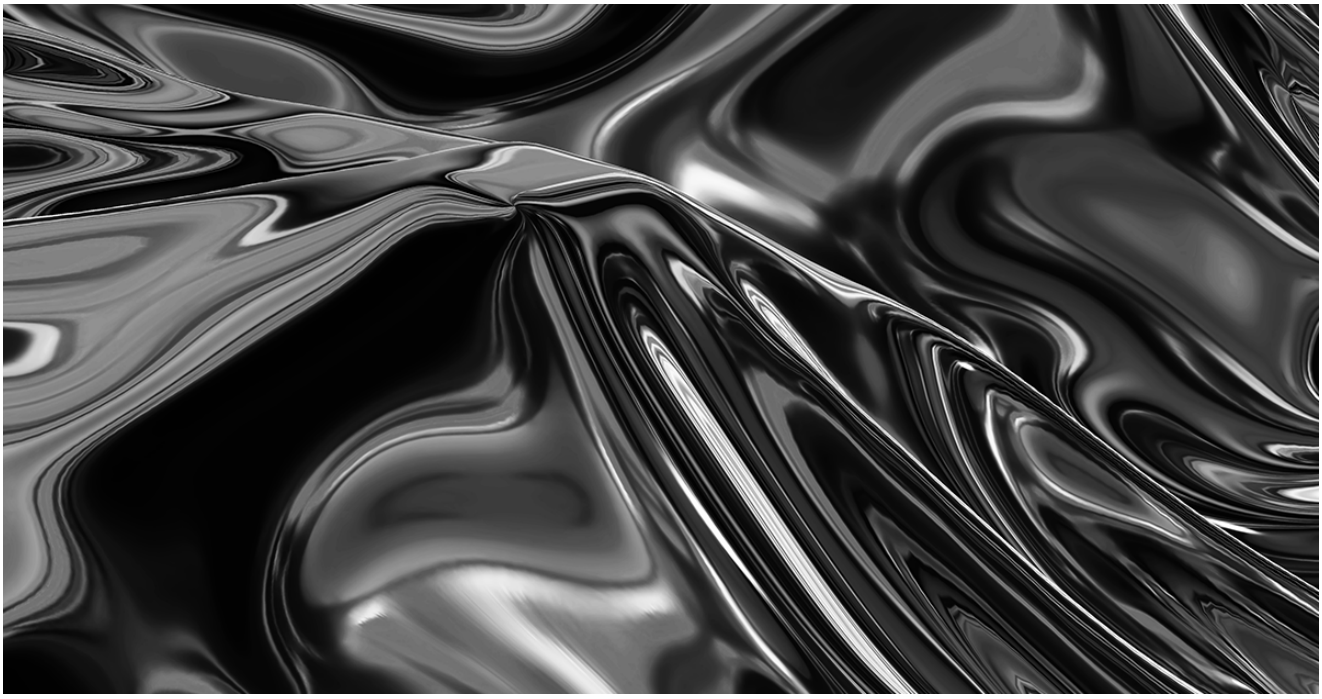
BlackMatter ransomware emerges from the shadow of DarkSide

news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/

Mark Loman August 9, 2021



On Friday May 7, 2021, an affiliate of the DarkSide Ransomware-as-a-Service (RaaS) hit Colonial Pipeline, a major U.S. fuel pipeline. The attack led to widespread supply disruption, global headlines, and intense scrutiny by the national authorities. A week later, DarkSide announced it was shutting down its operations after its servers were allegedly seized and its cryptocurrency wallets drained. DarkSide was followed into apparent retirement by another ransomware service, REvil, the threat actor behind the attack on Kaseya.

In late July, a new RaaS appeared on the scene. Calling itself BlackMatter, the ransomware claims to fill the void left by DarkSide and REvil – adopting the best tools and techniques from each of them, as well as from the still-active LockBit 2.0.

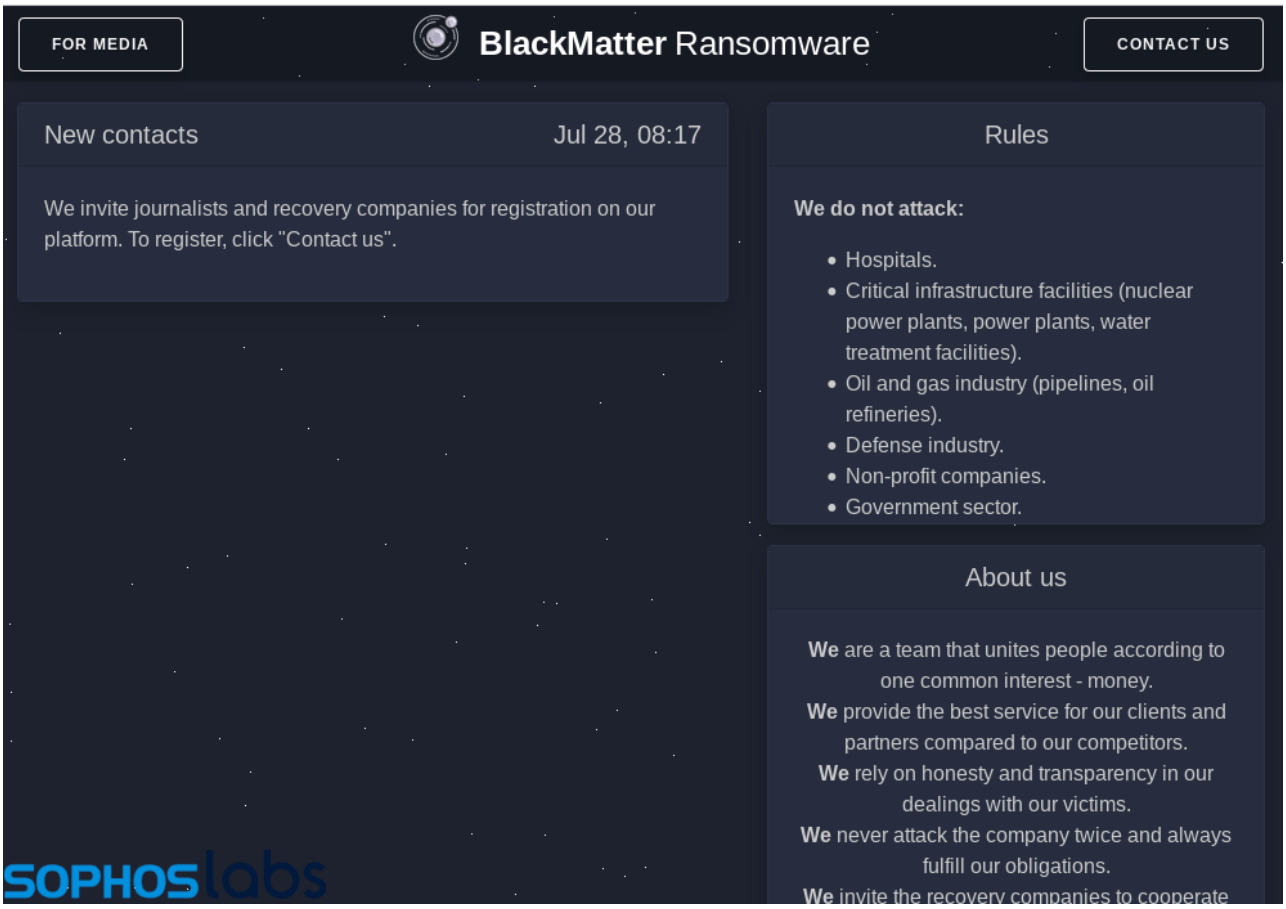
SophosLabs decided to take a closer look at the malware and the claims being made by the new adversary to see what's really going on.

Note: A Ransomware-as-a-Service (RaaS) comprises a core group of developers who maintain the ransomware and payment sites as well as recruited affiliates or "customers" who rent the ransomware, breach victims' networks and encrypt devices.

Malware analysis

The Sophos research is based on a sample of the BlackMatter ransomware, with the SHA-256 hash: 22D7D67C3AF10B1A37F277EBABE2D1EB4FD25AFBD6437D4377400E148BCC08D6.

The operators behind the BlackMatter RaaS have established a presence on the dark web:



The list of sectors and entities this threat actor says it will not attack reflect the recent global incidents involving DarkSide (Colonial Pipeline) and REvil (Kaseya) ransomware, which drew widespread and probably unwelcome attention.

The operators behind BlackMatter claim that their ransomware incorporates the best features of DarkSide, REvil, and LockBit 2.0 ransomware. They also say that while they are closely acquainted with the Darkside operators, they are not the same people.

To better understand the potential relationships between the ransomware groups, SophosLabs has analyzed a BlackMatter ransomware sample, and uncovered a number of technical similarities with DarkSide and the other ransomware families that are worth noting.

Below is a short comparison of some of the capabilities seen in the various groups:

Feature	REvil	Lockbit 2.0	DarkSide	BlackMatter
Type	RaaS	RaaS	RaaS	RaaS

Network first	–	Yes	No	No
Multi-threaded	Yes	Yes	Yes	Yes
File encryption	In-place	In-place	In-place	In-place
Encrypt size	Full	Partial, 4 KB	Partial, 512 KB	Partial, 1.024 KB
Rename	After	After	Before	Before
Decryption blob	End of File	End of File	End of File	End of File
Wallpaper	Yes	Yes	Yes	Yes
Encrypts Russian systems	No	Yes	No	Yes

Wallpaper

When victims are hit with the BlackMatter ransomware and the files on the drives are encrypted, BlackMatter sets a wallpaper that is very similar to DarkSide's. Also, like DarkSide, this is stored in the same folder on disk (C:\ProgramData), with an identical file size (2,818,366 bytes), image format (.BMP) and image size (1706 x 826 pixels, 16-bit color depth.)

Figure: BlackMatter resetting the desktop wallpaper to a ransom notice

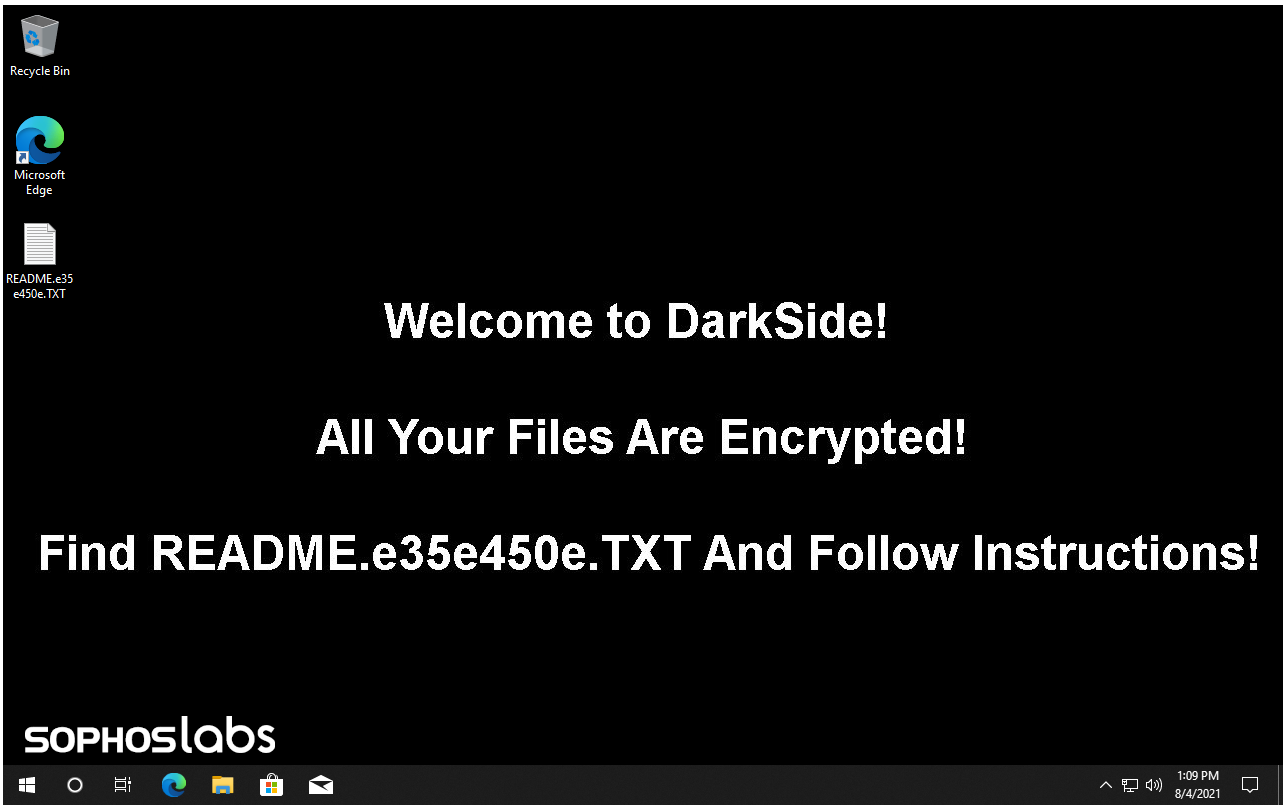


Figure: DarkSide resetting the desktop wallpaper to a ransom notice

Initial access brokers

Although DarkSide (and REvil) seem to have disappeared from the RaaS scene, we have detected an increase in LockBit 2.0 ransomware attacks. A recent ransom wallpaper set by LockBit contains an advertisement to recruit an initial access broker, possibly a corporate insider, to help them breach and encrypt networks for million-dollar payouts:

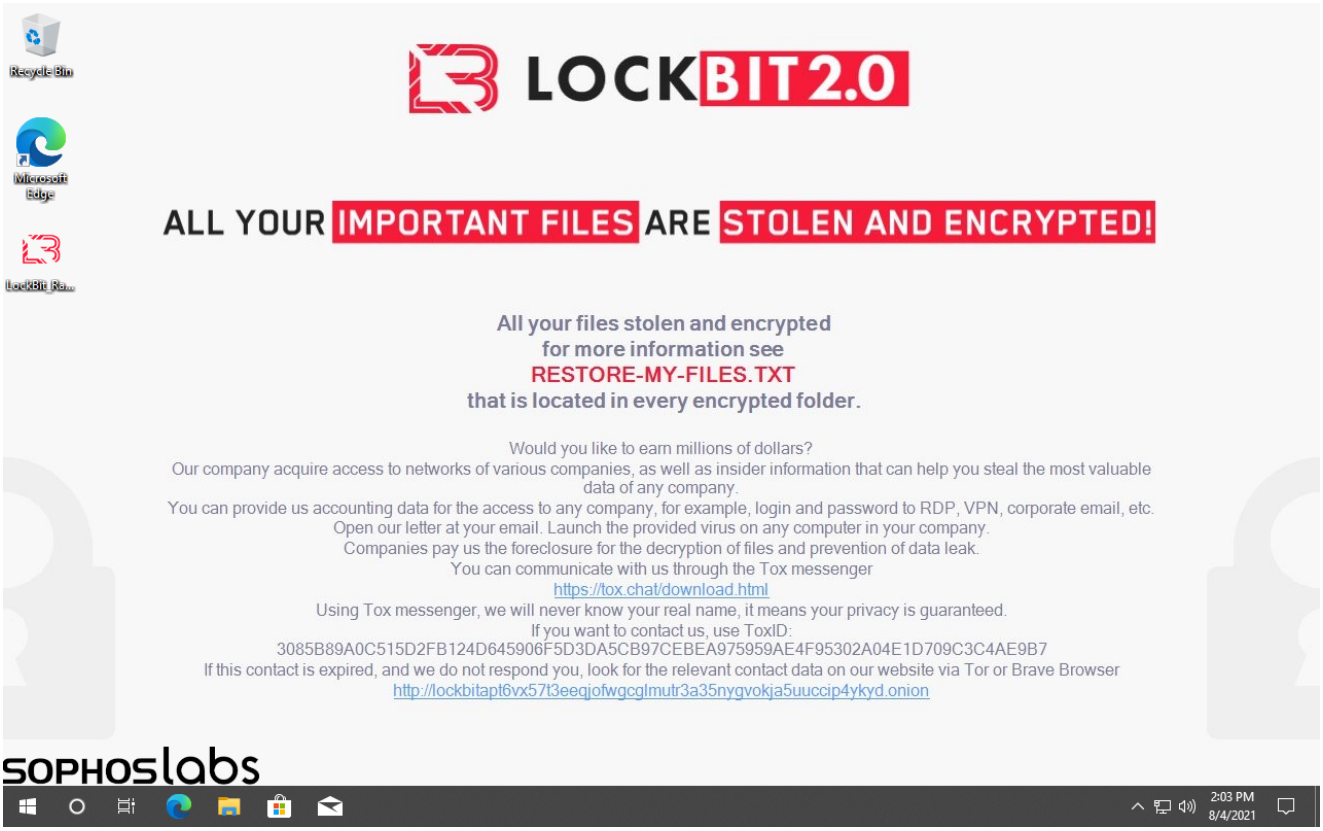


Figure: Lockbit 2.0 resetting the desktop wallpaper to a ransom notice with a recruitment ad

"Would you like to earn millions of dollars? Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger"

Competitive actors

Ransomware actors compete to attract the best criminal hackers (partners) to work for them. To appeal to potential recruits the groups want to show they have superior tools and techniques, for instance, by being able to lock data faster than others.

BlackMatter, DarkSide and LockBit 2.0 all employ a partial encryption scheme, which means they do not encrypt the entire file but only a portion. This has the same effect but significantly shortens the attack duration since only a fraction of a file is read and overwritten.

Depending on the protection software, being fast offers an advantage as it often takes a few seconds before protection initiates a memory scan and can determine that a malware is running in memory and the files are under attack. By then, many files may have already

become scrambled and inaccessible.

Knowing that solid-state drives (SSD) or M.2 NVMe storage can reach speeds of hundreds or thousands of megabytes per second (MB/s), you can imagine that attacking merely 1 MB of each file means hundreds of files can become encrypted in a second.

Multithreaded file system activity

In addition to partial encryption, most recent ransomware-as-a-service families make use of multithreading. This technology is available in CPUs since 2001 and increases the utilization of a processor core by using the complementary processes of thread-level parallelism and instruction-level parallelism.

This effectively leads to higher throughput and lower latency since data in a faster medium (such as memory) can be retrieved by one thread while another thread retrieves data from a slower medium (such as storage), with neither thread waiting for the other to finish.

During encryption, the BlackMatter ransomware's file system activity and use of multithreading looks the same as DarkSide's. The steps are very similar:

BlackMatter

Step	Thread	Operation	Purpose
1	A	CreateFile (Generic Read)	Open original document for reading only
2	A	ReadFile	Read last 132 bytes of original document (look for decryption blob)
3	A	ReadFile	Read last **1,051 bytes** of original document (look for decryption blob)
4	A	CloseFile	Close original document (no changes made)
5	A	CreateFile (Read Attributes)	Open original document
6	A	SetRenameInformationFile	Rename document by adding a file extension, for example .7xit0dGt6
7	A	CloseFile	Close now renamed original document
8	A	CreateFile (Generic Read/Write)	Open renamed original document for reading and writing

9	B	ReadFile	Read 1 MB of renamed original document
10	B	WriteFile	Write 1 MB of encrypted document in renamed original document
11	C	WriteFile (Offset: -1)	Add decryption blob, 132 bytes, to end of file
12	B	CloseFile	Close now encrypted file

Table: BlackMatter ransomware file system activity when it encrypts a document

DarkSide

Step	Thread	Operation	Purpose
1	A	CreateFile (Generic Read/Write)	Open original document for reading and writing
2	A	ReadFile	Read last 144 bytes of original document (look for decryption blob)
3	A	ReadFile	Read last **1,051 bytes** of original document (look for decryption blob)
4	A	CloseFile	Close original document (no changes made)
5	A	CreateFile (Read Attributes)	Open original document
6	A	SetRenameInformationFile	Rename document by adding a file extension, for example .e35e450e
7	A	CloseFile	Close now renamed original document
8	A	CreateFile (Generic Read/Write)	Open renamed original document for reading and writing
9	B	ReadFile	Read 0.5 MB of renamed original document in blocks of 64 KB
10	B	WriteFile	Write 0.5 MB of encrypted document in renamed original document in blocks of 64 KB
11	C	WriteFile (Offset: -1)	Add decryption blob, 144 bytes, to end of file
12	B	CloseFile	Close now encrypted file

Table: DarkSide ransomware file system activity when it encrypts a document

Decryption blob

Ransomware stores a decryption blob in or alongside encrypted files. This blob is essential for the decryption tool that the adversary provides to restore files after a target has paid the ransom.

This blob of data is usually appended to the end of the file but can be prepended or stored in one or more separate files, depending on the ransomware family. BlackMatter, DarkSide, REvil and LockBit all add the decryption blob at the end of the file – which is typical for most ransomware.

Granting access to “Everyone”

Unlike DarkSide, the BlackMatter ransomware takes ownership of a document before encrypting it by setting its discretionary access control list (DACL) to “Full” for group “Everyone” (via the SetSecurityFile function.) This makes the document accessible to every Windows user. Because of the malicious encryption that follows, this doesn’t immediately cause a breach of privacy. However, victims who pay the ransom demand will receive a decrypter from the attacker that cannot restore the original access permissions as this security information has been lost.

IT admins should therefore check and re-enforce proper permissions when recovering from a BlackMatter ransomware attack.

Deployment and abuse of “Safe Mode” like REvil

SophosLabs research into an attack involving BlackMatter ransomware revealed that once a BlackMatter operator gains access to a target’s network and is ready to deploy the ransomware, a scheduled task is set up that executes a PowerShell script on a domain-accessible UNC path on a server, e.g., a domain controller.

The ransomware binary itself is base64 encoded and embedded inside the PowerShell script. Although the PowerShell script has support to decode and reflectively load the ransomware binary straight into memory (like some REvil ransomware attacks), the binary can also be dropped to disk.

In the presence of robust endpoint protection software, the attacker can opt to use BlackMatter’s Safe Mode capability. Via the **-safe** command-line switch, the BlackMatter ransomware can restart Windows into a diagnostic mode known as Safe Mode, where endpoint protection is typically not active, and perform the entire encryption attack there. These are the steps:

- Enable the Windows built-in local **Administrator** account, which is normally disabled by default
- Create the **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon** registry key and set it to **1**
- Create the **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName** registry key and set it to **Administrator**
- Create the **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultDomainName** registry key and set it to local hostname
- Create an entry under the **HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce** registry key, using a random string starting with an asterisk, like ***VHJ544uhjC**, and set its value to the full path of the ransomware executable
- Change the default boot configuration to safe mode with networking, by running this command: **bcdedit /set {current} safeboot network**

The ransomware then forces the machine to restart and Windows automatically boots into "Safe Mode with Networking," where the ransomware can encrypt the files on the machine without being disrupted by endpoint protection software. The local account **Administrator** is automatically logged in and the ransomware runs automatically. When the ransomware has finished encrypting, it runs the following command to make sure that, going forward, the machine boots into normal mode: **bcdedit /deletevalue {current} safeboot**. The machine is restarted, although the abused Administrator account remains automatically logged in.

These steps are almost identical to those seen in a ransomware attack involving REvil ransomware, which provided Safe Mode support via the **-smode** command-line switch.

Privilege elevation

Like REvil, LockBit 2.0 and DarkSide, BlackMatter also attempts to elevate its privileges when it is limited by User Account Control (UAC). It does so via an elevated COM interface, by executing a function with this object name: **Elevation:Administrator!new:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}**
The same elevation trick is used by DarkSide and LockBit 2.0.

String encryption

Like DarkSide (and REvil), BlackMatter uses a run-time API that can hinder static analysis of the malware. And like the other two ransomware groups, strings are also encrypted and revealed during runtime. While both of these techniques are common across many recent malware, the way in which the runtime API and string decryption function in BlackMatter is very similar to the functionality seen in DarkSide and REvil.

```
int (__stdcall *sub_455E5C())(int, _DWORD, int)
{
  int (__stdcall *result)(int, _DWORD, int); // eax
  int v1; // esi
  int (__stdcall *v2)(int, _DWORD, int); // edi

  result = (int (__stdcall *)(int, _DWORD, int))getdll_viaPEB(0x260B0745);
  if ( result )
  {
    result = (int (__stdcall *)(int, _DWORD, int))result(0x40000, 0, 0);
    v1 = (int)result;
    if ( result )
    {
      result = (int (__stdcall *)(int, _DWORD, int))getdll_viaPEB(0x6E6047DB);
      v2 = result;
      if ( result )
      {
        getapi_byhash((int)&unk_4612AC, dword_455AFC, v1, result);
        getapi_byhash((int)&unk_461368, dword_455BBC, v1, v2);
        getapi_byhash((int)&unk_461428, dword_455C80, v1, v2);
        getapi_byhash((int)&unk_461480, dword_455CDC, v1, v2);
        getapi_byhash((int)&unk_4614B4, dword_455D14, v1, v2);
        getapi_byhash((int)&unk_4614EC, dword_455D50, v1, v2);
        getapi_byhash((int)&unk_4614FC, dword_455D64, v1, v2);
        getapi_byhash((int)&unk_461518, dword_455D84, v1, v2);
        getapi_byhash((int)&unk_461540, dword_455DB0, v1, v2);
        getapi_byhash((int)&unk_46154C, dword_455DC0, v1, v2);
        getapi_byhash((int)&unk_461554, dword_455DCC, v1, v2);
        getapi_byhash((int)&unk_461568, dword_455DE4, v1, v2);
        getapi_byhash((int)&unk_461594, dword_455E14, v1, v2);
        result = (int (__stdcall *)(int, _DWORD, int))getapi_byhash((int)&unk_4615A8, dword_455E2C, v1, v2);
      }
    }
  }
  return result;
}
```

Runtime API calls in BlackMatter

In another shared similarity with both REvil and Darkside, BlackMatter ransomware stores configuration information in the binary in an encoded format. SophosLabs decoded this and found that BlackMatter ransomware has a similar structure and information stored in the configuration blob, like lists of processes and services to kill, the ransom note, C2 details, directories to avoid etc.

Killing processes

The ransomware can encrypt open (locked) documents. BlackMatter terminates several productivity related processes before encryption begins:

- ensvc
- thebat
- mydesktopqos
- xfssvccon
- firefox
- infopath

- winword
- steam
- synctime
- notepad
- ocomm
- onenote
- mspub
- thunderbird
- agensvc
- sql
- excel
- powerpnt
- outlook
- wordpad
- dbeng50
- isqlplussvc
- sqbcoreservice
- oracle
- ocautoupds
- dbsnmp
- msaccess
- tbirdconfig
- ocssd
- mydesktopservice
- visio

List of processes terminated by BlackMatter

Stealing victim details

The BlackMatter ransomware collects information from victim machines, like hostname, logged in user, operating system, domain name, system type (architecture), language, as well as the size of the disk and available free space.

The analyzed sample sends these details to a remote server hosted on **paymenthacks.com**

It uses a specific header to post the information:

Omitting countries

Some ransomware attacks are set up to avoid hitting computers in certain countries. This is often a configurable option that RaaS affiliates can select for a specific campaign or target. It means that a protection approach based on installing, for example, an additional Cyrillic,

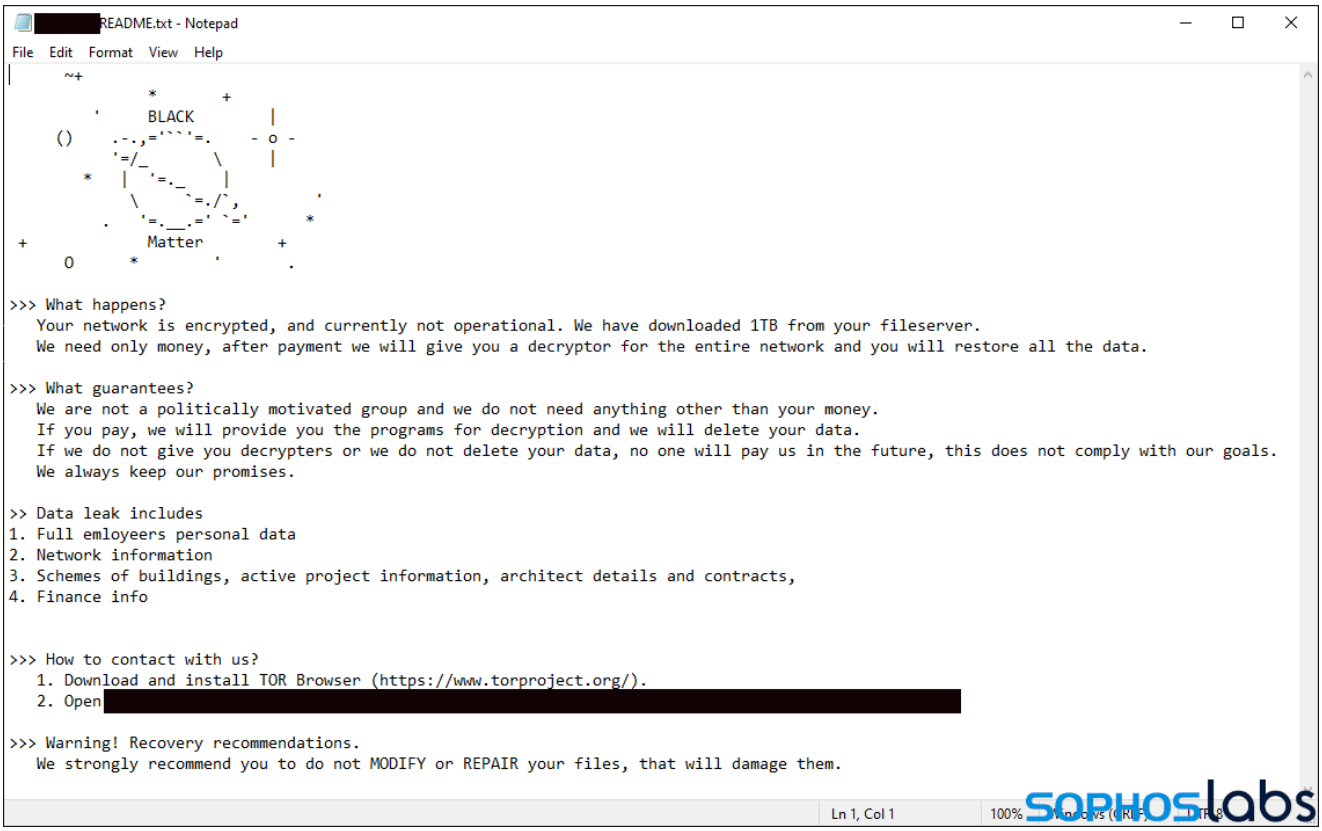
Russian or Ukrainian keyboard will not help.

DarkSide, for example, calls GetSystemDefaultUILanguage, which returns the language of the default user interface of the operating system, also known as the “install language” – which cannot be changed by the user.

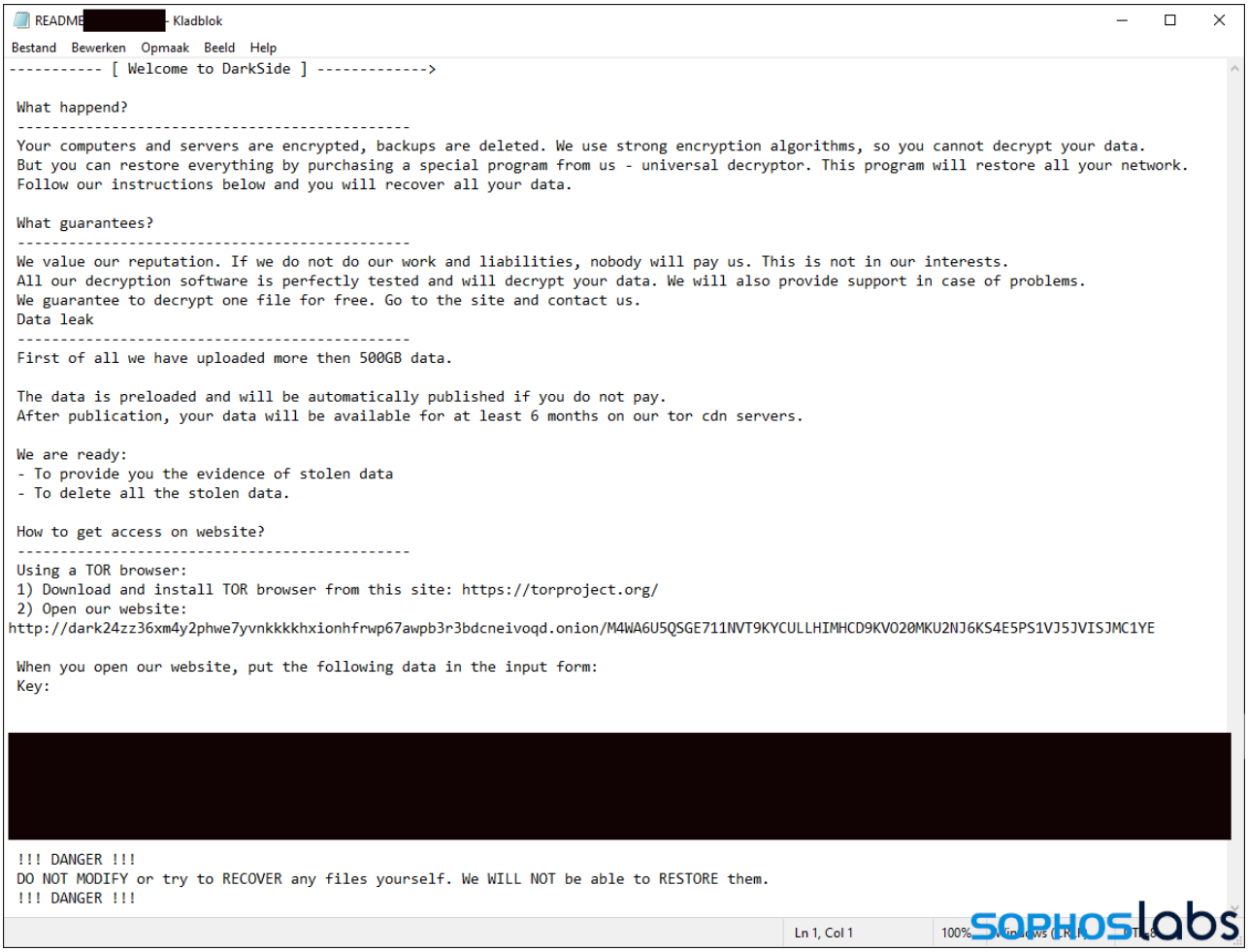
The analyzed BlackMatter sample encrypted our Russian machine whereas the DarkSide sample would not.

Ransom note

The BlackMatter ransomware drops a ransom note in user-accessible folders on the disk:



BlackMatter ransom note



DarkSide ransom note

The filename structure of DarkSide's ransom note is slightly different: the 'README' string is not behind but in front of the ransomware file extension. However, both notes first explain what happened and then talk about guarantees. DarkSide then goes on to claim to have stolen 500 gigabytes (GB) of data while BlackMatter mentions it has exfiltrated twice as much, 1 terabyte (TB).

In another recent sample we analyzed there is no mention of leaked data and the ransom note was tailored to the victim as it included the victim's company name. In addition, this sample sends a print job from each infected machine to the default printer, i.e., the ransom note is delivered on paper across the office. This can also be via printers at home – something we've also seen in recent LockBit 2.0 ransomware attacks.

DarkSide and BlackMatter: the same or just related?

There are a number of factors that suggest a connection between BlackMatter and DarkSide. However, this is not simply a rebranding from one to another. Malware analysis shows that while there are similarities with DarkSide ransomware, the code is not identical.

Summarizing our findings, the claims made recently by an alleged BlackMatter representative regarding its feature set are largely true.

In the hands of an experienced attacker, this ransomware can cause a lot of damage without triggering many alarms. It is important for defenders to promptly investigate endpoint protection alerts as they can be an indication of an imminent attack with disastrous consequences.

Note: Sophos Machine Learning automatically detects BlackMatter ransomware.

Acknowledgments

Sophos would also like to acknowledge SophosLabs researchers Anand Ajjan and Sean Gallagher, and Rapid Response manager Peter Mackenzie for their contributions to this report.