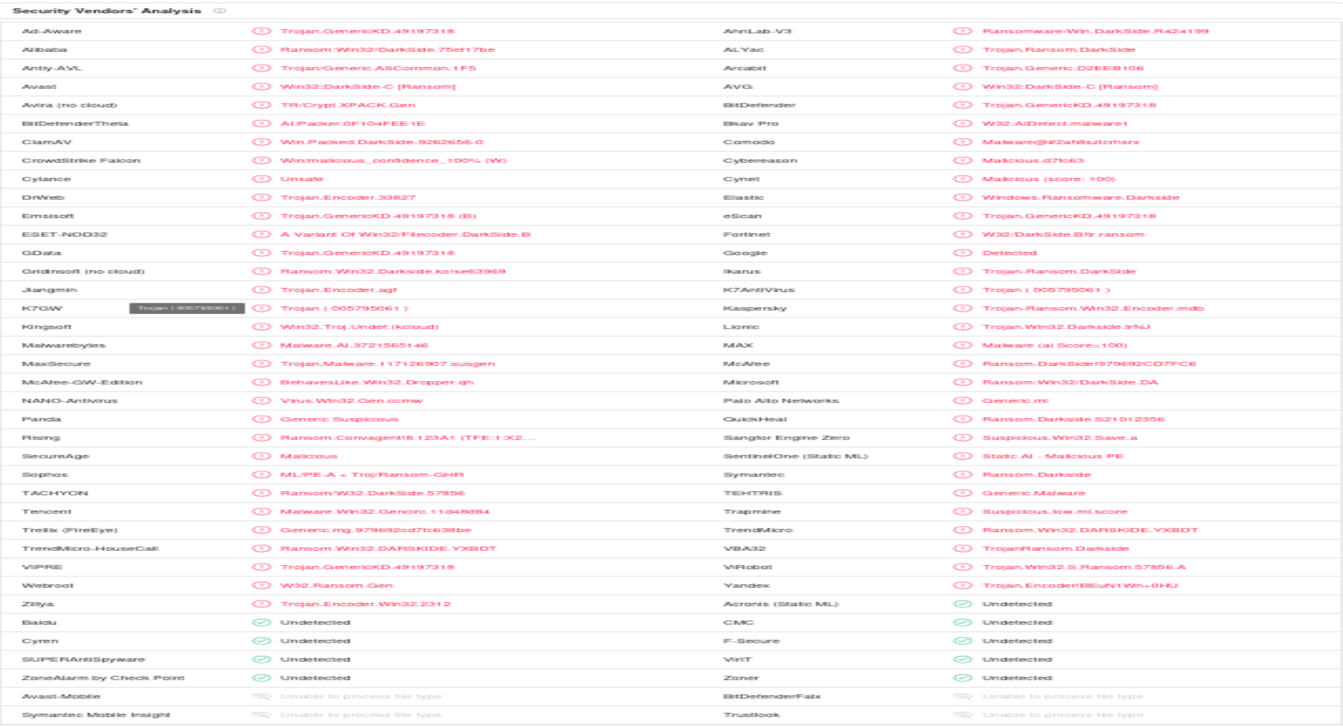


Welcome to DarkSide!

All Your Files Are Encrypted!

Find README.7d56db46.TXT And Follow Instructions!

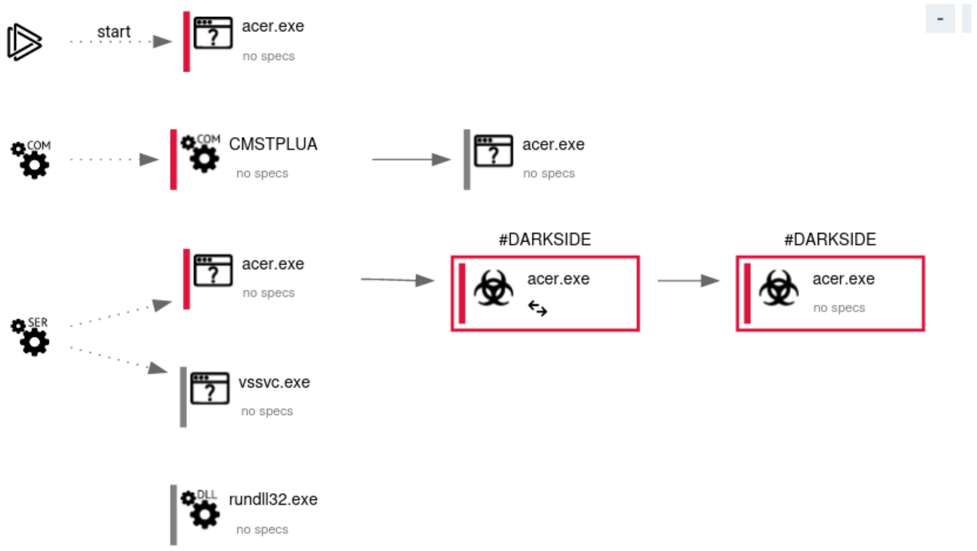
File Reputation :



Security Vendors' Analysis

Ad-Aware	Trojan.GenericKD.49197318	AhnLab-V3	Ransomware/Win.DarkSide.R424199
Alibaba	Ransom:Win32/DarkSide.75ef17be	ALYac	Trojan.Ransom.DarkSide
Antiy-AVL	Trojan/Generic.ASCommon.1F5	Arcabit	Trojan.Generic.D2EEB106
Avast	Win32:DarkSide-C [Ransom]	AVG	Win32:DarkSide-C [Ransom]
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	Trojan.GenericKD.49197318
BitDefenderTheta	AI:Packer.0F104FEE1E	Bkav Pro	W32.AIDetect.malware1
ClamAV	Win.Packed.DarkSide-9262656-0	Comodo	Malware@#2ah8szdcrhsrx
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.d7fc63
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.Encoder.33827	Elastic	Windows.Ransomware.Darkside
Emsisoft	Trojan.GenericKD.49197318 (B)	eScan	Trojan.GenericKD.49197318
ESET-NOD32	A Variant Of Win32/Filecoder.DarkSide.B	Fortinet	W32/DarkSide.B!tr.ransom
GData	Trojan.GenericKD.49197318	Google	Detected
Gridinsoft (no cloud)	Ransom.Win32.Darkside.ko!se63969	Ikarus	Trojan-Ransom.DarkSide
Jiangmin	Trojan.Encoder.agf	K7AntiVirus	Trojan (005795061)
K7GW Trojan (005795061)	Trojan (005795061)	Kaspersky	Trojan-Ransom.Win32.Encoder.mdb
Kingsoft	Win32.Troj.Undef.(kcloud)	Lionic	Trojan.Win32.Darkside.trNJ
Malwarebytes	Malware.AI.3721565146	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.117126907.susgen	McAfee	Ransom-DarkSide!979692CD7FC6
McAfee-GW-Edition	BehavesLike.Win32.Dropper.qh	Microsoft	Ransom:Win32/DarkSide.DA
NANO-Antivirus	Virus.Win32.Gen.ccmw	Palo Alto Networks	Generic.ml
Panda	Generic Suspicious	QuickHeal	Ransom.Darkside.S21012356
Rising	Ransom.Convagent!8.123A1 (TFE:1:X2...	Sangfor Engine Zero	Suspicious.Win32.Save.a
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Malicious PE
Sophos	ML/PE-A + Troj/Ransom-GHR	Symantec	Ransom.Darkside
TACHYON	Ransom/W32.DarkSide.57856	TEHTRIS	Generic.Malware
Tencent	Malware.Win32.Gencirc.11d48d84	Trapmine	Suspicious.low.ml.score
Trellix (FireEye)	Generic.mg.979692cd7fc638be	TrendMicro	Ransom.Win32.DARSKIDE.YXBDT
TrendMicro-HouseCall	Ransom.Win32.DARSKIDE.YXBDT	VBA32	TrojanRansom.Darkside
VIPRE	Trojan.GenericKD.49197318	ViRobot	Trojan.Win32.S.Ransom.57856.A
Webroot	W32.Ransom.Gen	Yandex	Trojan.Encoder!BEuN1Wn+0HU
Zillya	Trojan.Encoder.Win32.2312	Acronis (Static ML)	✓ Undetected
Baidu	✓ Undetected	CMC	✓ Undetected
Cyren	✓ Undetected	F-Secure	✓ Undetected
SUPERAntiSpyware	✓ Undetected	VirIT	✓ Undetected
ZoneAlarm by Check Point	✓ Undetected	Zoner	✓ Undetected
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

Process Graph :



DarkSide ransomware makes use of vulnerabilities CVE-2019-5544 and CVE-2020-3992 Both vulnerabilities have widely available patches, but attackers are targeting to organizations using unpatched or older versions of the software. During encryption DarkSide ransomware uses a customized ransom note and file extension for their victims.

DarkSide ransomware checks for if the user has administrator privileges; if not, it will try to get administrator privileges by using UAC bypass technique making use of CMSTPLUA COM interface.

Data Ex-filtration :

DarkSide ransomware identified data backup applications, ex-filtrates data, and then encrypts local files as part of the ransomware deployment.

Delete Volume Shadow Copies :

Ransomware often attempt to delete the volume shadow copies of the files on a given computer so that their victims will not be able to restore file access by reverting to the shadow copies. DarkSide ransomware deletes the volume shadow copies via PowerShell scripts.

Ex :

```
powershell -ep bypass -c “(0..61) | % {$s+=[char] [byte] (‘0x’+’4756742D576D694F626A6563742057696e33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20’.Substring(2*$_,2))};”
```

```
powershell -ep bypass -c “(0..61) | % {$s+=[char] [byte] (‘0x’+’Get-WmiObjectWin32_showdowcopy | ForEach-Object {$_.Delete();}’.Substring(2*$_,2))};’
```

Editing registry keys in windows :

HKEY_USERS\.DEFAULT\Software\Classes\Local Settings\MuiCache\16C\52C64B7E – Language

HKEY_USERS\.DEFAULT\Software\Microsoft\RestartManager\Session0000

HKEY_USERS\S-1-5-21-1302019708-1500728564-335382590-1000\Control Panel\Desktop – changing wallpaper

HKEY_USERS\S-1-5-21-1302019708-1500728564-335382590-1000\Control Panel\Desktop -

changing wallpaper style

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\CABD2A79A1076A31F21D253635CB039D4329A5E8 – changing the root certificates

Bypassing Security Protections :

DarkSide disables security protection services using the stuxnet (Impair Defenses) technique to avoid possible detection of their tools and activities. This can take the form of killing security software or event logging processes, deleting Registry keys so that tools do not start at run time, or other methods to interfere with security tools scanning or reporting information. DarkSide ransomware deletes the services .

Ransomware Execution :

Ransomware generates the custom file extension based on machine GUID and using API RtlComputeCRC32. File extension generated by using Machine GUID is of 8 characters and will be added to each encrypted file name.

To prevent ransomware detection, DarkSide uses encrypted APIs, strings and ransom notes

DarkSide ransomware excludes some of the files based on the file extension. Files are encrypted using Salsa20 and a key randomly generated using RtlRandomEx API and encrypted using an RSA-1024 public key.

Ransomware attackers can attack virtual infrastructure through weak versions of the VMware ESXi hypervisor. DarkSide ransomware attackers have used CVE-2019-5544 and CVE-2020-3992 vulnerabilities in VMware ESXi. Both vulnerabilities are patched, but attackers are still targeting organizations using unpatched or older versions of the software. Open SLP (Service Layer Protocol) is used for multiple virtual machines to store information on a single server in VMware ESXi hypervisor.

Detection & Metigation :

- Keep strong and unique passwords for login accounts.
- Configure firewall in following way:
  - Deny access to Public IPs to important ports (RDP port 3389)
  - Allow access to only IP6 which are under your control.
- Use VPN to access the network, instead of exposing RDP to the Internet. Possibly implement Two Factor Authentication (2FA).
- Create a separate network folder for each user when managing access to shared network folders.
- Establish a lockout policy that prevents the ability to guess credentials.
- Turn off the RDP if it is not used. If needed, change the RDP port to a non-standard port.
- Do not provide administrative privileges to users. Do not stay logged in as administrator unless strictly required. In addition, avoid browsing, opening documents, or other regular work activities while logged in as an administrator.

Conclusion :

To detect DarkSide ransomware attack, keep an eye out not only for attack code but also monitor for any evidence of the privilege escalation, impair defenses and data exfiltration techniques described above. To determine whether an organization has been impacted by DarkSide ransomware, check client-facing devices and applications for any signs of unauthorized access. To identify potential data exfiltration, identify unusual patterns of outbound traffic.

Files of DarkSide ransomware:

https://github.com/TUDDUMDEBBA/dark-side-ransomware.git

Report of DarkSide ransomware :

any.run (report of DarkSide Ransomware)

File reputation :

Virus total (report of DarkSIde Ransomeware)