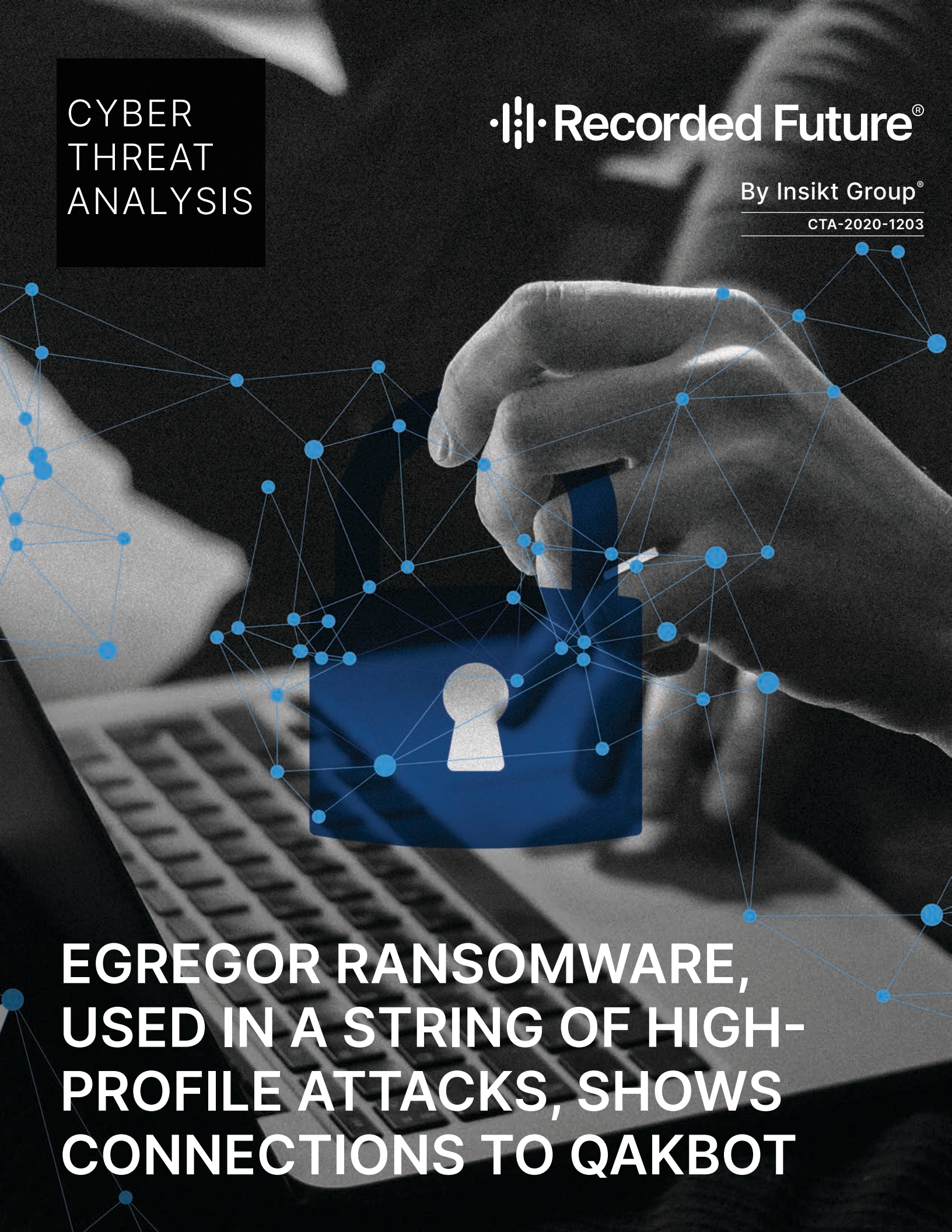
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-1203



EGREGOR RANSOMWARE, USED IN A STRING OF HIGH-PROFILE ATTACKS, SHOWS CONNECTIONS TO QAKBOT

This report provides an overview of the ransomware variant Egregor as well as suggested mitigations and detections. Recorded Future used the Recorded Future® Platform, PolySwarm, open source intelligence (OSINT) sources, and malware analysis to derive these detections. The target audience of this research includes day-to-day security practitioners as well executive decision-makers concerned about targeting by ransomware threat actors.

Executive Summary

Egregor ransomware is a complex piece of malware that appears to be associated with the operators of QakBot. The ransomware has been used against organizations across many industries since its debut in September 2020 and is likely to continue to present a threat to organizations in the future. Unlike most ransomware variants, Egregor's payload cannot be executed or decrypted fully without the correct cryptographic key provided to the malware at runtime, rendering static or dynamic analysis impossible. Because very little is known about the deployment of the ransomware in open sources and how the threat actors target victims, Recorded Future recommends employing mitigations for technical threats used by other "big game hunting" threat actors to mitigate the threat prior to ransom, using the provided hunting package to threat hunt Egregor and ensuring that internet-facing systems are appropriately configured to provide only the minimum needed access.

Key Judgments

- The Egregor ransomware is a complex piece of malware, employing obfuscation and anti-analysis techniques. In order to fully decrypt and deploy the payload, the password associated with the sample must be provided at runtime.
- Egregor ransomware is connected to the QakBot operators.
- The targets of the Egregor ransomware are organizations, which Egregor both ransoms and uses the "name and shame" double extortion technique to further victimize the companies.

Background

Egregor ransomware is part of the Sekhmet ransomware family and has been active since mid-September 2020. The name of the new ransomware strain, Egregor, is derived from Western occult traditions and is defined as the collective energy of a group of people, especially when aligned to a common goal.

Like many current ransomware variants, Egregor uses the "double-extortion" model of both encrypting files and naming and shaming victims and releasing stolen data on an extortion website to increase pressure on a victim to pay the ransom. Egregor News is an extortion website operated by the threat actors behind Egregor ransomware and is used to post the names and domains, along with data sets of Egregor victims. If the victim refuses to pay within three days, the threat actors will continue to leak additional data in increments ranging from 1 percent to 100 percent of the total stolen data. The most high-profile Egregor victim to date is the bookseller Barnes & Noble, with the ransomware operators claiming they stole unencrypted data prior to encrypting files on October 10, 2020.

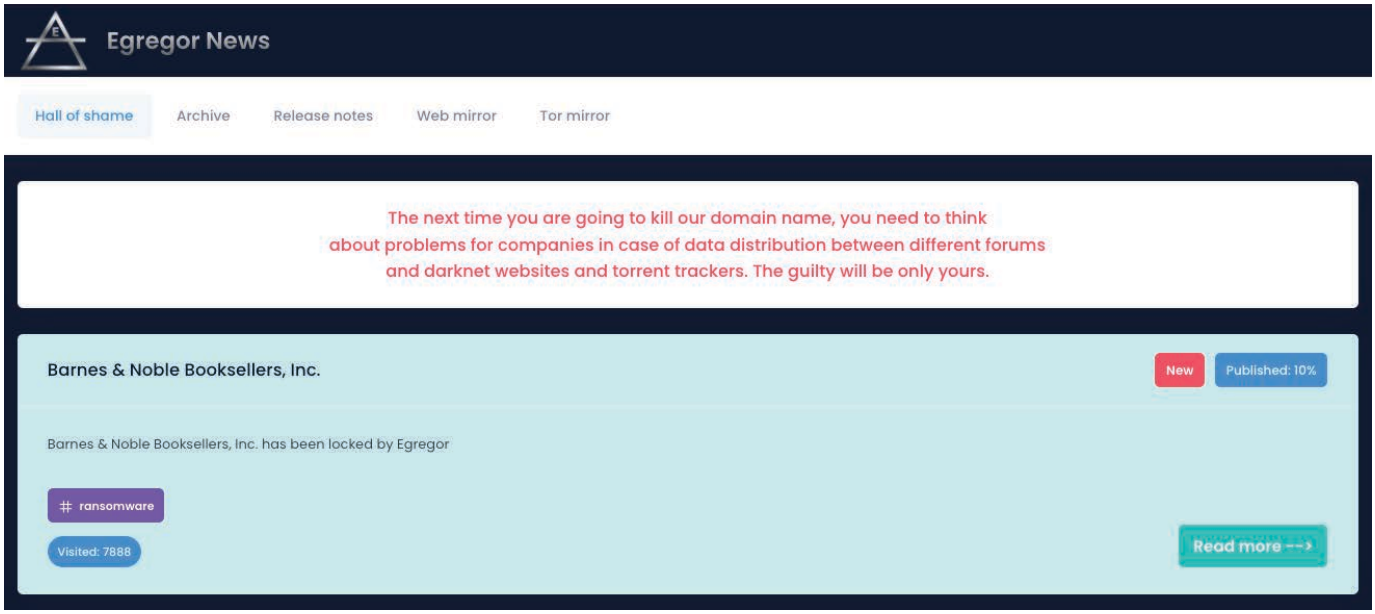


Figure 1: Egregor News

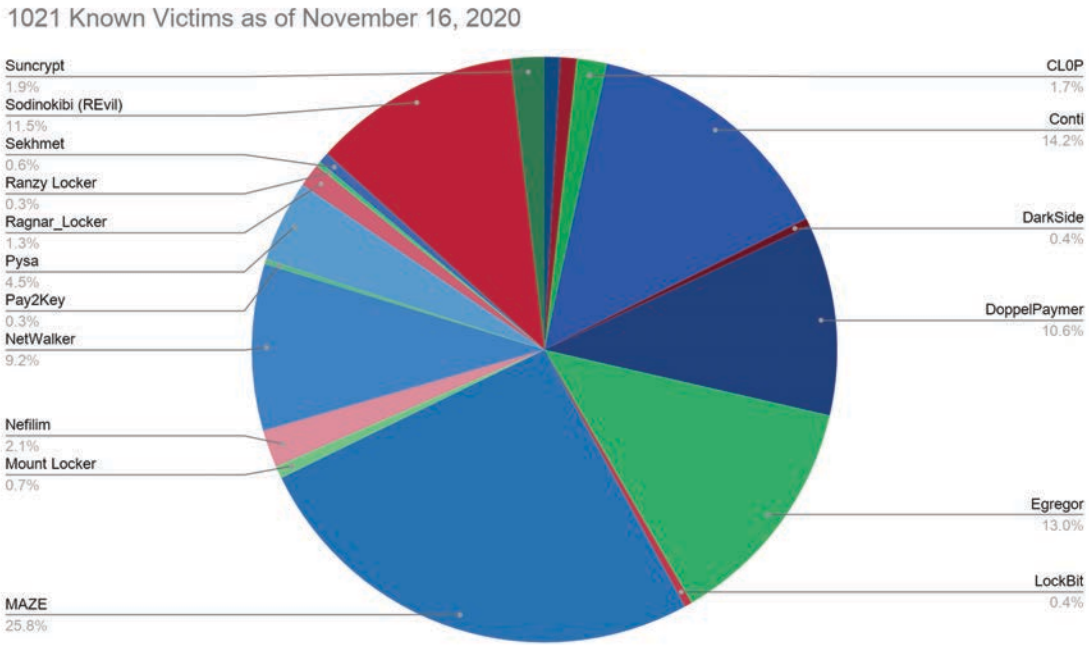


Figure 2: Ransomware victims chart, by ransomware variant (Source: Recorded Future)

According to the information available on Egregor News, they claimed 133 victims and are responsible for 13 percent of all currently known ransomware extortion cases, which is a large number for just two months of operations. We believe that ransomware operators and their affiliates are opportunistic by nature and do not focus on specific industries or geographic regions, but rather select and pursue corporations based on accessibility, opportunity, and company's revenue. These threat actors will very likely continue to consistently target larger organizations. This assessment is predicated on the understanding that the wide attack surface inherent to large corporations gives threat actors more chances to gain access. Furthermore, these businesses maintain an abundance of resources, and generally have strong cyber insurance policies, making it more likely that they will pay a large ransom demand.

According to a Bankinfosecurity article, QakBot operators have abandoned ProLock for Egregor ransomware. The TTPs used by the threat actors in Egregor attacks are almost identical to the ones used by the ProLock operators. Group-IB experts consider it very likely that QakBot operators have switched from ProLock to Egregor ransomware because the threat actors always employ Microsoft Excel documents impersonating DocuSign-encrypted spreadsheets to deliver Qakbot as an initial access vector. Also, Egregor operators have been using Rclone for data exfiltration, and the same tools and naming convention have been used as well — for example, md.exe, rdp.bat, and svchost.exe.

Technical Analysis

Recorded Future's Insikt Group identified several copies of packed Egregor ransomware and performed analysis on these samples. The ransomware has three main "stages": the top-level packer that decrypts the next stage using the Salsa20 stream cipher with compiled-in keys, a subsequent stage that uses a cryptographic key passed in at runtime to decrypt the payload, and finally the Egregor payload. Without the correct key passed to the ransomware when it is run, the payload is unable to be decrypted and analyzed either statically or dynamically. We identified one sample and cryptographic key pair that enabled analysis of the Egregor payload. To detonate the malware, the command that is run is:

```
rundll32.exe <dllname>.dll,DllRegisterServer -p<cryptographic key>
<payload arguments>
```

Initial Access

Currently, Recorded Future has not observed any open source information regarding the initial access vectors used by the threat actors behind Egregor. Several other researchers have tied Egregor to the Maze ransomware variant at the technical level, suggesting that similar initial access techniques could be used by the Egregor threat actors as those used by the Maze operators. Historically, the operators of Maze ransomware employed a wide array of techniques to gain initial access to organizations, most recently using RDP and remote services as initial access vectors to victim systems, but also exploiting CVE-2018-15982 and CVE-2018-4878 in Flash Player, CVE-2019-11510 in Pulse VPN, and CVE-2018-8174 in Internet Explorer. While past behavior does not guarantee future behavior, Maze's operators have used a wide variety of initial access vectors, suggesting that the threat actors behind Egregor may also do so.

Reconnaissance and Lateral Movement

Recorded Future has not observed any open source information regarding reconnaissance or lateral movement tools. Many threat actors are using Cobalt Strike Beacon and QakBot to enable reconnaissance and lateral movement, as well as deploying a variety of commodity tools such as Mimikatz, PowerShell Empire, and Metasploit prior to dropping and executing the ransomware payload.

Stage One Packer

The files identified by Insikt Group as containing the initial packer stage used by Egregor were highly similar in form and function, differing primarily in the compiled-in Salsa20 cryptographic keys, the file path it looks for upon initialization, and a command line parameter it checks for (but does not appear to have any real utility to the execution of the code). In addition, while some of the files did not employ obfuscation to the code, several did to complicate the static and dynamic reverse engineering process. This could suggest that the different copies originate from different affiliates, some who employ an obfuscator tool and some who do not. It is likely that this obfuscation is introduced by a tool, since both obfuscated and unobfuscated versions were observed in the wild, but Insikt Group is not sure whether the tool is homegrown by the actors or a commodity item purchased or downloaded from the internet.

To decrypt the second stage of the packed payload, which is contained in the .data section, the malware first does an XOR of the data with either 3 or 4, then does a base64-decode of the data, and finally the Salsa20 decryption. This code, from a sample that did not employ any anti-RE obfuscation, can be seen in Figure 3.

```
commandLine = GetCommandLineW();
ptr = do_wcsstr_z(commandLine,L"--nooperation");
if (ptr == (wchar_t *)0x0) {
  size = 0;
  decoded_base64_key = do_base64_decode_and_xor_z(ENCRYPTED_DATA,0x4e800,&size);
  if (decoded_base64_key == (byte *)0x0) {
    local_c = 1;
  }
  else {
    allocatedSpace = VirtualAlloc((LPVOID)0x0,size,0x3000,0x40);
    salsa20_key_expand(&expanded_key,"iFHDFSID8ysdgdhSDJSSGgFjiS9XhSA3",0x100);
    salsa20_iv(&expanded_key,"oDYdBSgs");
    salsa20_actual_decrypt_z(&expanded_key,decoded_base64_key,allocatedSpace,size);
    check_decrypted_section_z(allocatedSpace);
    Sleep(0xffffffff);
    if (decoded_base64_key != (byte *)0x0) {
      FID_conflict:_free(decoded_base64_key);
    }
    local_c = 0;
  }
}
else {
  local_c = 0;
}
```

Figure 3: Top-level packer for Egregor

Stage Two Packer

The second stage of the packer was nearly identical in every sample of the malware analyzed by Insikt Group. This stage was unobfuscated, even when extracted from samples that had an obfuscated stage one packer. The primary functionality of this stage is to create a thread that will read the cryptographic key passed in after the "-p" in the aforementioned malware execution command, and use that to decrypt the Egregor payload. The decryption scheme appears custom, with elements of SHA256 hashing and the lesser-known Rabbit cryptographic cipher combined to decrypt the payload. If it successfully decrypts this stage, it will run the decrypted payload. Typically, Insikt Group has not observed Rabbit cryptography employed in other ransomware variants.

Egregor Payload

The Egregor payload, if successfully decrypted, will cause the victim system to be encrypted. The ransomware contains obfuscation, both for the code and for some of the data contained within it. It also encrypts the ransom note contents, services, and processes to stop, and almost all of the strings that would help an analyst determine what the code was doing. A technical analysis of the ransomware payload revealed the following:

- A simple rolling XOR-based obfuscation technique is used to hide some of the strings in the malware. We have not observed this specific cipher in use by other ransomware variants.
- The malware contains an encrypted chunk of data, prefaced with ".PNG", including the contents of the ransom note, a list of processes and services to stop, and a public RSA key. These pieces of data are used throughout the execution of the ransomware.
- Egregor's payload can accept several command line arguments, including:
  - --fast: The parameter requires a number as an argument, the file size in megabytes, and is used to limit file size for encryption.
  - --full: perform encryption of the full victim system (including local and network drives).
  - --multiproc: if set, does not create mutex Global\\<system data and CRC32 hash>. This value is presumably created to ensure only one copy runs at a time. This same string of characters is placed in the ransom note to identify the victim.
  - --nomimikatz: Insikt Group was unable to determine the functionality of this parameter. Mimikatz is an open source toolkit that allows the extraction of plaintext passwords, Kerberos tickets, PINs, and hashes from memory, so this parameter may be related to collecting user authentication information.
  - --nonet: does not encrypt network drives.
  - --path: specific folder to encrypt.
  - --target: target extension for encryption.
  - --append: file extension to append to encrypted files. Otherwise, a random series of five to six characters (in our analysis) is appended to the filenames.
  - --norename: does not rename the files it encrypts.
  - --greetings: prepends the name to the ransom note, presumably to directly address a victim.
  - --samba: Insikt Group was unable to determine the functionality of this parameter. TrendMicro indicates that the parameter is used to set the DELETE_ON_CLOSE attribute for created .lnk files.
  - --killrdp: the malware also looks for TeamViewer and TermService (Remote Desktop Service) by name and shuts the services down.
- The malware checks the "Default Language ID" of the victim system and user account. If the language is any of the following, it exits and does not execute: Uzbek, Romanian, Azerbaijani, Turkmen, Georgian, Kyrgz, Ukrainian, Kazakh, Tatar, Russian, Tajik, Armenian, Belarusian, Romanian.
- Collects victim system information, including username, computer name, general system information, domain name, workgroup, and installed AV programs (such as Windows Defender).
- Deletes shadow copies using WMI.
- The malware creates the following files:
  - LNK file: <8 characters>.lnk file in each encrypted directory. The .lnk filename appears to be the CRC32 hash of a subset of victim information, so will be the same for every run of the malware, though different per victim system. This .lnk file is deleted after the encryption completes.
  - Ransom note: the ransom note (RECOVER-FILES.txt) in each encrypted directory.
  - %ProgramData%\\dtb.dat: this file name was also used in Sekhmet ransomware.
- To prevent recovery measures or backup features an organization might enact when the encryption begins, Egregor looks for a list of processes to shut down, including outlook.exe, thunderbird.exe, procmon.exe, and sqlservr.exe. The full list can be found in Appendix A. It also looks to terminate services containing "sql" or "database."
- The ransomware will exclude a specific list of files and directories from encryption:
  - The extension list from our sample included: "lnk", "exe", "sys", and "dll". Encrypting these files would likely render the victim's system unable to operate correctly, which would negatively impact the ability to pay the ransom.
  - Folders that the malware excludes: Windows, Program Files, Tor Browser, ProgramData, \\cache2\\entries (Firefox cache), \\Low\\Content.IE5\\ (temporary IE internet files), \\User Data\\Default\\Cache, and All Users.
  - Files containing the following strings: dtb.dat (dropped by the ransomware), autorun.inf, boot.ini, desktop.ini, ntuser.dat, iconcache.db, bootsect.bak, ntuser.dat.log, thumbs.db, Bootfont.bin, and RECOVER-FILES.txt (created by the ransomware).

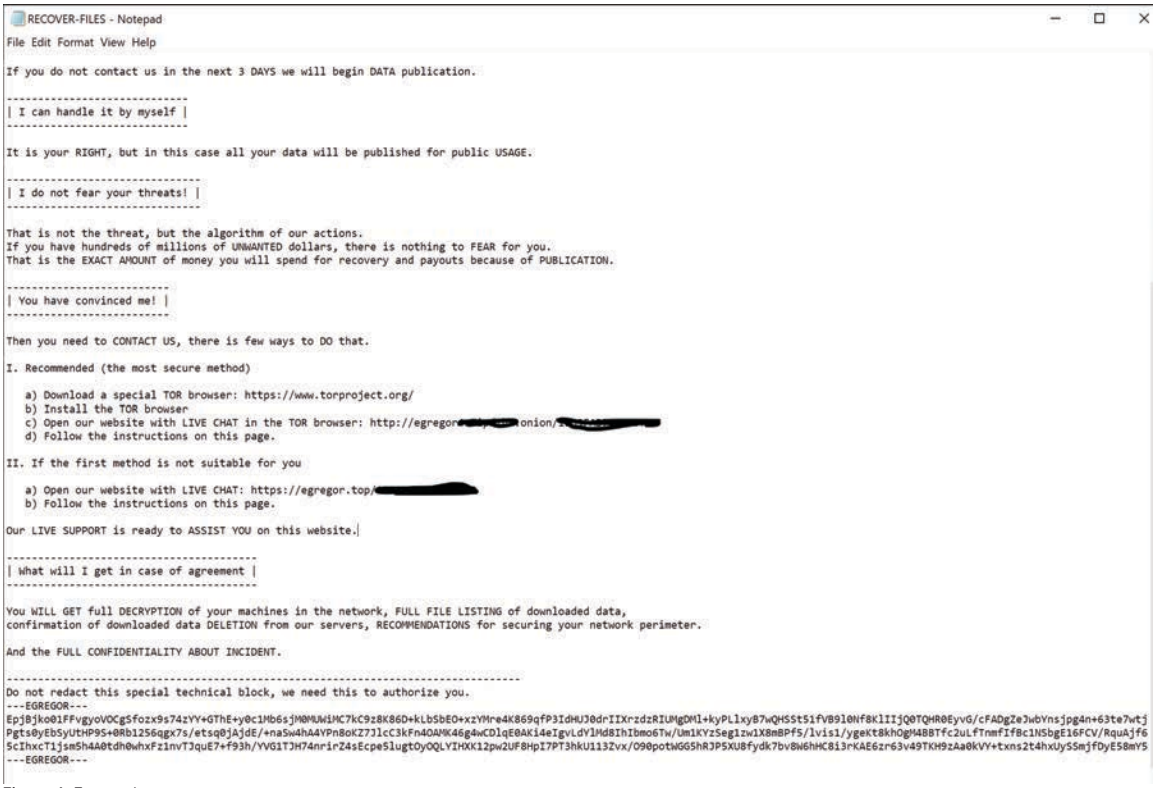


Figure 4: Egregor's ransom note

- The ransomware appears to have the capability to create an internet connection, specifically a POST request to http://<url>/update.php?id=<id> but Insikt Group was unable to cause this connection to occur. In the Sekhmet ransomware, this POST is used to send gathered victim data back to the threat actor, suggesting that this functionality may remain in the code, but is currently unused by Egregor.
- The ransom note dropped by the payload can be seen in Figure 4, below. The Tor chat link contains the victim identifier used with the created mutex:

Recently, in an attack on a retail organization, the threat actor not only encrypted the systems on the network, but printed out copies of the ransom note on printers attached to the systems, further underscoring the sophistication of the threat actors.

Mitigations

While currently there is very little known in open sources regarding how Egregor is being deployed to victim systems, Recorded Future has identified the following recommendations:

- It is most effective to detect a ransomware threat prior to the deployment of the ransomware. While Insikt Group has not observed any evidence of how the threat actor gains initial access to victim systems, sophisticated threat actors often deploy commodity tools such as Cobalt Strike and QakBot to perform reconnaissance and lateral movement prior to the deployment of a ransomware payload. Organizations should monitor for use of these and other lateral movement/reconnaissance tools on corporate systems in addition to the ransomware payload.
- Because ransomware threat actors often use exploits as a means of initial access to victimized systems, it is critical that organizations ensure that any internet-facing systems are appropriately configured to provide the appropriate needed access. These systems should be patched to help mitigate the threat of vulnerabilities that are often exploited by these types of threat actors.
- Organizations should also be aware of the risk of phishing attacks, the use of fake download websites, the targeting of unpatched publicly accessible systems, and the exploitation of misconfigurations in publicly accessible systems.

Outlook

The team behind Egregor has targeted several high-profile organizations to date, and is very likely to continue doing so. The group behind Egregor will likely remain active and continue to employ techniques associated with sophisticated threat actors and "big-game hunting."

Appendix A : Technical Details

Processes to Kill

msftesql.exe
sqlagent.exe
sqlbrowser.exe
sqlwriter.exe
oracle.exe
ocssd.exe
dbsnmp.exe
synctime.exe
agntsvc.exe
isqlplussvc.exe
xfssvccon.exe
sqlservr.exe
mydesktopservice.exe
ocautoupds.exe
encsvc.exe
firefoxconfig.exe
tbirdconfig.exe
mydesktopqos.exe
ocomm.exe
mysqld.exe
mysqld-nt.exe
mysqld-opt.exe
dbeng50.exe
sqbcoreservice.exe
excel.exe
infopath.exe
msaccess.exe
mspub.exe
onenote.exe
outlook.exe
powerpnt.exe
sqlservr.exe
thebat.exe
steam.exe
thebat64.exe
thunderbird.exe
visio.exe
winword.exe
wordpad.exe
QBW32.exe
QBW64.exe
ipython.exe
wpython.exe
python.exe
dumpcap.exe
procmon.exe
procmon64.exe
procexp.exe
procexp64.exe

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.