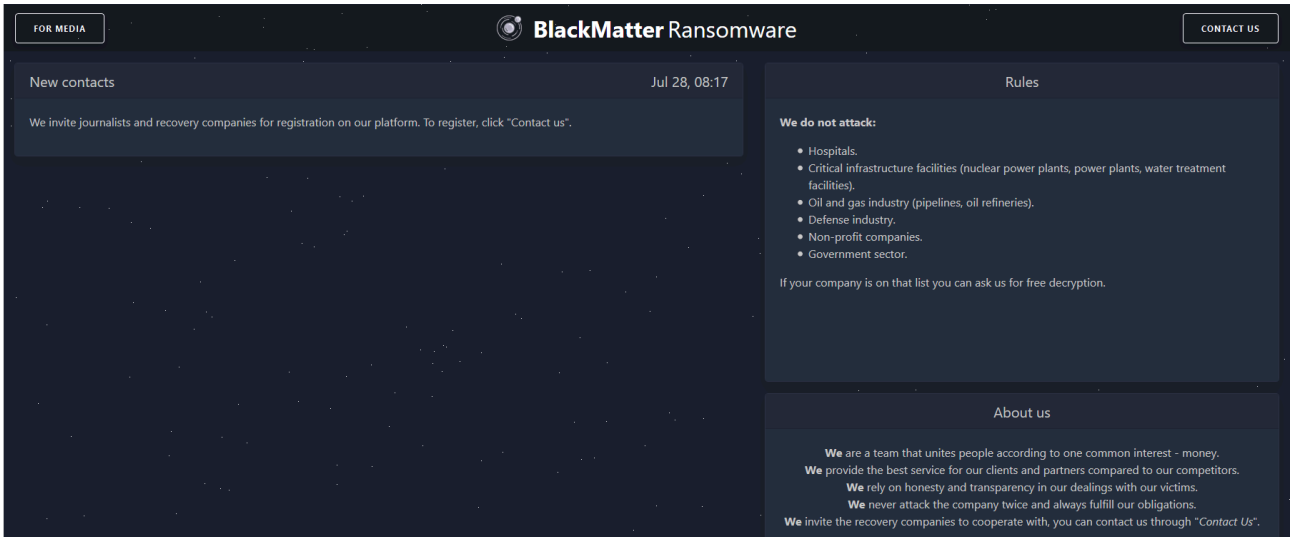
BlackMatter Ransomware: Story behind DarkSide strain | Group-IB Blog

Archived: 2026-05-05 02:42:35 UTC

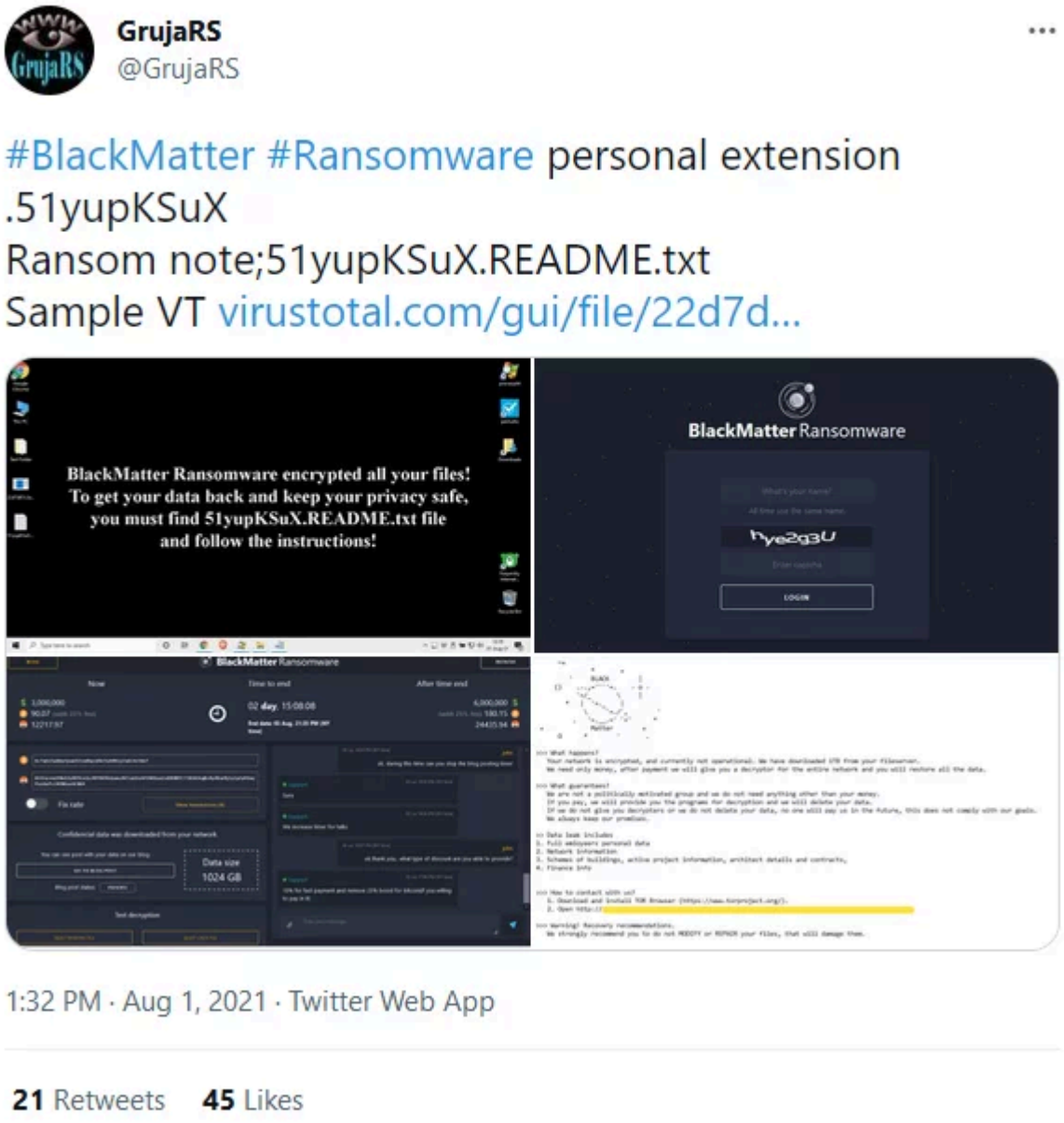
Summer 2021 brought hot weather, but also hot news from the world of ransomware. In late May, DoppelPaymer used a marketing trick and renamed its new ransomware Grief (Pay OR Grief). Moreover, in June-July the hacker groups DarkSide and REvil disappeared from the radars after the notorious attacks against Colonial Pipeline and Kaseya, respectively. By the end of July, a new player called BlackMatter had entered the ransomware market. Is BlackMatter really new on the scene, however?

Meet BlackMatter

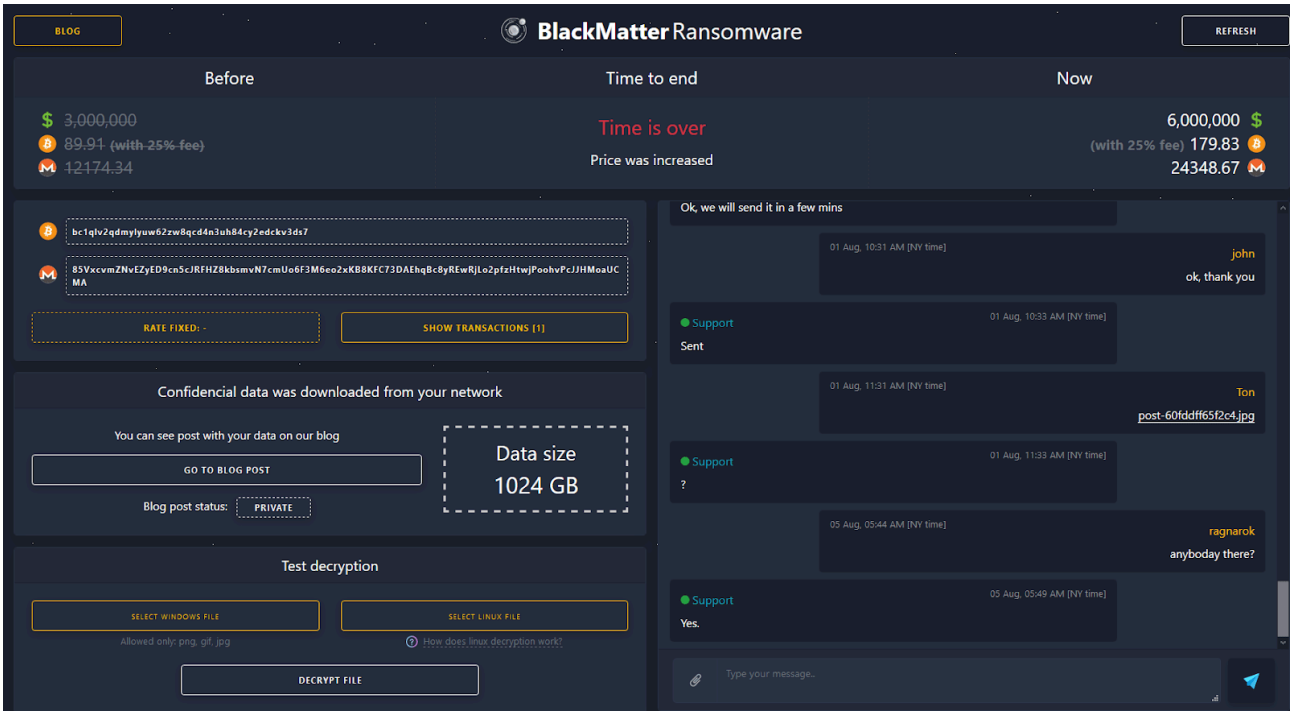
According to information on the hackers' website, the group has been active since July 28, 2021. Here's what they say about themselves:



The first victim of BlackMatter was an architecture company in the United States. When communicating with the victim, the hackers were tough and uncompromising.



They increased the ransomware demand after the ultimatum time was over.



We got our hands on a sample of BlackMatter for Windows that was used to attack the architecture company. In general, the BlackMatter group has developed ransomware not only for Windows but for Linux as well, which made it possible for the threat actors to attack Linux-based servers, including ESXi.

BlackMatter ransomware, the successor of DarkSide?

As soon as we started analyzing **the BlackMatter sample**, we experienced a feeling of déjà vu. We had already seen this: the conceptual approach to obfuscation, encrypted configuration data located in a special section, string encryption and obfuscation of API calls… Of course! REvil and DarkSide had used the same set of obfuscation techniques. The techniques were implemented in a different manner, however.

To avoid unnecessary comparisons, we can go as far as to say that the differences were drastic. Despite their small size, BlackMatter, REvil, and DarkSide programs are relatively functional and have very fast multithreaded file encryption mechanisms involving the I/O (input/output) completion port. Nothing extra — just business. It is obvious that **the ransomware samples that we obtained were developed by highly qualified programmers** with an in-depth knowledge of system programming under Windows.

Further analysis of the sample showed that **both BlackMatter and DarkSide use the Salsa20 algorithm to encrypt the victim's files and the RSA-1024 public key for the keys generated for each file**. A comparative analysis of the encryption code implementation with the Darkside samples also revealed that they are very similar.

It should be pointed out that, in March, the people behind REvil started using a political agenda in their programs. For example, REvil samples contained the following registry key: "*SOFTWARE\BlackLivesMatter*". The last daring attacks performed by DarkSide and REvil infuriated "the deities", and the hacker groups were punished by the thunderers and "banished to Tartarus". The question that interested everyone, from the cybersecurity community to the media, was: "For how long?" and "And what will they bring with them when they return?"

Here are the answers. A new project with the provocative name "BlackMatter", which had a lot in common with its predecessors, appeared on the scene two weeks after REvil's websites were shut down. **The new malware already has one victim, and it can be considered a starting point for BlackMatter.**

Results of the BlackMatter sample analysis

In the BlackMatter program analyzed, the developers indicated the malware version as 1.2. It is obvious that there had been earlier versions that had been tested out. It should be noted that **BlackMatter malware does not initiate checks** that identify whether the victim belongs to a CIS country, as had been the case with REvil and DarkSide. It is no wonder that the designers of BlackMatter do not want to be associated with Russian-speaking criminal groups anymore.

When BlackMatter is launched, it verifies the rights of the current user and, if necessary, attempts to bypass the UAC (User Account Control) by elevating privileges using the ICMLuaUtil COM interface. In addition, if the corresponding flag is set in the configuration, when launched the malware attempts to authenticate using the accounts contained in the configuration data.

Depending on the command line parameters, the program can operate in five modes. We identified the values of the parameters by hash:

-path <PATH>- encrypts the specified object (directory, file, network resource).
-safe- registers in the RunOnce system registry autorun key and reboots in safe mode to encrypt files.
-wall- creates a BMP image with a message about file encryption and sets it as the desktop wallpaper.
<PATH> – encrypts the specified directory / file.

When other (or no) parameters are set, the malware encrypts files on the hard drive and on other available network resources. After completing the encryption, the program creates a BMP file with a message about encryption and

sets it as the desktop wallpaper.

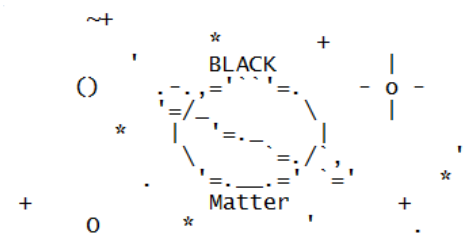
Before starting the encryption, BlackMatter deletes the shadow copies of the directories using request WQL (WMI Query Language).

As mentioned before, BlackMatter uses the most productive ways to implement the multithreaded mechanisms to encrypt files using the I/O (input/output) completion port. The program sets the highest priority for enumeration and encryption threads (*THREAD_PRIORITY_HIGHEST*). By default, files are encrypted only within the first megabyte. The data block with an encrypted key is added to the end of the file. The encrypted file names are as follows:

FILENAME: original file name;

VICTIM_ID: the victim's ID based on the string contained in the parameter MachineGuid of the registry directory *HKLM\SOFTWARE\Microsoft\Cryptography*.

In each processed directory, the ransomware creates text files containing a ransom demand:




```
>>> What happens?
   Your network is encrypted, and currently not operational. We have downloaded 1TB from your
fileserver.
   We need only money, after payment we will give you a decryptor for the entire network and
you will restore all the data.

>>> What guarantees?
   We are not a politically motivated group and we do not need anything other than your money.
   If you pay, we will provide you the programs for decryption and we will delete your data.
   If we do not give you decrypters or we do not delete your data, no one will pay us in the
future, this does not comply with our goals.
   We always keep our promises.

>> Data leak includes
1. Full emloyeers personal data
2. Network information
3. Schemes of buildings, active project information, architect details and contracts,
4. Finance info


>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open
http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/7NT6LXKC1XQHW5O39BLOV.

>>> Warning! Recovery recommendations.
   We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.
```

Directory names skipped during encryption

windows, system volume information, intel, $windows.~ws, application data, $recycle.bin, mozilla, program files (x86), program files, $windows.~bt, public, msocache, default, all users, tor browser, programdata, boot, config.msi, google, perflogs, appdata, windows.old

Names of excluded files

desktop.ini, autorun.inf, ntldr, bootsect.bak, thumbs.db, boot.ini, ntuser.dat, iconcache.db, bootfont.bin, ntuser.ini, ntuser.dat.log

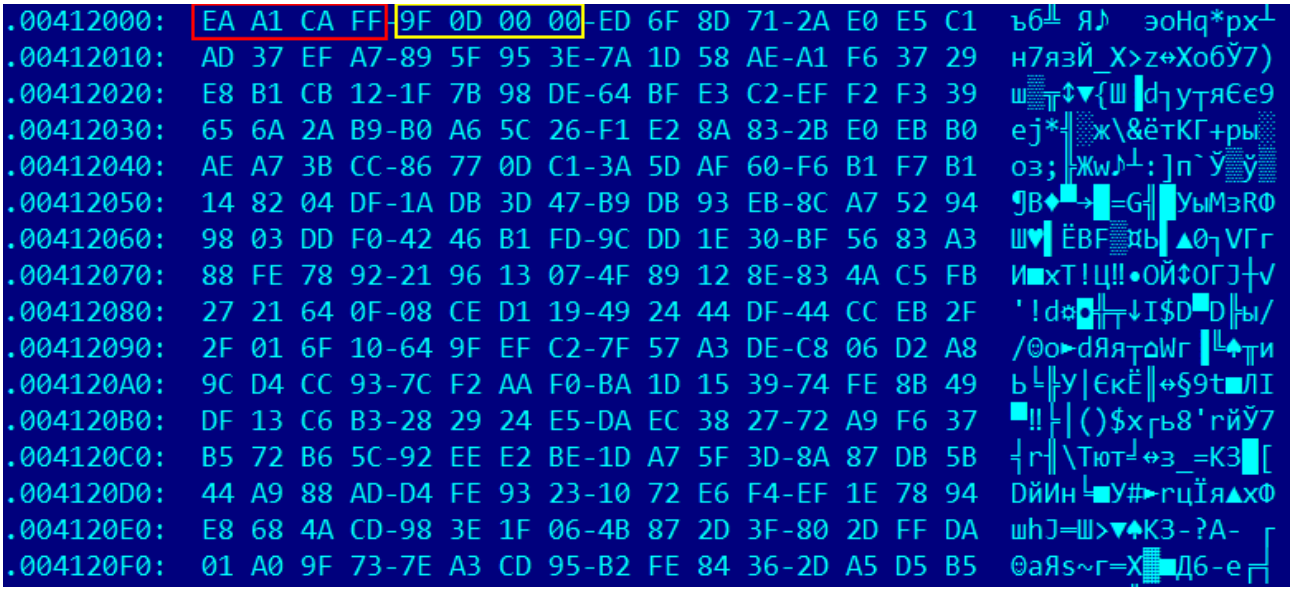
File extensions that are not encrypted by BlackMatter

themepack, nls, diagpkg, msi, lnk, exe, cab, scr, bat, drv, rtp, msp, prf, msc, ico, key, ocx, diagcab, diagcfg, pdb, wpx, hlp, icns, rom, dll, msstyles, mod, ps1, ics, hta, bin, cmd, ani, 386, lock, cur, idx, sys, com, deskthemepack, shs, ldf, theme, mpa, nomedia, spl, cpl, adv, icl, msu

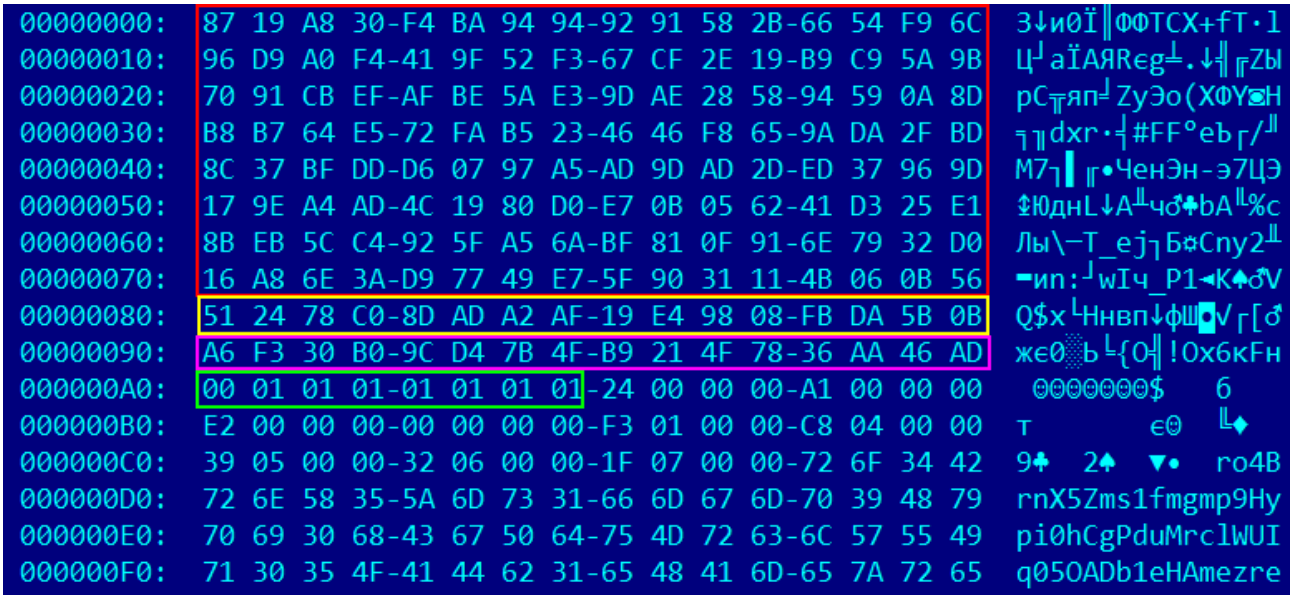
The list of exclusions is contained in the BlackMatter configuration in the form of hashes of corresponding strings. They are largely identical to the lists in DarkSide except for one exclusion. The content of the lists is clearly not a coincidence.

Configuration

BlackMatter configuration data is contained in the section disguised as the resource "*.rsrc*", yet there are no resources in the program.



The first 32-bit value (0FFCAA1EAh) in the section represents the seed for the pseudorandom number generator (random seed) used to encrypt the program data. The second 32-bit value represents the actual size of the configuration data that follows. Before encryption, the configuration data is pre-compressed using a compression algorithm aPLib, which is very popular among ransomware developers. The algorithm has already been detected in ransomware belonging to DarkSide, DoppelPaymer, Clop, and other families.



The decrypted and unpacked configuration data uses a public key called RSA-1024, an identifier named “bot_company” by the designers, and the key AES-128 ECB to encrypt data sent to attackers.

This is followed by 8 logical flags, which define the ransomware configuration (the value set in the sample is presented in parentheses):

- Encrypting odd megabytes in large files starting with the first one (0);
- Applying authentication attempts using the following credentials contained in the configuration (1):
  - aheisler@hhcp.com:120Heisler
  - dsmith@hhcp.com:Tesla2019
  - administrator@hhcp.com:iteam8**
- Mounting volumes and encrypting files on them (1).
- Encrypting files on available network resources (1). While performing this operation, the program also enumerates Active Directory using LDAP requests.
- Terminating processes that contain the following substrings in their names (1):
  - encsvc, thebat, mydesktopqos, xfssvccon, firefox, infopath,winword, steam, synctime, notepad, ocomm, onenote, mspub, thunderbird, agntsvc, sql, excel, powerpnt, outlook, wordpad, dbeng50, isqlplussvc, sqbcoreservice, oracle, ocautoupds, dbsnmp, msaccess, tbirdconfig, ocssd, mydesktopservice, visio
- Stopping and deleting services (1):
  - mepocs, memtas, veeam, svc$, backup, sql, vss
- Creating and checking the mutex (1):
  - Global\<MUTEX_NAME>
  - MUTEX_NAME: name of the mutex, formed based on the string from the registry parameter MachineGuid.
- Transferring information about compromised system and encryption results to threat actors (1). Encrypted information (AES-128 ECB) is transferred as HTTP POST requests to one of the following addresses:
  - https://paymenthacks[.]com
  - http://paymenthacks[.]com

- https://mojobiden[.]com
- http://mojobiden[.]com

The rest of the configuration data is contained as Base64 strings. The strings have a list of hashes of the bypassed directory/file names and file extensions, a list of substrings in the names of the terminated processes, names of services to be removed, links to attackers' resources used for transferring credentials, an encrypted list of credentials used for authentication attempts, and an encrypted text with ransomware demands.

Obfuscation

To compare the strings in the program, the hashes are used to hide the used strings and complicate any attempts to analyze the malware. It has already been mentioned that excluded names and directories, as well as file extensions, are verified by comparing the string hashes. Command line parameters are also identified by hash.

```
BOOL __stdcall CheckDirName(LPCWSTR pszDirName)
{
  int hash; // ebx
  int *pHash; // esi
  int hash2; // eax
  BOOL res; // [esp+8h] [ebp-4h]

  res = FALSE;
  if ( g_pDirHashes )
  {
    hash = get_wide_str_hash(pszDirName, 0);
    pHash = (int *)g_pDirHashes;
    while ( TRUE )
    {
      hash2 = *pHash++;
      if ( !hash2 )
        break;
      if ( hash == hash2 || hash == 0xE3426CD7 )// L"windows"
        return TRUE;
    }
  }
  return res;
}
```

The program uses two functions for calculating the hash: for Unicode strings and ANSI strings, respectively.

```
; DWORD __stdcall get_wide_str_hash(LPCWSTR s, DWORD hash)
get_wide_str_hash proc near             ; CODE XREF: resolve_api_func+89↓p
                                        ; sub_405928+11B↓p ...

s               = dword ptr  8
hash            = dword ptr  0Ch

                push    ebp
                mov     ebp, esp
                push    edx
                push    esi
                xor     eax, eax
                mov     edx, [ebp+hash]
                mov     esi, [ebp+s]

loc_4010C8:                             ; CODE XREF: get_wide_str_hash+2C↓j
                lodsw
                cmp     ax, 41h ; 'A'
                jb      short loc_4010DA
                cmp     ax, 5Ah ; 'Z'
                ja      short loc_4010DA
                or      ax, 20h

loc_4010DA:                             ; CODE XREF: get_wide_str_hash+13↑j
                                        ; get_wide_str_hash+19↑j
                add     dh, 61h ; 'a'
                sub     dh, 61h ; 'a'
                ror     edx, 0Dh
                add     edx, eax
                test    eax, eax
                jnz     short loc_4010C8
                mov     eax, edx
                pop     esi
                pop     edx
                pop     ebp
                retn    8
get_wide_str_hash endp
```

As can be seen, the function for Unicode strings uses lowercase Latin letters to calculate the hash. The function for ANSI string uses the same calculation algorithm, but it is case sensitive.

The functions are similar to those used in Metasploit/Cobalt Strike.

They are also used to obfuscate calls to API functions. A common hash on behalf of the DLL and the function name are used to identify API functions. To obtain the addresses of the API functions required for the program, the DLL (Dynamic Link Library) and the functions exported by them are enumerated via PEB (Process Environment Block). If the hash matches the one specified in the program code, the address of the function found is retrieved and stored in the table. In such cases, the system does not save the function's direct address, but the address to the allocated memory block with the following code allowing for additional obfuscation of the API function call:

- mov eax, <ENC_FUNC_ADDR>
- xor eax, 22065FEDh
- jmp eax

ENC_FUNC_ADDR is the result of modulo 2 addition (XOR) of the received API function address and the value 22065FEDh. This way of calling a function masks its actual address and makes it more complicated to analyze the program.

The configuration data, strings and data in the data section are encrypted using a pseudo-random sequence of 32-bit values and XORing these values. The initial value of the generator (random seed) 0FFCAA1EAh is contained at the beginning of the configuration data.

Strings and data generated in the stack, as well as the program version number and some hashes of strings in the program, are encrypted using a circular XOR operation with a 32-bit value 022065FEDh.

While it operates, the program also uses an anti-debugging technique that hides threads from the debugger by carrying out an undocumented call to the function NtSetInformationThread with the parameter ThreadHideFromDebugger (11h).

Conclusion

The analysis revealed an obvious connection between BlackMatter and DarkSide and REvil samples, especially DarkSide.

Ransomware comparison: spot the difference

GROUP-IB

	BlackMatter	DarkSide	REvil
File encryption			
File encryption algorithm	Salsa20 custom matrix	Salsa20 custom matrix	Salsa20
Key encryption algorithm	RSA-1024	RSA-1024	Curve25519
Multithreaded encryption	I/O completion port	I/O completion port	I/O completion port
Skipping files / folders	file name list folder name list file extension list (configuration)	file name list folder name list file extension list (configuration)	file name list folder name list file extension list (configuration)
Large file encryption	Types: 0 – first megabyte; 1 – all odd megabytes (configuration)	Types: 1 – all data 2 – first megabyte Other value – all odd megabytes (configuration)	Types: 0 – all data; 1 – first megabyte; 2 – megabytes in a specified interval (configuration)
Encryption in Windows Safe Mode	optional (command line)	no	optional (command line)
Encrypting local disks	yes	optional (configuration)	optional (command line)
Encrypting network shares	optional (configuration)	optional (configuration)	optional (command line)
Mount volumes	optional (configuration)	yes	no
Notifying the user about encryption	Create Bitmap and set as Desktop wallpaper	Create Bitmap and set as Desktop wallpaper	Extract image and set as Desktop wallpaper (configuration)
Ransom note	<VICTIM_ID>.README.txt In every processed directory	README.<VICTIM_ID>.TXT In every processed directory	(configuration) In every processed directory
Name of the encrypted file	<FILENAME>.<VICTIM_ID>	<FILENAME>.<VICTIM_ID>	<FILENAME>.<VICTIM_ID>
Terminating processes	optional (configuration)	optional (configuration)	optional (configuration)
Stopping services	optional (configuration)	optional (configuration)	optional (configuration)
Deleting volume shadow copies	yes WQL queries	optional (configuration) WQL queries	yes WQL queries
Privilege Escalation			
UAC Bypass	if necessary ICMLuaUtil	optional (configuration) ICMLuaUtil	optional (configuration) CVE-2018-8453
Valid accounts	optional (configuration)	no	no
Defense Evasion			
Configuration data encryption / packing / encoding	custom / aPLib / Base64	custom / Base64 / aPLib	RC4
Location of the configuration data	Separate PE-section	Separate PE-section	Separate PE-section
Configuration data format	binary	binary	JSON
Comparison of strings by hash	yes	no	no
Encryption of strings and program data	custom	custom	RC4
Obfuscation of API function calls	yes	yes	yes
C&C communication, data encryption/encoding	optional (configuration) HTTP/ HTTPS POST-request AES 128 ECB / Base64	optional (configuration) HTTP/ HTTPS POST-request	optional (configuration) HTTP/ HTTPS POST-request
Anti-Debug	NtSetInformationThread with parameter ThreadHideFromDebugger	no	no
Other			
Language check	no	optional (configuration)	optional (configuration)
Creating mutex, Mutex name	optional (configuration) The name is created based on MachineGuid	optional (configuration) The name is encrypted based on MachineGuid	yes The name is hardcoded
Victim Id / ransom extension	Created based on MachineGuid	Created based on MachineGuid	Random

Group-IB: "It's alive: The story behind the BlackMatter ransomware strain", 2021

At the moment, we cannot be sure that the same development team is behind all three ransomware programs. However, it is clear that the vacant place did not remain unoccupied for long: **DarkSide and REvil were replaced by the no less sophisticated BlackMatter**. According to a statement in Russian made by the hacker group's representative as part of an interview for Recorded Future, the work on the ransomware took about six

months, and the best solutions from the LockBit, REvil, and DarkSide programs were used to create the program. We believe that the representative is hiding something. It is doubtful that the unrelated groups LockBit, REvil, and DarkSide would share their expensive source code with a competitor, while reverse engineering ransomware is time-consuming and makes little sense.

The shadow economy created by those behind the ransomware is attracting more and more new players, while old ones either change their mask or unite into new partnership programs and create spin-off projects. **Today, ransomware is the most profitable cybercriminal business.** It thrives thanks to a mutually beneficial business model that brings together cybercriminals with various specializations. Failure to clearly understand the ransomware business is the number one problem for any company, industry, or country.

Victims often neglect information security and save money on building an effective defense against such threats only to then pay out a lot more to criminals and in fact sponsor criminal activities.

How to protect your network against ransomware:

- Make your remote access tools secure. Use multifactor authentication or at least set complex passwords and change them regularly.
- Eliminate vulnerabilities in publicly accessible apps as soon as possible, especially those that could allow attackers to bypass the external perimeter.
- Implement comprehensive email protection to detect and stem the most sophisticated threats. More
- Monitor what your contractors do in your network. Providing them with remote access should be strictly regulated.
- Instantly patch vulnerabilities on hosts on the internal network that attackers could leverage to escalate privileges or propagate across the network.
- Monitor the use of dual-use tools that could help attackers conduct network reconnaissance, obtain authentication data, and much more.
- Restrict access to cloud storage. This will help keep attackers from exfiltrating data from the corporate network.
- Make sure all accounts have the least possible privileges on the systems. In case of an attack, this will make it difficult for threat actors to move laterally across the network.
- Use separate accounts with multifactor authentication to access servers containing backups. Moreover, make sure that you have offline copies.
- Implement a modern threat monitoring and blocking tool that will help contain and repel attacks at any stage of the kill chain. More

For more information about attacks using manually controlled ransomware, **see the Group-IB report “Ransomware 2021/2022”:**
