New attack vectors for the DarkSide ransomware gang

Archived: 2026-04-05 16:37:52 UTC

Summary

- Discovered in August 2020
- Targets only English-speaking countries, avoiding the former Soviet countries
- Does not attack hospitals, hospices, schools, universities, non-profit organizations, or government institutions
- Uses Salsa20 with custom matrix and RSA-1024 encryption algorithms
- Ransom demands range from $200,000 to $2,000,000
- Caused shutdown of the Colonial Pipeline — the largest fuel pipeline in the U.S.
- Uses Silent Night botnet (Zloader backdoor) for delivery
- Attackers have exploited Palo Alto's CVE-2019-1579 and Microsoft Exchange vulnerabilities to breach a target environment

Attack vectors and targets

DarkSide ransomware recently attacked the Colonial Pipeline — the largest pipeline in the United States, used to transfer fuel from New York to Texas. According to a recent Bloomberg publication, Colonial Pipeline Co. paid the demanded $5 million ransom with cryptocurrency. However, they faced a performance issue — DarkSide ransomware, despite using a fast Salsa20 file encryption algorithm, has a slow file encryption/decryption procedure. As a result, the company continued using their own backups to hasten the restoration of pipeline operations.

DarkSide stands out from other ransomware as a service (RaaS) threats, as one of the attack vectors is based on the Zloader botnet (also known as "Silent Night") which played a key role in DarkSide's success.

Zloader is a variant of the Zeus financial malware that has been targeting banks since 2006. After a short break, its activity resumed in January 2020. Since then, the botnet's affiliates have carried out a series of attacks on the United States, Canada, Germany, and Poland. Zloader is a first-stage Trojan loader that infects the victim's peripheral domain. Once a foothold is established, the Cobalt Strike red teaming tool is used to spread and deploy DarkSide ransomware.

In some cases, DarkSide ransomware has also been delivered through compromised third-party service providers. In others, the CVE-2019-1579 vulnerability in Palo Alto's GlobalProtect portal and GlobalProtect Gateway interface products and Microsoft Exchange server exposure were used. As a result of exploitation, an unauthenticated attacker could execute malicious code remotely (RCE).

Configuration

As DarkSide employs an RaaS model, the configuration data is embedded in the binary built for a specific affiliate. To hide these settings from analysis, the configuration data is compressed with a PLib.

At the very start of its execution, immediately after loading libraries, the ransomware locates its configuration by searching for the terminating hex string “0xDEADBEEF”. In the past, this string was usually used to mark deallocated memory.

After that, the configuration is decoded.

This configuration defines which particular features are enabled in this ransomware sample by an affiliate. The ransomware configuration includes the following parameters:

- **Victim’s ID** — used for encrypted file extension, in README.[Victim's ID].TXT, and to access the decryption service in Tor.
- **Encryption mode** – can be chosen from one of the following values:
  o ‘1’: ‘FULL’
  o ‘2’: ‘FAST’
  o Any other values: ‘AUTO’
- **Flags** — enable/disable the following features (all flags are set to ‘yes’ in the analyzed sample)
  o Encrypt local disks
  o Encrypt network shares
  o Perform language check
  o Delete volume shadow copies
  o Empty Recycle Bin
  o Self-delete
  o Perform UAC bypass if necessary
  o Adjust token privileges
  o Logging
  o Ignore specific folders
  o Ignore specific files
  o Ignore specific file extensions
  o Terminate processes
  o Stop services
  o Drop ransom note
  o Create a mutex
- **Folders to skip.** For example: "$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."
- **Files to skip**. For example: "autorun.inf, boot.ini, bootfont.bin, bootsect.bak, desktop.ini, iconcache.db, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini, thumbs.db."
- **Extensions to skip**. For example: "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."

- **Folders to delete**. For example: "backup."
- **Processes to skip** when terminating.
- **Processes to terminate** to unlock files.
- **C&C URLs**
- **Services to stop**
- **Wallpaper message** directing victims to the ransom note
- **Ransom note**

The latest version of DarkSide attempts to stop the same list of backup and anti-malware services as previous versions targeted:

vss
sql
svc$
memtas
mepocs
sophos
veeam
backup
GxVss
GxBlr
GxFWD
GxCVD
GxCIMgr

DarkSide kills processes that contain the following strings in their names to unlock the files:

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

DarkSide doesn't touch the following processes to prevent their accidental termination, which may lead to system crash or the disconnection of a remote session:

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

These lists have been not changed since the previous analyzed version of DarkSide.

File encryption

No changes here since our last analysis. DarkSide ransomware still uses Salsa20 for file encryption and RSA1024 for file keys encryption.

C&C communication

The analyzed DarkSide sample has a C&C connection flag enabled in the configuration. It connects to the following domains, sending a check-in request and providing information that will be used to uniquely identify an infected computer:

- securebestapp20.com
- temisleyes.com

Ransom note

The string from the configuration is used to generate the following wallpaper:

The ransom note template hasn’t changed since our last analysis.

Detection by Acronis

Acronis’ Active Protection technology uses machine intelligence and behavioral analysis to successfully identify and stop DarkSide attacks — as well as any other known or unknown cyberthreats. Backups are protected against tampering, and enable the automatic and rapid restoration of any encrypted files.

Conclusion

Compared to previous variants, we haven’t found significant changes in the DarkSide ransomware code and configuration. However, DarkSide's new TTPs rely on exploitation of Palo Alto’s CVE-2019-1579 and Microsoft Exchange vulnerabilities as well as the Silent Night (Zloader) botnet in recent major attacks.

IoCs

SHA256: 151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5
securebestapp20.com
temisleyes.com
