Shining a Light on DARKSIDE Ransomware Operations

By Mandiant

Published: 2021-05-11 · Archived: 2026-04-05 19:06:37 UTC

Written by: Jordan Nuce, Jeremy Kennelly, Kimberly Goody, Andrew Moore, Alyssa Rahman, Matt Williams, Brendan McKeague, Jared Wilson

---

Update (May 14): Mandiant has observed multiple actors cite a May 13 announcement that appeared to be shared with DARKSIDE RaaS affiliates by the operators of the service. This announcement stated that they lost access to their infrastructure, including their blog, payment, and CDN servers, and would be closing their service. Decrypters would also be provided for companies who have not paid, possibly to their affiliates to distribute. The post cited law enforcement pressure and pressure from the United States for this decision. We have not independently validated these claims and there is some speculation by other actors that this could be an exit scam.

Background

Since initially surfacing in August 2020, the creators of DARKSIDE ransomware and their affiliates have launched a global crime spree affecting organizations in more than 15 countries and multiple industry verticals. Like many of their peers, these actors conduct multifaceted extortion where data is both exfiltrated and encrypted in place, allowing them to demand payment for unlocking and the non-release of stolen data to exert more pressure on victims.

The origins of these incidents are not monolithic. DARKSIDE ransomware operates as a ransomware-as-a-service (RaaS) wherein profit is shared between its owners and partners, or affiliates, who provide access to organizations and deploy the ransomware. Mandiant currently tracks multiple threat clusters that have deployed this ransomware, which is consistent with multiple affiliates using DARKSIDE. These clusters demonstrated varying levels of technical sophistication throughout intrusions. While the threat actors commonly relied on commercially available and legitimate tools to facilitate various stages of their operations, at least one of the threat clusters also employed a now patched zero-day vulnerability.

Reporting on DARKSIDE has been available in advance of this blog post to users of Mandiant Advantage Free, a no-cost version of our threat intelligence platform.

Targeting

Mandiant has identified multiple DARKSIDE victims through our incident response engagements and from reports on the DARKSIDE blog. Most of the victim organizations were based in the United States and span across multiple sectors, including financial services, legal, manufacturing, professional services, retail, and technology. The number of publicly named victims on the DARKSIDE blog has increased overall since August 2020, with the exception of a significant dip in the number of victims named during January 2021 (Figure 1). It is plausible that

the decline in January was due to threat actors using DARKSIDE taking a break during the holiday season. The overall growth in the number of victims demonstrates the increasing use of the DARKSIDE ransomware by multiple affiliates.

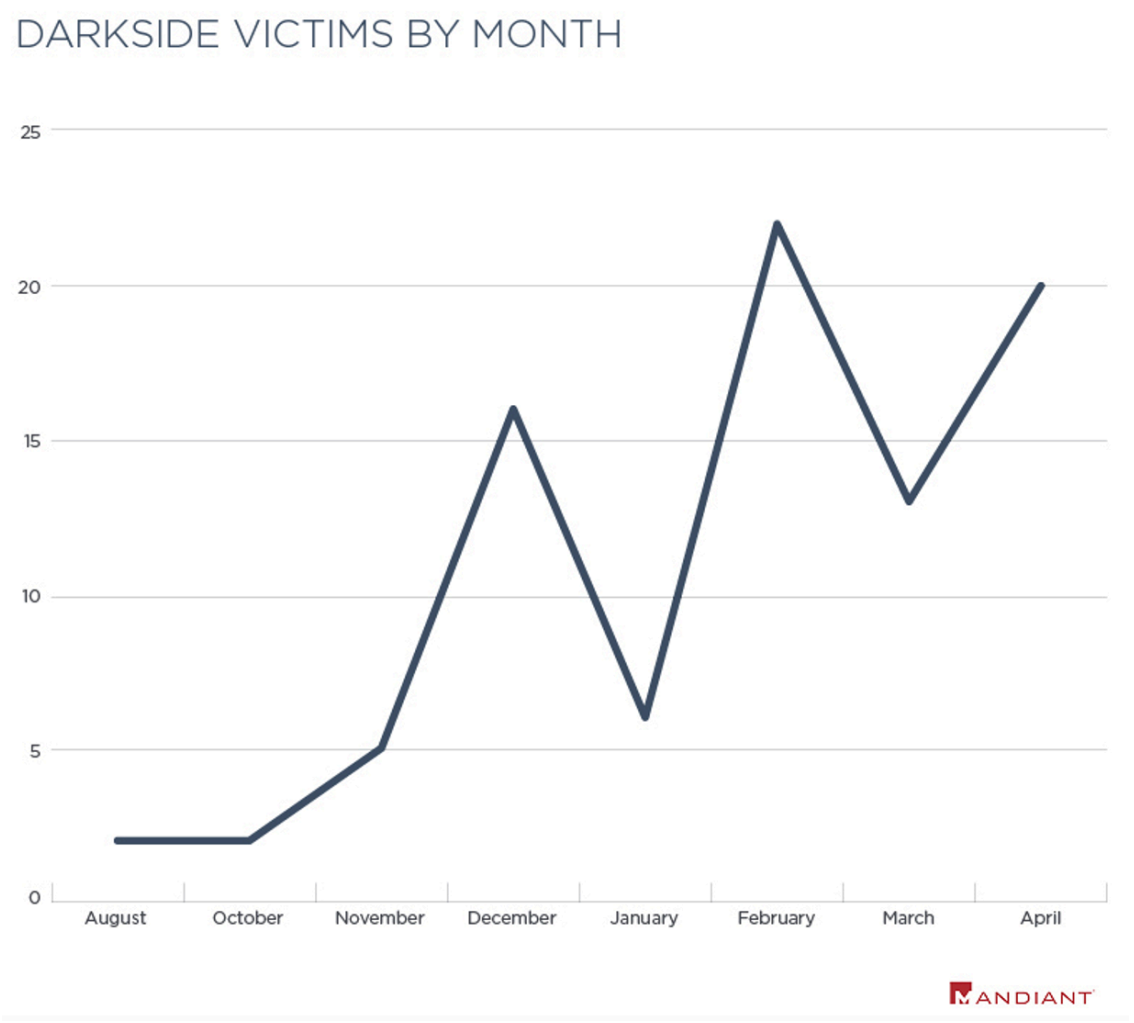

Figure 1: Known DARKSIDE victims (August 2020 to April 2021)

DARKSIDE Ransomware Service

Beginning in November 2020, the Russian-speaking actor "darksupp" advertised DARKSIDE RaaS on the Russian-language forums exploit.in and xss.is. In April 2021, darksupp posted an update for the "Darkside 2.0" RaaS that included several new features and a description of the types of partners and services they were currently seeking (Table 1). Affiliates retain a percentage of the ransom fee from each victim. Based on forum advertisements, the RaaS operators take 25% for ransom fees less than $500,000, but this decreases to 10 percent for ransom fees greater than $5 million.

In addition to providing builds of DARKSIDE ransomware, the operators of this service also maintain a blog accessible via TOR. The actors use this site to publicize victims in an attempt to pressure these organizations into paying for the non-release of stolen data. A recent update to their underground forum advertisement also indicates that actors may attempt to DDoS victim organizations. The actor darksupp has stated that affiliates are prohibited from targeting hospitals, schools, universities, non-profit organizations, and public sector entities. This may be an

effort by the actor(s) to deter law enforcement action, since targeting of these sectors may invite additional scrutiny. Affiliates are also prohibited from targeting organizations in Commonwealth of Independent States (CIS) nations.

Advertisement Date/Version	**Feature/Update**	**Related Reporting (for Mandiant Advantage customers)**
Nov. 10, 2020 (V1)	Ability to generate builds for both Windows and Linux environments from within the administration panel. Encrypts files using Salsa20 encryption along with an RSA-1024 public key Access to an administrative panel via TOR that can be used by clients 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 for the purposes of shaming victims and coercing them to pay ransom demands	20-00023273
April 14, 2021 (V2.0)	Automated test decryption. The process from encryption to withdrawal of money is automated and no longer relies on support. 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	21-00008435

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

DARKSIDE Affiliates

DARKSIDE RaaS affiliates are required to pass an interview after which they are provided access to an administration panel (Figure 2). Within this panel, affiliates can perform various actions such as creating a ransomware build, specifying content for the DARKSIDE blog, managing victims, and contacting support. Mandiant has identified at least five Russian-speaking actors who may currently, or have previously, been DARKSIDE affiliates. Relevant advertisements associated with a portion of these threat actors have been aimed at finding either initial access providers or actors capable of deploying ransomware on accesses already obtained.

Some actors claiming to use DARKSIDE have also allegedly partnered with other RaaS affiliate programs, including BABUK and SODINOKIBI (aka REvil). For more information on these threat actors, please see Mandiant Advantage.

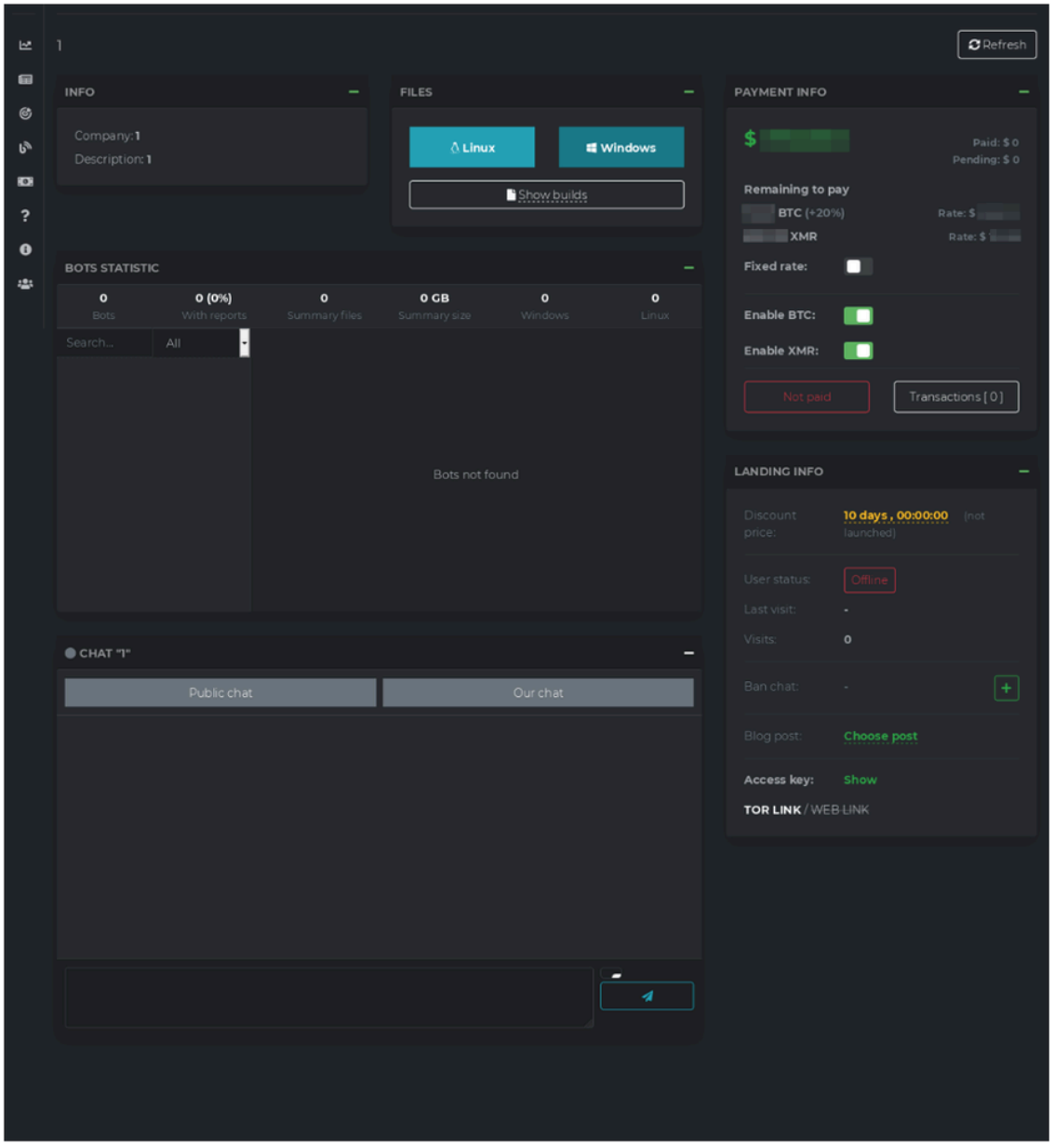

Figure 2: DARKSIDE affiliate panel

Attack Lifecycle

Mandiant currently tracks five clusters of threat activity that have involved the deployment of DARKSIDE. For more information on uncategorized threats, refer to our post, "DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors." These clusters may represent different affiliates of the DARKSIDE RaaS platform. Throughout observed incidents, the threat actor commonly relied on various publicly available and legitimate tools that are commonly used to facilitate various stages of the attack lifecycle in post-exploitation ransomware attacks (Figure 3). Additional details on three of these UNC groups are included below.

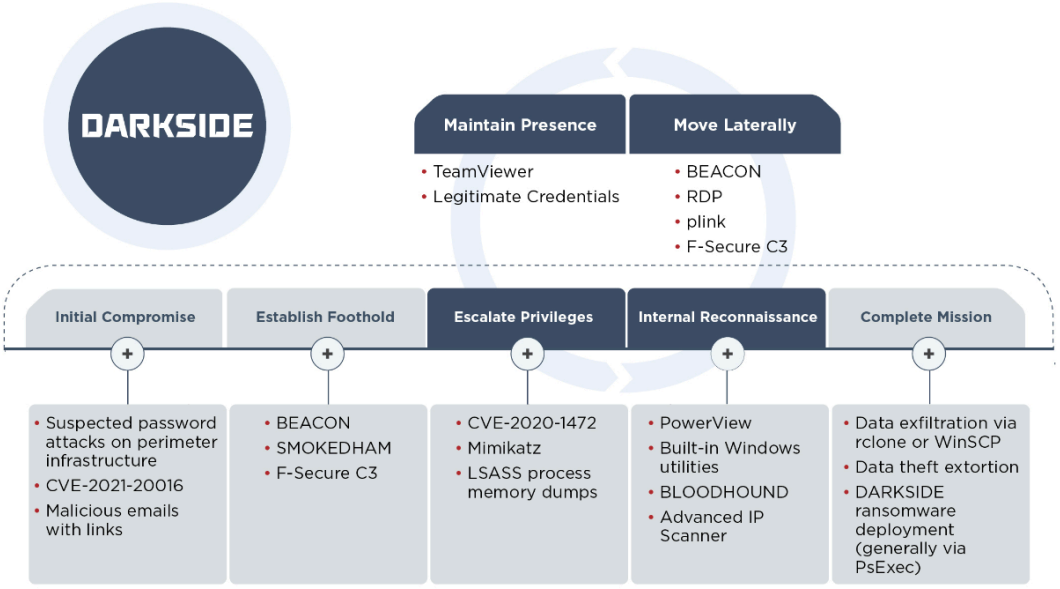

Figure 3: TTPs seen throughout DARKSIDE ransomware engagements

UNC2628

UNC2628 has been active since at least February 2021. Their intrusions progress relatively quickly with the threat actor typically deploying ransomware in two to three days. We have some evidence that suggests UNC2628 has partnered with other RaaS including SODINOKIBI (REvil) and NETWALKER.

- In multiple cases we have observed suspicious authentication attempts against corporate VPN infrastructure immediately prior to the start of interactive intrusion operations. The authentication patterns were consistent with a password spraying attack, though available forensic evidence was insufficient to definitively attribute this precursor activity to UNC2628.
- In cases where evidence was available, the threat actor appeared to obtain initial access through corporate VPN infrastructure using legitimate credentials.
- UNC2628 has interacted with victim environments using various legitimate accounts, but in multiple cases has also created and used a domain account with the username 'spservice'. Across all known intrusions, UNC2628 has made heavy use of the Cobalt Strike framework and BEACON payloads. BEACON command and control (C2) infrastructure attributed to this actor has included the following:
    - hxxps://104.193.252[.]197:443/
    - hxxps://162.244.81[.]253:443/
    - hxxps://185.180.197[.]86:443/
    - hxxps://athaliaoriginals[.]com/
    - hxxps://lagrom[.]com:443/font.html
    - hxxps://lagrom[.]com:443/night.html
    - hxxps://lagrom[.]com:443/online.html
    - hxxps://lagrom[.]com:443/send.html
    - hxxps://lagrom[.]com/find.html?key=id#-
- In at least some cases there is evidence to suggest this actor has employed Mimikatz for credential theft and privilege escalation.

- The threat actor appeared to have used built-in commands such as ‘net’ and ‘ping’ to perform basic reconnaissance of the internal network, though it is likely that additional reconnaissance was performed via BEACON and not represented in available log sources.
- UNC2628 has moved laterally in environments almost exclusively via RDP using legitimate credentials and Cobalt Strike BEACON payloads. This threat cluster uses both HTTPS BEACON payloads and SMB BEACON, the latter almost exclusively using named pipes beginning with “\\.\pipe\UIA_PIPE_”
- Intrusions attributed to this threat cluster have progressed swiftly from intrusion to data theft and ransomware deployment, and have thus not focused heavily on maintaining a persistent foothold in impacted environments. Despite this, UNC2628 has maintained access via the collection of legitimate credentials, the creation of attacker-controlled domain accounts (spservice), and via the creation of Windows services intended to launch BEACON. Notably, UNC2628 has repeatedly loaded BEACON with a service named ‘CitrixInit’.
- UNC2628 has also employed F-Secure Labs' Custom Command and Control (C3) framework, deploying relays configured to proxy C2 communications through the Slack API. Based on this actor's other TTPs they were likely using C3 to obfuscate Cobalt Strike BEACON traffic.
- The threat actor has exfiltrated data over SFTP using Rclone to systems in cloud hosting environments. Rclone is a command line utility to manage files for cloud storage applications. Notably, the infrastructure used for data exfiltration has been reused across multiple intrusions. In one case, the data exfiltration occurred on the same day that the intrusion began.
- UNC2628 deploys DARKSIDE ransomware encryptors using PsExec to a list of hosts contained in multiple text files.
- The threat actor has used the following directories, placing copies of backdoors, ransomware binaries, copies of PsExec, and lists of victim hosts within them.
    - C:\run\
    - C:\home\
    - C:\tara\
    - C:\Users\[username]\Music\
    - C:\Users\Public

UNC2659

UNC2659 has been active since at least January 2021. We have observed the threat actor move through the whole attack lifecycle in under 10 days. UNC2659 is notable given their use of an exploit in the SonicWall SMA100 SSL VPN product, which has since been patched by SonicWall. The threat actor appeared to download several tools used for various phases of the attack lifecycle directly from those tools’ legitimate public websites.

- The threat actor obtained initial access to their victim by exploiting CVE-2021-20016, an exploit in the SonicWall SMA100 SSL VPN product, which has been patched by SonicWall. There is some evidence to suggest the threat actor may have used the vulnerability to disable multi-factor authentication options on the SonicWall VPN, although this has not been confirmed.
- The threat actor leveraged TeamViewer (TeamViewer_Setup.exe) to establish persistence within the victim environment. Available evidence suggests that the threat actor downloaded TeamViewer directly from the following URL and also browsed for locations from which they could download the AnyDesk utility.

    - hxxps://dl.teamviewer[.]com/download/version_15x/TeamViewer_Setup.exe
- The threat actor appeared to download the file rclone.exe directly from rclone[.]org - hxxps://downloads.rclone[.]org/v1.54.0/rclone-v1.54.0-windows-amd64.zip. The threat actors were seen using rclone to exfiltrate hundreds of gigabytes of data over the SMB protocol to the pCloud cloud-based hosting and storage service.
- The threat actor deployed the file power_encryptor.exe in a victim environment, encrypting files and creating ransom notes over the SMB protocol.
- Mandiant observed the threat actor navigate to ESXi administration interfaces and disable snapshot features prior to the ransomware encryptor deployment, which affected several VM images.

UNC2465

UNC2465 activity dates back to at least April 2019 and is characterized by their use of similar TTPs to distribute the PowerShell-based .NET backdoor SMOKEDHAM in victim environments. In one case where DARKSIDE was deployed, there were months-long gaps, with only intermittent activity between the time of initial compromise to ransomware deployment. In some cases, this could indicate that initial access was provided by a separate actor.

- UNC2465 used phishing emails and legitimate services to deliver the SMOKEDHAM backdoor. SMOKEDHAM is a .NET backdoor that supports keylogging, taking screenshots, and executing arbitrary .NET commands. During one incident, the threat actor appeared to establish a line of communication with the victim before sending a malicious Google Drive link delivering an archive containing an LNK downloader. More recent UNC2465 emails have used Dropbox links with a ZIP archive containing malicious LNK files that, when executed, would ultimately lead to SMOKEDHAM being downloaded onto the system.
- UNC2465 has used Advanced IP Scanner, BLOODHOUND, and RDP for internal reconnaissance and lateral movement activities within victim environments.
- The threat actor has used Mimikatz for credential harvesting to escalate privileges in the victim network.
- UNC2465 also uses the publicly available NGROK utility to bypass firewalls and expose remote desktop service ports, like RDP and WinRM, to the open internet.
- Mandiant has observed the threat actor using PsExec and cron jobs to deploy the DARKSIDE ransomware.
- UNC2465 has called the customer support lines of victims and told them that data was stolen and instructed them to follow the link in the ransom note.

Implications

We believe that threat actors have become more proficient at conducting multifaceted extortion operations and that this success has directly contributed to the rapid increase in the number of high-impact ransomware incidents over the past few years. Ransomware operators have incorporated additional extortion tactics designed to increase the likelihood that victims will acquiesce to paying the ransom prices. As one example, in late April 2021, the DARKSIDE operators released a press release stating that they were targeting organizations listed on the NASDAQ and other stock markets. They indicated that they would be willing to give stock traders information about upcoming leaks in order to allow them potential profits due to stock price drops after an announced breach. In another notable example, an attacker was able to obtain the victim's cyber insurance policy and leveraged this

information during the ransom negotiation process refusing to lower the ransom amount given their knowledge of the policy limits. This reinforces that during the post-exploitation phase of ransomware incidents, threat actors can engage in internal reconnaissance and obtain data to increase their negotiating power. We expect that the extortion tactics that threat actors use to pressure victims will continue to evolve throughout 2021.

Based on the evidence that DARKSIDE ransomware is distributed by multiple actors, we anticipate that the TTPs used throughout incidents associated with this ransomware will continue to vary somewhat. For more comprehensive recommendations for addressing ransomware, please refer to our blog post: "Ransomware Protection and Containment Strategies: Practical Guidance for Endpoint Protection, Hardening, and Containment" and the linked white paper.

Acknowledgements

Beyond the comparatively small number of people who are listed as authors on this report are hundreds of consultants, analysts and reverse-engineers who tirelessly put in the work needed to respond to intrusions at breakneck pace and still maintain unbelievably high analytical standards. This larger group has set the foundation for all of our work, but a smaller group of people contributed more directly to producing this report and we would like to thank them by name. We would like to specifically thank Bryce Abdo and Matthew Dunwoody from our Advanced Practices team and Jay Smith from FLARE, all of whom provided analytical support and technical review. Notable support was also provided by Ioana Teaca, and Muhammadumer Khan.

Appendix A: DARKSIDE Ransomware Analysis

DARKSIDE is a ransomware written in C that may be configured to encrypt files on fixed and removable disks as well as network shares. DARKSIDE RaaS affiliates are given access to an administration panel on which they create builds for specific victims. The panel allows some degree of customization for each ransomware build such as choosing the encryption mode and whether local disks and network shares should be encrypted (Figures 4). The following malware analysis is based on the file MD5: 1a700f845849e573ab3148daef1a3b0b. A more recently analyzed DARKSIDE sample had the following notable differences:

- The option for beaconing to a C2 server was disabled and the configuration entry that would have contained a C2 server was removed.
- Included a persistence mechanism in which the malware creates and launches itself as a service.
- Contained a set of hard-coded victim credentials that were used to attempt to logon as a local user. If the user token retrieved based on the stolen credentials is an admin token and is part of the domain administrators' group, it is used for network enumeration and file permission access.

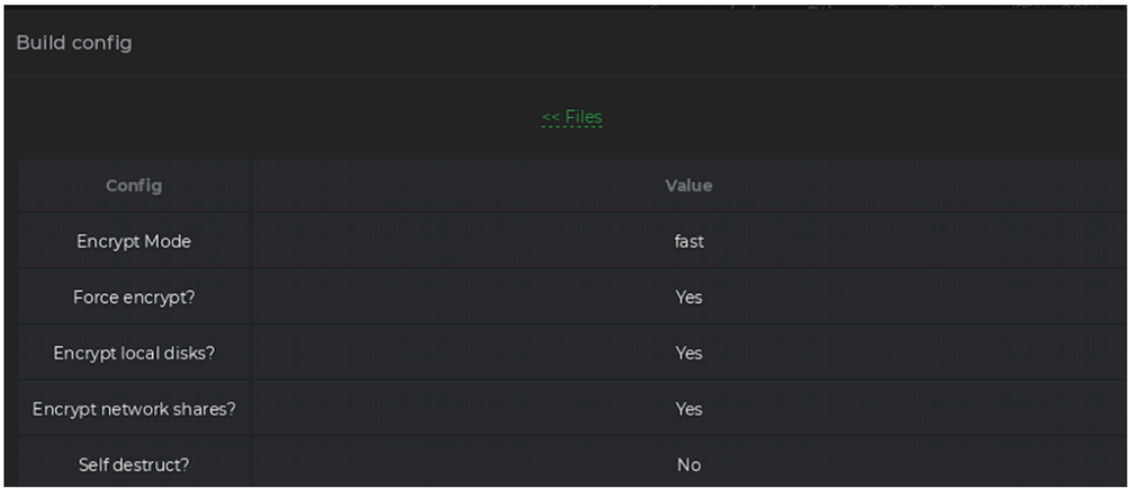

Figure 4: DARKSIDE build configuration options appearing in the administration panel

Host-Based Indicators

Persistence Mechanism

Early versions of the malware did not contain a persistence mechanism. An external tool or installer was required if the attacker desired persistence. A DARKSIDE version observed in May 2021 implement a persistence mechanism through which the malware creates and launches itself as a service with a service name and description named using eight pseudo-randomly defined lowercase hexadecimal characters (e.g., ".e98fc8f7") that are also appended by the malware to various other artifacts it created. This string of characters is referenced as . :

Service Name:
Description:

Filesystem Artifacts

Created Files

%CD%\LOG.TXT
README.TXT

May version: %PROGRAMDATA%\.ico

Registry Artifacts

The DARKSIDE version observed in May sets the following registry key:

HKCR\\DefaultIcon\\DefaultIcon=%PROGRAMDATA%\.ico

Details

Configuration

The malware initializes a 0x100-byte keystream used to decrypt strings and configuration data. Strings are decrypted as needed and overwritten with NULL bytes after use. The malware's configuration size is 0xBE9 bytes. A portion of the decrypted configuration is shown in Figure 5.

```
 00000000  01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000080  95 AA A8 7C 2B 6A D5 12 0E 73 B3 7D BD 16 25 62  •ª¨|+jÕ..s³}½.%b
00000090  A4 A8 BF 19 73 F7 E0 BC DF 02 A8 94 32 CF 0C C0  ¤¨¿.s÷à¼ß.¨"2Ï.À
000000A0  C5 83 0F 14 66 02 87 EE FD 29 96 DF 02 05 C1 12  Åƒ..f.‡îý)–ß..Á.
000000B0  3E 43 A7 59 E1 F0 C4 5D AE E1 20 2E 77 D9 CA 3C  >C§YáðÄ]®á .wÙÊ<
000000C0  AD C6 BC 84 75 1C E7 0B F0 30 2A 51 13 7A B2 66  .Æ¼„u.ç.ð0*Q.z²f
000000D0  44 73 79 E1 E4 69 C3 CA 1B C1 76 63 65 95 EA CA  DsyáäiÃÊ.Ávce•êÊ
000000E0  F6 10 68 0D CE 36 61 F9 57 B9 19 50 31 D4 E1 70  ö.h.Î6aùW¹.P1Ôáp
000000F0  EC 7B 33 1E 4F 17 E1 80 1D BC CF 8C D8 C5 66 41  ì{3.O.á€.¼ÏŒØÅfA
00000100  E5 0A 00 00 02 6E 01 02 15 03 43 01 8E 24 0E 72  å....n....C.Ž$.r
<cut>
```

Figure 5: Partial decrypted configuration

The sample's 0x80-byte RSA public key blob begins at offset 0x80. The DWORD value at offset 0x100 is multiplied by 64 and an amount of memory equivalent to the result is allocated. The remaining bytes, which start at offset 0x104, are aPLib-decompressed into the allocated buffer. The decompressed bytes include the ransom note and other elements of the malware's configuration described as follows (e.g., processes to terminate, files to ignore). The first 0x60 bytes of the decompressed configuration are shown in Figure 6.

```
 00000000  02 01 01 01 00 01 01 00 01 01 01 01 01 01 01 01  ................
00000010  01 01 01 01 01 01 24 00 72 00 65 00 63 00 79 00  ......$.r.e.c.y.
00000020  63 00 6C 00 65 00 2E 00 62 00 69 00 6E 00 00 00  c.l.e...b.i.n...
00000030  63 00 6F 00 6E 00 66 00 69 00 67 00 2E 00 6D 00  c.o.n.f.i.g...m.
00000040  73 00 69 00 00 00 24 00 77 00 69 00 6E 00 64 00  s.i...$.w.i.n.d.
00000050  6F 00 77 00 73 00 2E 00 7E 00 62 00 74 00 00 00  o.w.s...~.b.t...
<cut>
```

Figure 6: Partial decompressed configuration

The first byte from Figure 6 indicates the encryption mode. This sample is configured to encrypt using FAST mode. Supported values are as follows:

- 1: FULL

- 2: FAST
- Other values: AUTO

The individual bytes from offset 0x02 to offset 0x15 in Figure 6 are Boolean values that dictate the malware's behavior. The malware takes the actions listed in Table 2 based on these values. Table 2 also identifies features that are enabled or disabled for the current sample.

Offset	Enabled	Description
0x01	Yes	Unknown
0x02	Yes	Encrypt local disks
0x03	Yes	Encrypt network shares
0x04	No	Perform language check
0x05	Yes	Delete volume shadow copies
0x06	Yes	Empty Recycle Bins
0x07	No	Self-delete
0x08	Yes	Perform UAC bypass if necessary
0x09	Yes	Adjust token privileges
0x0A	Yes	Logging
0x0B	Yes	Feature not used but results in the following strings being decrypted: • https://google.com/api/version • https://yahoo.com/v2/api
0x0C	Yes	Ignore specific folders
0x0D	Yes	Ignore specific files
0x0E	Yes	Ignore specific file extensions
0x0F	Yes	Feature not used; related to these strings: "backup" and "here_backups"

0x10	Yes	Feature not used: related to these strings: "sql" and "sqlite"
0x11	Yes	Terminate processes
0x12	Yes	Stop services
0x13	Yes	Feature not used; related to a buffer that contains the repeated string "blah"
0x14	Yes	Drop ransom note
0x15	Yes	Create a mutex

Table 2: Configuration bits

UAC Bypass

If the malware does not have elevated privileges, it attempts to perform one of two User Account Control (UAC) bypasses based on the operating system (OS) version. If the OS is older than Windows 10, the malware uses a documented *slui.exe* file handler hijack technique. This involves setting the registry value HKCU\Software\Classes\exefile\shell\open\command\Default to the malware path and executing *slui.exe* using the verb "runas."

If the OS version is Windows 10 or newer, the malware attempts a UAC bypass that uses the CMSTPLUA COM interface. The decrypted strings listed in Figure 7 are used to perform this technique.

```
 Elevation:Administrator!new:
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
```

Figure 7: Decrypted UAC bypass strings

Encryption Setup

The malware generates a pseudo-random file extension based on a MAC address on the system. In a DARKSIDE version observed in May 2021, the file extension is generated using a MachineGuid registry value as a seed rather than the MAC address. The file extension consists of eight lowercase hexadecimal characters (e.g., ".e98fc8f7") and is referred to as *<ransom_ext>*. The file extension generation algorithm has been recreated in Python. If logging is enabled, the malware creates the log file *LOG<ransom_ext>.TXT* in its current directory.

The malware supports the command line argument "-path," which allows an attacker to specify a directory to target for encryption.

The sample analyzed for this report is not configured to perform a system language check. If this functionality were enabled and the check succeeded, the string "This is a Russian-Speaking System, Exit" would be written to the log file and the malware would exit.

Anti-Recovery Techniques

The malware locates and empties Recycle Bins on the system. If the process is running under WOW64, it executes the PowerShell command in Figure 8 using CreateProcess to delete volume shadow copies.

```
 powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]
('0x'+'4765742D576D694F626A6563742057696E33325F536861646F7763
6F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2*$_,2))};iex $s"
```

Figure 8: Encoded PowerShell command

The decoded command from Figure 4 is "Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}." If the malware is not running under WOW64, it uses COM objects and WMI commands to delete volume shadow copies. The decrypted strings in Figure 9 are used to facilitate this process.

```
 root/cimv2
SELECT * FROM Win32_ShadowCopy
Win32_ShadowCopy.ID='%s'
```

Figure 9: Decrypted strings related to shadow copy deletion

System Manipulation

Any service the name of which contains one of the strings listed in Figure 10 is stopped and deleted.

```
 vss
sql
svc$
memtas
mepocs
sophos
veeam
backup
```

Figure 10: Service-related strings

The version observed in May 2021 is additionally configured to stop and delete services containing the strings listed in Figure 11.

```
 GxVss
GxBlr
GxFWD
GxCVD
GxCIMgr
```

Figure 11: Additional service-related strings in May version

Any process name containing one of the strings listed in Figure 12 is terminated.

```
 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
```

Figure 12: Process-related strings

File Encryption

Based on its configuration, the malware targets fixed and removable disks as well as network shares. Some processes may be terminated so associated files can be successfully encrypted. However, the malware does not terminate processes listed in Figure 13.

```
 vmcompute.exe
vmms.exe
vmwp.exe
svchost.exe
TeamViewer.exe
explorer.exe
```

Figure 13: Processes not targeted for termination

The malware uses the strings listed in Figure 14 to ignore certain directories during the encryption process.

```
 windows
appdata
application data
boot
google
mozilla
program files
program files (x86)
programdata
system volume information
tor browser
windows.old
intel
msocache
perflogs
x64dbg
public
all users
default
```

Figure 14: Strings used to ignore directories

The files listed in Figure 15 are ignored.

```
 $recycle.bin
config.msi
$windows.~bt
$windows.~ws
```

Figure 15: Ignored files

The version observed in May 2021 is additionally configured to ignore the files listed in Figure 16.

```
 autorun.inf
boot.ini
bootfont.bin
bootsect.bak
desktop.ini
iconcache.db
ntldrntuser.dat
ntuser.dat
logntuser.ini
thumbs.db
```

Figure 16: Additional ignored files in May version

Additional files are ignored based on the extensions listed in Figure 17.

```
.386, .adv, .ani, .bat, .bin, .cab, .cmd, .com, .cpl, .cur, .deskthemepack, .diagcab, .diagcfg, .diagpkg, .dll
```

Figure 17: Ignored file extensions

Files are encrypted using Salsa20 and a key randomly generated using RtlRandomEx. Each key is encrypted using the embedded RSA-1024 public key.

Ransom Note

The malware writes the ransom note shown in Figure 18 to *README<ransom_ext>.TXT* files written to directories it traverses.

```
 ----------- [ Welcome to Dark ] ------------>

What happend?
---------------------------------------------
Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you canno
But you can restore everything by purchasing a special program from us - universal decryptor. This program will
Follow our instructions below and you will recover all your data.
Data leak
---------------------------------------------
First of all we have uploaded more then 100 GB data.
Example of data:
 - Accounting data
 - Executive data
 - Sales data
 - Customer Support data
 - Marketing data
```

```
 - Quality data
 - And more other...
Your personal leak page: http://darksidedxcftmqa[.]onion/blog/article/id/6/<REDACTED>
The data is preloaded and will be automatically published if you do not pay.
After publication, your data will be available for at least 6 months on our tor cdn servers.
We are ready:
- To provide you the evidence of stolen data
- To give you universal decrypting tool for all encrypted files.
- To delete all the stolen data.
What guarantees?
---------------------------------------------
We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our intere
All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case
We guarantee to decrypt one file for free. Go to the site and contact us.
How to get access on website?
---------------------------------------------
Using a TOR browser:
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://darksidfqzcuhtk2[.]onion/<REDACTED>
When you open our website, put the following data in the input form:
Key:
<REDACTED>
!!! DANGER !!!
DO NOT MODIFY or try to RECOVER any files yourself. We WILL NOT be able to RESTORE them.
!!! DANGER !!!
```

Figure 18: Ransom note

Decrypted Strings

```
 Global\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
https://google.com/api/version
https://yahoo.com/v2/api
sql
sqlite
$recycle.bin
config.msi
$windows.~bt
$windows.~ws
windows
appdata
application data
boot
google
mozilla
program files
program files (x86)
```

```
programdata
system volume information
tor browser
windows.old
intel
msocache
perflogs
x64dbg
public
all users
default
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
vmcompute.exe
vmms.exe
vmwp.exe
svchost.exe
TeamViewer.exe
explorer.exe
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
vss
sql
svc$
memtas
mepocs
sophos
veeam
backup
\r\nblahblahblahblahblahblahblahblahblahblahblahblahblahblahblahblah\r\nblahblahblahblahblahblahbl
ahblahblahblahblahblahblahblahblah\r\nblahblahblahblahblahblahblahblahblahblahblahblahblah
blahblah\r\nblahblahblah\r\n
\r\n----------- [ Welcome to Dark ] ------------->\r\n\r\nWhat happend?\r\n-------------------------------------
-path
INF
DBG
/C DEL /F /Q
 >> NUL
ComSpec
README
.TXT
Start Encrypting Target Folder
Encrypt Mode - AUTO
Started %u I/O Workers
Encrypted %u file(s)
Start Encrypt
[Handle %u]
File Encrypted Successful
Encrypt Mode - FAST
Encrypt Mode - FULL
This is a Russian-Speaking System, Exit
System Language Check
Encrypting Network Shares
Encrypting Local Disks
README
.TXT
Encrypt Mode - AUTO
Started %u I/O Workers
Encrypted %u file(s)
Start Encrypt
[Handle %u]
File Encrypted Successful
Encrypt Mode - FAST
Encrypt Mode - FULL
Terminating Processes
```

```
Deleting Shadow Copies
Uninstalling Services
Emptying Recycle Bin
This is a Russian-Speaking System, Exit
System Language Check
Start Encrypting All Files
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77
6F7079207C20466F72456163682D4F626A656374207B245F2E44656C65746528293B7D20'.Substring(2
*$_,2))};iex $s"
root/cimv2
WQL
SELECT * FROM Win32_ShadowCopy
ID
Win32_ShadowCopy.ID='%s'
.exe
LOG%s.TXT
README%s.TXT
Software\Classes\exefile\shell\open\command
\slui.exe
runas
Elevation:Administrator!new:
{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
explorer.exe
```

Figure 19: Decrypted strings

Appendix B: Indicators for Detection and Hunting

Yara Detections

The following YARA rules are not intended to be used on production systems or to inform blocking rules without first being validated through an organization's own internal testing processes to ensure appropriate performance and limit the risk of false positives. These rules are intended to serve as a starting point for hunting efforts to identify related activity; however, they may need adjustment over time if the malware family changes.

```
 rule Ransomware_Win_DARKSIDE_v1__1
{
    meta:
        author = “FireEye”
        date_created = “2021-03-22”
        description = “Detection for early versions of DARKSIDE ransomware samples based on the encryption mode
        md5 = “1a700f845849e573ab3148daef1a3b0b”
    strings:
        $consts = { 80 3D [4] 01 [1-10] 03 00 00 00 [1-10] 03 00 00 00 [1-10] 00 00 04 00 [1-10] 00 00 00 00 [1-
    condition:
```

```
        (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and $consts
}
```

Figure 20: DARKSIDE YARA rule

```
 rule Dropper_Win_Darkside_1
{
    meta:
        author = "FireEye"
        date_created = "2021-05-11"
        description = "Detection for on the binary that was used as the dropper leading to DARKSIDE."
    strings:
        $CommonDLLs1 = "KERNEL32.dll" fullword
        $CommonDLLs2 = "USER32.dll" fullword
        $CommonDLLs3 = "ADVAPI32.dll" fullword
        $CommonDLLs4 = "ole32.dll" fullword
        $KeyString1 = { 74 79 70 65 3D 22 77 69 6E 33 32 22 20 6E 61 6D 65 3D 22 4D 69 63 72 6F 73 6F 66 74 2E 5
        $KeyString2 = { 74 79 70 65 3D 22 77 69 6E 33 32 22 20 6E 61 6D 65 3D 22 4D 69 63 72 6F 73 6F 66 74 2E 5
        $Slashes = { 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C 7C }
    condition:
        filesize < 2MB and filesize > 500KB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and (
}
```

Figure 21: DARKSIDE Dropper YARA rule

```
 rule Backdoor_Win_C3_1
{
    meta:
        author = “FireEye”
        date_created = "2021-05-11"
        description = "Detection to identify the Custom Command and Control (C3) binaries."
        md5 = "7cdac4b82a7573ae825e5edb48f80be5"
    strings:
        $dropboxAPI = "Dropbox-API-Arg"
        $knownDLLs1 = "WINHTTP.dll" fullword
        $knownDLLs2 = "SHLWAPI.dll" fullword
        $knownDLLs3 = "NETAPI32.dll" fullword
        $knownDLLs4 = "ODBC32.dll" fullword
        $tokenString1 = { 5B 78 5D 20 65 72 72 6F 72 20 73 65 74 74 69 6E 67 20 74 6F 6B 65 6E }
        $tokenString2 = { 5B 78 5D 20 65 72 72 6F 72 20 63 72 65 61 74 69 6E 67 20 54 6F 6B 65 6E }
        $tokenString3 = { 5B 78 5D 20 65 72 72 6F 72 20 64 75 70 6C 69 63 61 74 69 6E 67 20 74 6F 6B 65 6E }
    condition:
        filesize < 5MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and (((all of ($knownDLLs*
```

Figure 22: Custom Command and Control (C3) YARA rule

Detecting DARKSIDE

FireEye products detect this activity at multiple stages of the attack lifecycle. The following table contains specific detections intended to identify and prevent malware and methods seen at these intrusions. For brevity, this list does not include FireEye's existing detections for BEACON, BloodHound/SharpHound, and other common tools and malware that FireEye has observed both in this campaign and across a broad range of intrusion operations

Platform(s)	**Detection Name**
Network SecurityEmail SecurityDetection On DemandMalware AnalysisFile Protect	• Ransomware.SSL.DarkSide • Trojan.Generic • Ransomware.Linux.DARKSIDE • Ransomware.Win.Generic.MVX • Ransomware.Win.DARKSIDE.MVX • Ransomware.Linux.DARKSIDE.MVX • Ransomware.Win32.DarkSide.FEC3 • FE_Ransomware_Win_DARKSIDE_1 • FE_Ransomware_Win32_DARKSIDE_1 • FE_Ransomware_Linux64_DARKSIDE_1 • FE_Ransomware_Linux_DARKSIDE_1 • FEC_Trojan_Win32_Generic_62 • FE_Loader_Win32_Generic_177 • FE_Loader_Win32_Generic_197 • FE_Backdoor_Win_C3_1 • FE_Backdoor_Win32_C3_1 • FE_Backdoor_Win32_C3_2 • FE_Backdoor_Win_C3_2 • Backdoor.Win.C3 • FE_Dropper_Win_Darkside_1
Endpoint Security	**Real-Time (IOC)** • BABYMETAL (BACKDOOR) • DARKSIDE RANSOMWARE (FAMILY) • SUSPICIOUS POWERSHELL USAGE (METHODOLOGY) • SUSPICIOUS POWERSHELL USAGE B (METHODOLOGY) **Malware Protection(AV/MG)** • Generic.mg.*

	• Gen:Heur.FKP.17 • Gen:Heur.Ransom.RTH.1 • Gen:Trojan.Heur.PT.omZ@bSEA3vk • Gen:Variant.Razy.* • Trojan.CobaltStrike.CB • Trojan.GenericKD.* • Trojan.Linux.Ransom.H **UAC Protect** • Malicious UAC bypass program detected
Helix	• VPN ANALYTICS [Abnormal Logon] • WINDOWS ANALYTICS [Abnormal RDP Logon] • TEAMVIEWER CLIENT [User-Agent] • WINDOWS METHODOLOGY [Plink Reverse Tunnel] • WINDOWS METHODOLOGY - SERVICES [PsExec]

Mandiant Security Validation Actions

Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID	Title
A101-700	Malicious File Transfer - DARKSIDE, Download, Variant #2
A101-701	Malicious File Transfer - DARKSIDE, Download, Variant #3
A101-702	Malicious File Transfer - DARKSIDE, Download, Variant #4
A101-703	Malicious File Transfer - DARKSIDE, Download, Variant #5
A101-704	Malicious File Transfer - DARKSIDE, Download, Variant #6

A101-705	Malicious File Transfer - DARKSIDE, Download, Variant #7
A101-706	Malicious File Transfer - DARKSIDE, Download, Variant #8
A101-707	Malicious File Transfer - DARKSIDE, Download, Variant #9
A101-708	Malicious File Transfer - DARKSIDE, Download, Variant #10
A101-709	Malicious File Transfer - DARKSIDE, Download, Variant #11
A101-710	Malicious File Transfer - DARKSIDE, Download, Variant #12
A101-711	Malicious File Transfer - DARKSIDE, Download, Variant #13
A101-712	Malicious File Transfer - DARKSIDE, Download, Variant #14
A101-713	Malicious File Transfer - DARKSIDE, Download, Variant #15
A101-714	Malicious File Transfer - DARKSIDE, Download, Variant #16
A101-715	Malicious File Transfer - DARKSIDE, Download, Variant #17
A101-716	Malicious File Transfer - DARKSIDE, Download, Variant #18
A101-717	Malicious File Transfer - DARKSIDE, Download, Variant #19
A101-718	Malicious File Transfer - DARKSIDE, Download, Variant #20
A101-719	Malicious File Transfer - DARKSIDE, Download, Variant #21

A101-720	Malicious File Transfer - DARKSIDE, Download, Variant #22
A101-721	Malicious File Transfer - DARKSIDE, Download, Variant #23
A101-722	Malicious File Transfer - DARKSIDE, Download, Variant #24
A101-723	Malicious File Transfer - DARKSIDE, Download, Variant #25
A101-724	Malicious File Transfer - DARKSIDE, Download, Variant #26
A101-725	Malicious File Transfer - DARKSIDE, Download, Variant #27
A101-726	Malicious File Transfer - DARKSIDE, Download, Variant #28
A101-727	Malicious File Transfer - DARKSIDE, Download, Variant #29
A101-728	Malicious File Transfer - DARKSIDE, Download, Variant #30
A101-729	Malicious File Transfer - DARKSIDE, Download, Variant #31
A101-730	Malicious File Transfer - DARKSIDE, Download, Variant #32
A101-731	Malicious File Transfer - DARKSIDE, Download, Variant #33
A101-732	Malicious File Transfer - DARKSIDE, Download, Variant #34
A101-733	Malicious File Transfer - DARKSIDE, Download, Variant #35
A101-734	Malicious File Transfer - DARKSIDE, Download, Variant #36

A101-735	Malicious File Transfer - NGROK, Download, Variant #1
A101-736	Malicious File Transfer - UNC2465, LNK Downloader for SMOKEDHAM, Download
A101-737	Malicious File Transfer - BEACON, Download, Variant #3
A101-738	Data Exfiltration - RCLONE, Exfil Over SFTP
A101-739	Malicious File Transfer - RCLONE, Download, Variant #2
A101-740	Command and Control - DARKSIDE, DNS Query, Variant #1
A101-741	Command and Control - DARKSIDE, DNS Query, Variant #2
A101-742	Application Vulnerability - SonicWall, CVE-2021-20016, SQL Injection
A104-771	Protected Theater - DARKSIDE, PsExec Execution
A104-772	Host CLI - DARKSIDE, Windows Share Creation
A104-773	Protected Theater - DARKSIDE, Delete Volume Shadow Copy

Related Indicators

UNC2628

Indicator	**Description**
104.193.252[.]197:443	BEACON C2

162.244.81[.]253:443	BEACON C2
185.180.197[.]86:443	BEACON C2
athaliaoriginals[.]com	BEACON C2
lagrom[.]com	BEACON C2
ctxinit.azureedge[.]net	BEACON C2
45.77.64[.]111	Login Source
181ab725468cc1a8f28883a95034e17d	BEACON Sample

UNC2659

Indicator	Description
173.234.155[.]208	Login Source

UNC2465

Indicator	**Description**
81.91.177[.]54 :7234	Remote Access
koliz[.]xyz	File Hosting
los-web[.]xyz	EMPIRE C2

sol-doc[.]xyz	Malicious Infrastructure
hxxp://sol-doc[.]xyz/sol/ID-482875588	Downloader URL
6c9cda97d945ffb1b63fd6aabcb6e1a8	Downloader LNK
7c8553c74c135d6e91736291c8558ea8	VBS Launcher
27dc9d3bcffc80ff8f1776f39db5f0a4	Ngrok Utility

DARKSIDE Ransomware Encryptor

DARKSIDE Sample MD5
04fde4340cc79cd9e61340d4c1e8ddfb
0e178c4808213ce50c2540468ce409d3
0ed51a595631e9b4d60896ab5573332f
130220f4457b9795094a21482d5f104b
1a700f845849e573ab3148daef1a3b0b
1c33dc87c6fdb80725d732a5323341f9
222792d2e75782516d653d5cccfcf33b
29bcd459f5ddeeefad26fc098304e786

3fd9b0117a0e79191859630148dcdc6d
47a4420ad26f60bb6bba5645326fa963
4d419dc50e3e4824c096f298e0fa885a
5ff75d33080bb97a8e6b54875c221777
66ddb290df3d510a6001365c3a694de2
68ada5f6aa8e3c3969061e905ceb204c
69ec3d1368adbe75f3766fc88bc64afc
6a7fdab1c7f6c5a5482749be5c4bf1a4
84c1567969b86089cc33dccf41562bcd
885fc8fb590b899c1db7b42fe83dddc3
91e2807955c5004f13006ff795cb803c
9d418ecc0f3bf45029263b0944236884
9e779da82d86bcd4cc43ab29f929f73f
a3d964aaf642d626474f02ba3ae4f49b
b0fd45162c2219e14bdccab76f33946e

b278d7ec3681df16a541cf9e34d3b70a
b9d04060842f71d1a8f3444316dc1843
c2764be55336f83a59aa0f63a0b36732
c4f1a1b73e4af0fbb63af8ee89a5a7fe
c81dae5c67fb72a2c2f24b178aea50b7
c830512579b0e08f40bc1791fc10c582
cfcfb68901ffe513e9f0d76b17d02f96
d6634959e4f9b42dfc02b270324fa6d9
e44450150e8683a0addd5c686cd4d202
f75ba194742c978239da2892061ba1b4
f87a2e1c3d148a67eaeb696b1ab69133
f913d43ba0a9f921b1376b26cd30fa34
f9fc1a1a95d5723c140c2a8effc93722

Posted in

- Threat Intelligence
- Security & Identity
