Egregor Awakens: Taking A Tour of A Threat Actor’s New Digs

Lindsay Kaye
Director, Operational Outcomes, Insikt Group
Recorded Future

Recorded Future®

About Me

- Lindsay Kaye, Director, Operational Outcomes, Insikt Group at Recorded Future

- Malware analyst and reverse engineer - I like taking apart weird cryptography

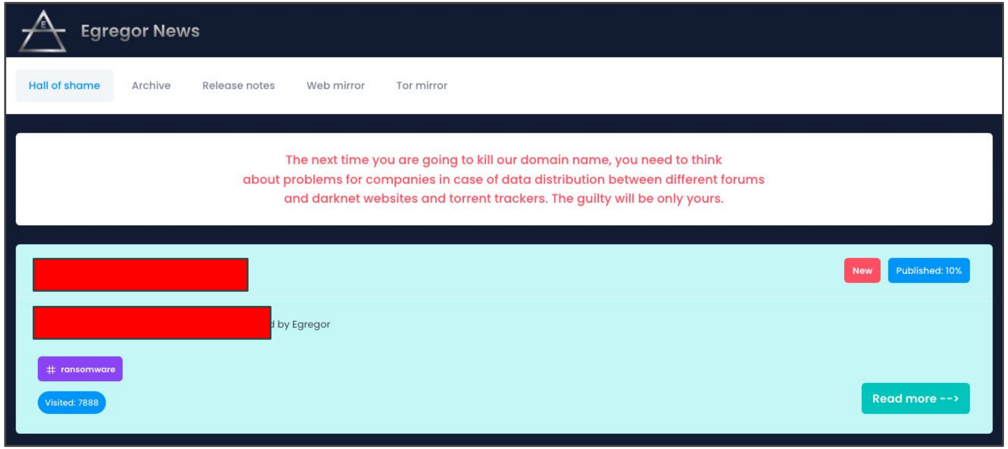
- Currently run Insikt Group's technical team at Recorded Future

Overview

- Background on Egregor
- Technical deep dive
- Overlaps with other threat actors
- Ways to track Egregor

Who is Egregor?

- Began operating in September 2020 - considered a variant of the Sekhmet family
- Many affiliates of the Maze ransomware variant have likely moved to Egregor
  - Maze stopped encrypting new victims in September 2020
- “Name and shame” of victims on extortion site “Egregor News”



The next time you are going to kill our domain name, you need to think about problems for companies in case of data distribution between different forums and darknet websites and torrent trackers. The guilty will be only yours.

[redacted]

New

Published: 10%

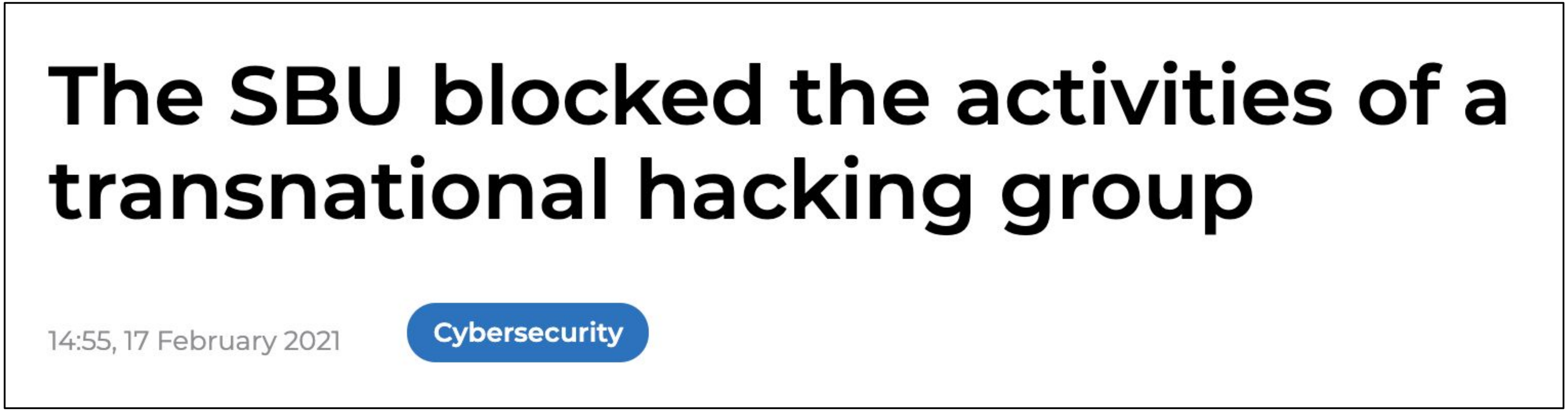
[redacted] by Egregor

ransomware

Visited: 7888

Egregor News, leak site (Source: Recorded Future)

Who is Egregor?



The SBU blocked the activities of a transnational hacking group

14:55, 17 February 2021

Source: ssu.gov.ua

- In mid-February, members of the Egregor Ransomware-as-a-Service were arrested in Ukraine
- We saw their infrastructure (C2s, leak site) down since at least 2/12/21
- Since then, Egregor have stopped encrypting victims and they do not appear to have rebuilt their infrastructure

Egregor: Ransomware-as-a-Service

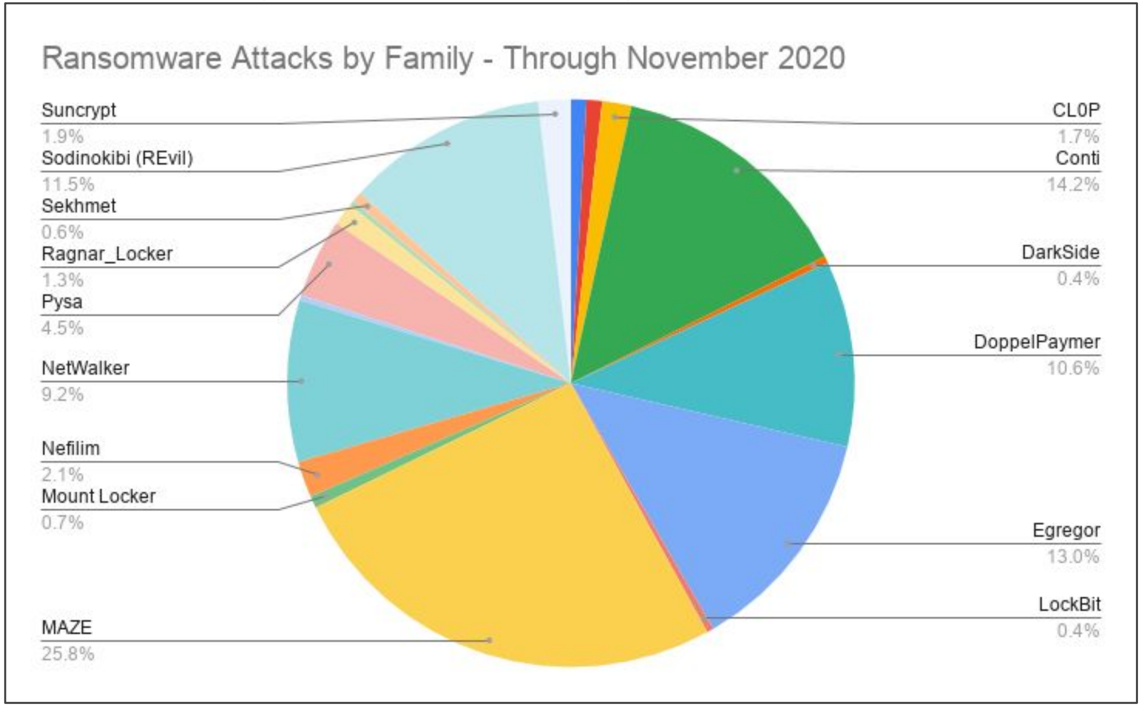
- What is RaaS?
  - Ransomware developer creates ransomware code
  - Affiliates can buy or lease the malware to execute their own attacks
  - Developer usually gets some cut of the ransom

- Because Egregor uses a RaaS model, TTPs will vary between attacks
  - Initial access techniques
  - Pre-encryption: lateral movement, reconnaissance, credential stealing etc.
  - Tools used in any stage of the attack

- Some affiliates may be or have been involved with other ransomware groups

Egregor's Victims

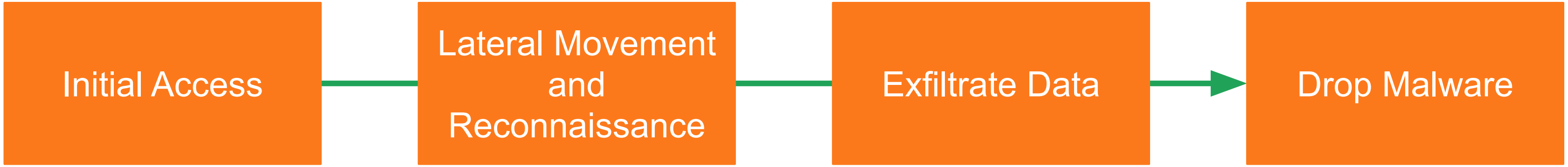
By the end of 2020, Egregor had claimed 206 victims - including many large, well-known organizations according to its extortion site



Ransomware victims by ransomware variant in 2020 (Source: Recorded Future)

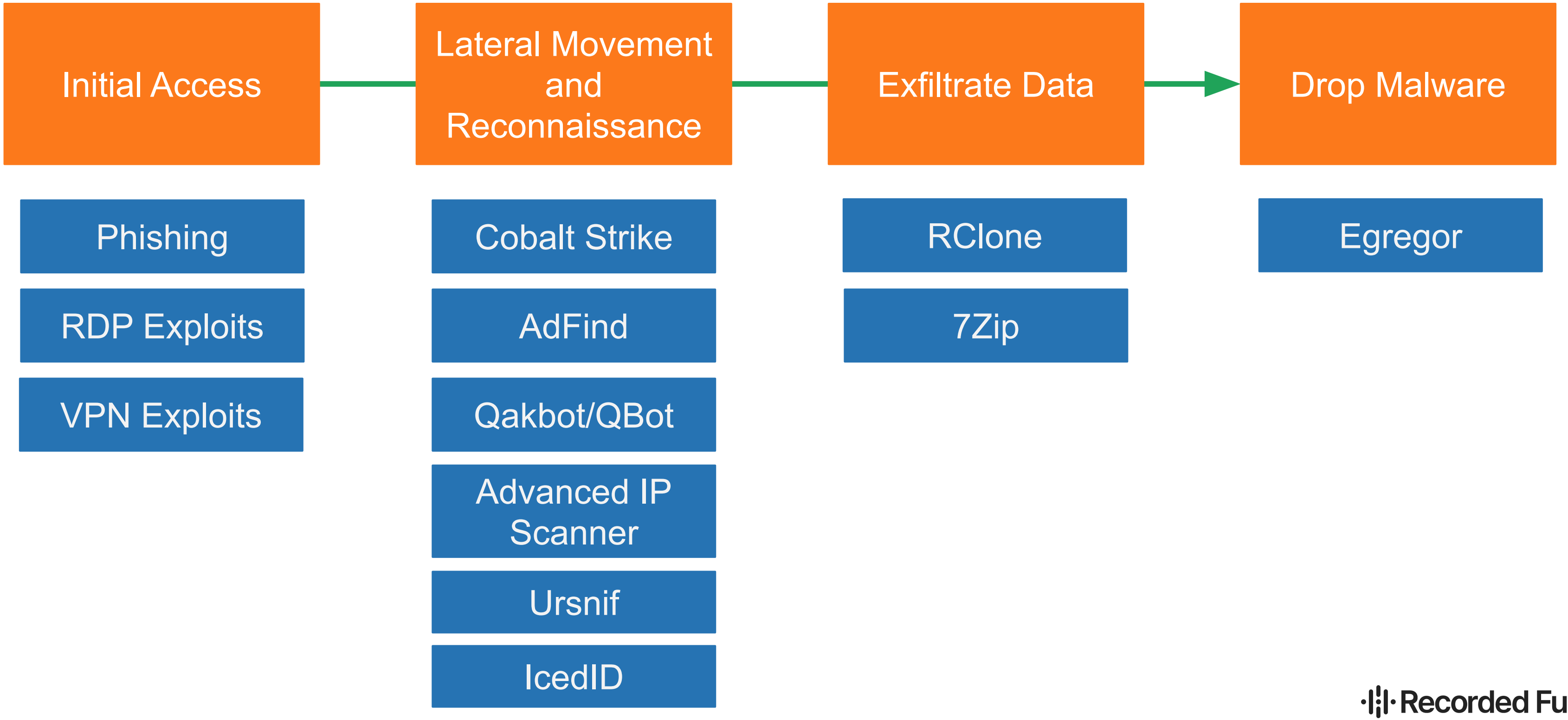
Recorded Future®

How Do Egregor Attacks Unfold?



Recorded Future®

How Do Egregor Attacks Unfold?



Initial Access

- Phishing
- RDP Exploits
- VPN Exploits

Lateral Movement and Reconnaissance

- Cobalt Strike
- AdFind
- Qakbot/QBot
- Advanced IP Scanner
- Ursnif
- IcedID

Exfiltrate Data

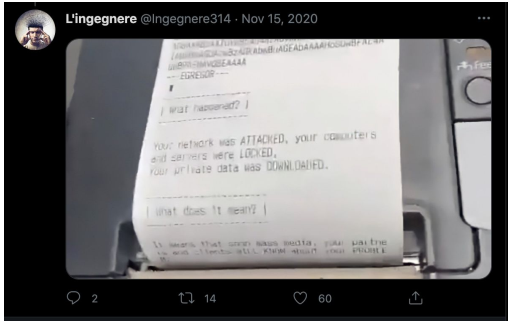
- RClone
- 7Zip

Drop Malware

- Egregor

How Do Egregor Attacks Unfold?

Initial Access	Lateral Movement and Reconnaissance	Exfiltrate Data	Drop Malware
Phishing	Cobalt Strike	RClone	Egregor
RDP Exploits	AdFind	7Zip	Print Bomb Ransom note
VPN Exploits	Qakbot/QBot		
	Advanced IP Scanner		
	Ursnif		
	IcedID		



L'ingegnere @Ingegnere314 · Nov 15, 2020

[illegible]

--- EGREGOR ---

| What happened? |

Your network was ATTACKED, your computers and servers were LOCKED,
Your private data was DOWNLOADED.

| What does it mean? |

It means that soon mass media, your partners and clients will KNOW about your PROBLEM.

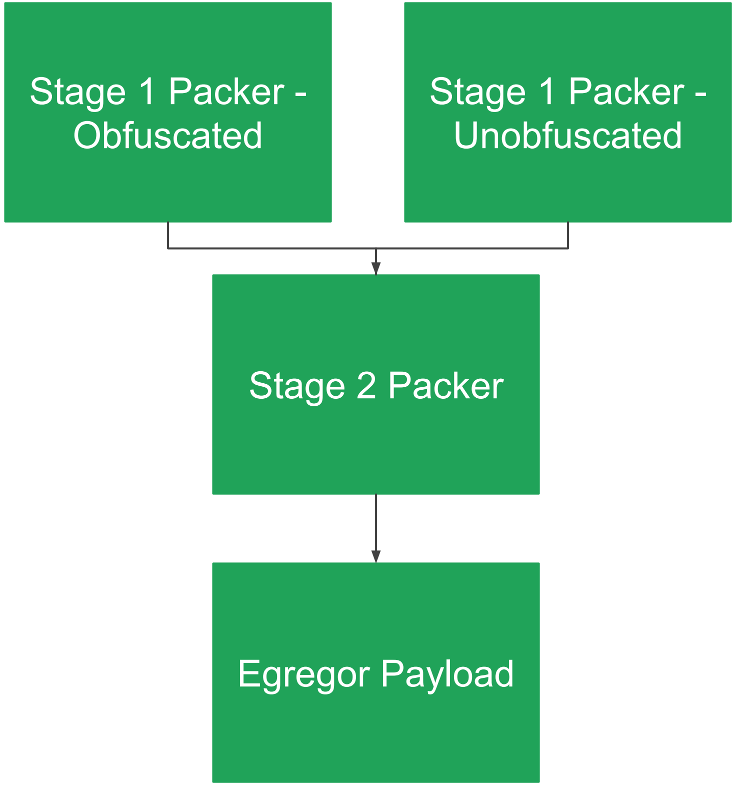
(Source: Twitter)

Yes, really

Recorded Future®

Egregor Ransomware Payload

- Three “layers” to the malware
- In order to execute the payload, need a correct cryptographic key
- Accepts several command line arguments to determine functionality/behavior



Stage 1 Packer - Obfuscated

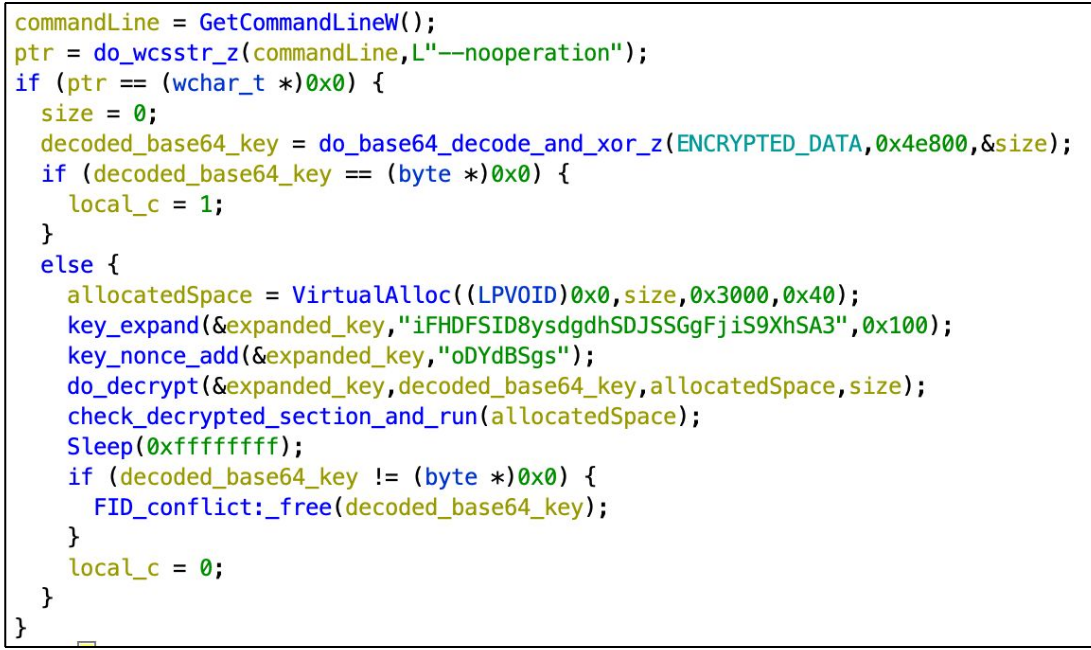
Stage 1 Packer - Unobfuscated

Stage 2 Packer

Egregor Payload

Stage 1 Packer

- Two versions seen: obfuscated and unobfuscated
  - Suggests compile-time obfuscation utility
- Baked-in cryptographic key material
- Overall, very similar, with slight differences
  - Command line parameter
  - XOR value (3 or 4)
  - Crypto key/IV



```
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);
    key_expand(&expanded_key,"iFHDFSID8ysdgdhSDJSSGgFjiS9XhSA3",0x100);
    key_nonce_add(&expanded_key,"oDYdBSgs");
    do_decrypt(&expanded_key,decoded_base64_key,allocatedSpace,size);
    check_decrypted_section_and_run(allocatedSpace);
    Sleep(0xffffffff);
    if (decoded_base64_key != (byte *)0x0) {
      FID_conflict:_free(decoded_base64_key);
    }
    local_c = 0;
  }
}
```

Egregor’s first stage packer, unobfuscated (Source: Recorded Future)

Stage 1 Packer

- Some had baked-in PDB paths that were fairly similar to each other
  - M:\ewdk\*
  - M:\sc\p\*
- Could suggest multiple individuals compiling the code, with some more active than others
- Of course, PDB is very easy to modify per build - but patterns are still interesting

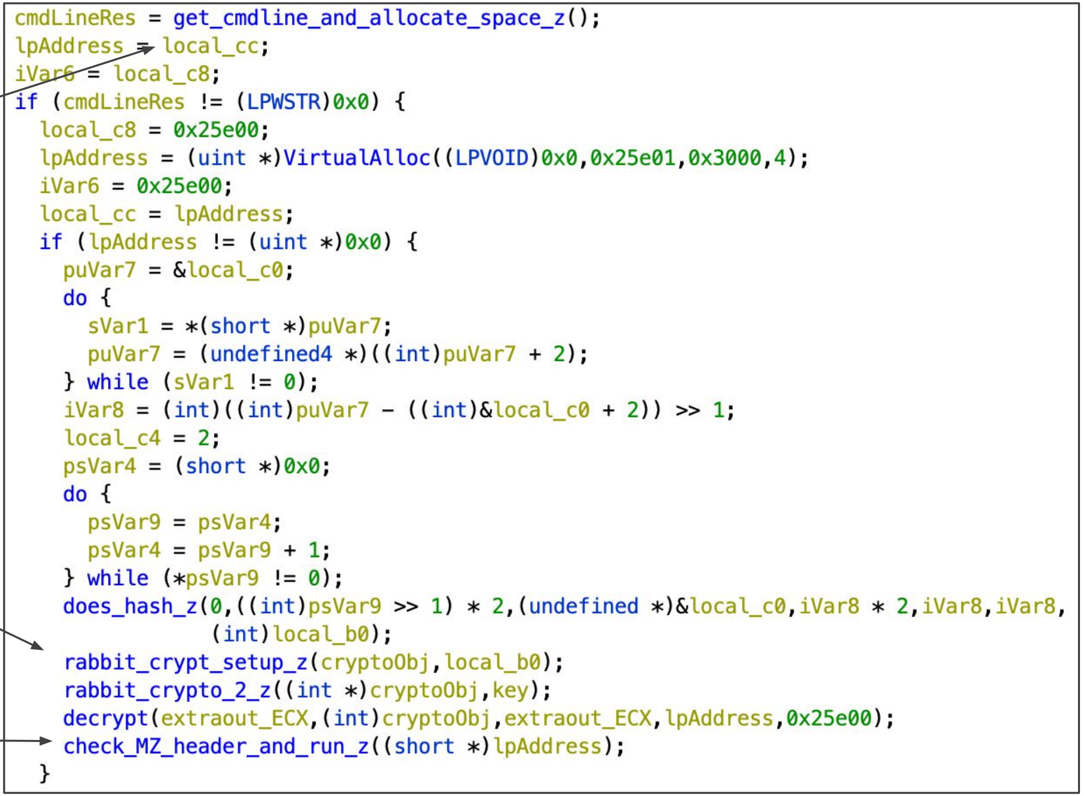
PDB Path	Count
M:\sc\p\testbuild.pdb	11
M:\ewdk\Program Files\Microsoft\ExtensionManager\Extensions\Microsoft\Windows Kits\10\Debug\ewdk.pdb	10
M:\sc\p\sed.pdb	5
M:\ewdk\CommonAppData\Microsoft\HelpLibrary2\Catalogs\VisualStudio14\clang.pdb	4
G:\fasm\INCLUDE\API\fasm.pdb	4
G:\defaultlog\installator\debug\*	4
M:\ewdk\CommonAppData\Microsoft\HelpLibrary2\Catalogs\VisualStudio14\msvc.pdb	3
G:\0\0.pdb	2
M:\trash\project\ocx.pdb	1
G:\Intel\Logs\qqqqq.pdb	1

Stage 2 Packer

Read command line, looking for argument after “-p” (this is the password)

Use password in Rabbit decryption function

Check for the MZ header (valid PE file) and run



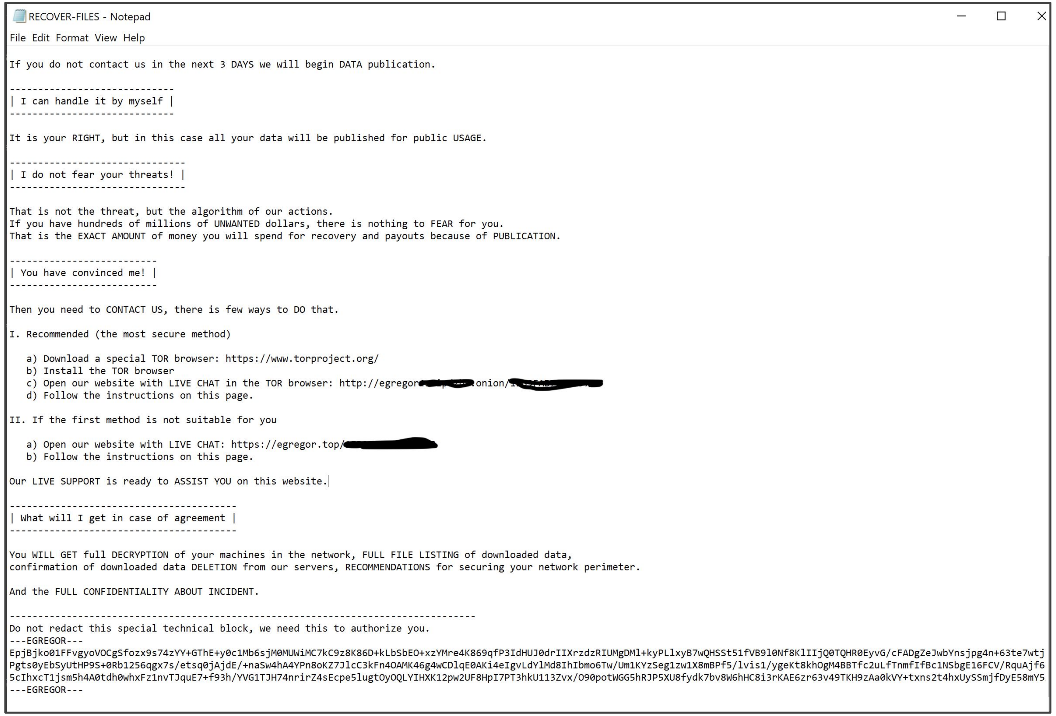
```
cmdLineRes = get_cmdline_and_allocate_space_z();
lpAddress = local_cc;
iVar6 = local_c8;
if (cmdLineRes != (LPWSTR)0x0) {
  local_c8 = 0x25e00;
  lpAddress = (uint *)VirtualAlloc((LPVOID)0x0,0x25e01,0x3000,4);
  iVar6 = 0x25e00;
  local_cc = lpAddress;
  if (lpAddress != (uint *)0x0) {
    puVar7 = &local_c0;
    do {
      sVar1 = *(short *)puVar7;
      puVar7 = (undefined4 *)((int)puVar7 + 2);
    } while (sVar1 != 0);
    iVar8 = (int)((int)puVar7 - ((int)&local_c0 + 2)) >> 1;
    local_c4 = 2;
    psVar4 = (short *)0x0;
    do {
      psVar9 = psVar4;
      psVar4 = psVar9 + 1;
    } while (*psVar9 != 0);
    does_hash_z(0,((int)psVar9 >> 1) * 2,(undefined *)&local_c0,iVar8 * 2,iVar8,iVar8,
                (int)local_b0);
    rabbit_crypt_setup_z(cryptoObj,local_b0);
    rabbit_crypto_2_z((int *)cryptoObj,key);
    decrypt(extraout_ECX,(int)cryptoObj,extraout_ECX,lpAddress,0x25e00);
    check_MZ_header_and_run_z((short *)lpAddress);
  }
```

Egregor’s second stage packer (Source: Recorded Future)

Egregor Payload

Overall, pretty typical ransomware behaviors

- Language checks for CIS countries
- Deletes shadow copies using WMI
- Stops processes and services that could aid in recovery, backup
- Encrypts files on victim system, except for specific file extensions and folders

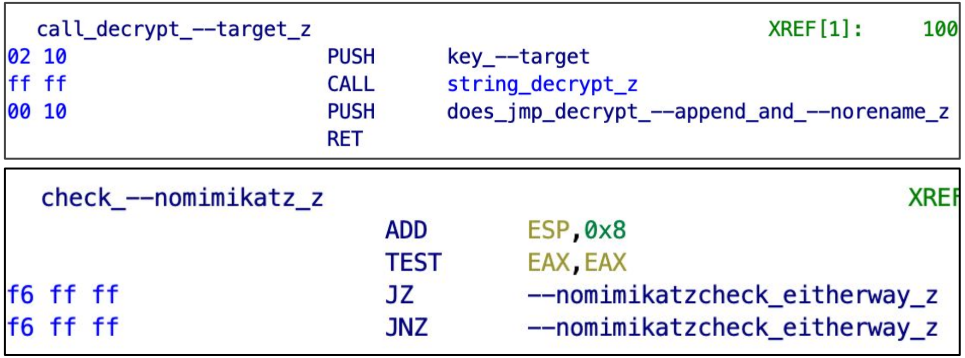


```
If you do not contact us in the next 3 DAYS we will begin DATA publication.

----------------------------
| I can handle it by myself |
----------------------------

It is your RIGHT, but in this case all your data will be published for public USAGE.

-----------------------------
| I do not fear your threats! |
-----------------------------

That is not the threat, but the algorithm of our actions.
If you have hundreds of millions of UNWANTED dollars, there is nothing to FEAR for you.
That is the EXACT AMOUNT of money you will spend for recovery and payouts because of PUBLICATION.

-------------------------
| You have convinced me! |
-------------------------

Then you need to CONTACT US, there is few ways to DO that.

I. Recommended (the most secure method)

   a) Download a special TOR browser: https://www.torproject.org/
   b) Install the TOR browser
   c) Open our website with LIVE CHAT in the TOR browser: http://egregor[redacted]onion/[redacted]
   d) Follow the instructions on this page.

II. If the first method is not suitable for you

   a) Open our website with LIVE CHAT: https://egregor.top/[redacted]
   b) Follow the instructions on this page.

Our LIVE SUPPORT is ready to ASSIST YOU on this website.

---------------------------------------
| What will I get in case of agreement |
---------------------------------------

You WILL GET full DECRYPTION of your machines in the network, FULL FILE LISTING of downloaded data,
confirmation of downloaded data DELETION from our servers, RECOMMENDATIONS for securing your network perimeter.

And the FULL CONFIDENTIALITY ABOUT INCIDENT.

----------------------------------------------------------------------------------
Do not redact this special technical block, we need this to authorize you.
---EGREGOR---
EpjBjko01FFvgyoVOCgSfozx9s74zYY+GThE+y0c1Mb6sjM0MUWiMC7kC9z8K86D+kLbSbEO+xzYMre4K869qfP3IdHUJ0drIIXrzdzRIUMgDMl+kyPLlxyB7wQHSSt51fVB9l0Nf8KlIIjQ0TQHR0EyvG/cFADgZeJwbYnsjpg4n+63te7wtj
Pgts0yEbSyUtHP9S+0Rb1256qgx7s/etsq0jAjdE/+naSw4hA4YPn8oKZ7JlcC3kFn4OAMK46g4wCDlqE0AKi4eIgvLdYlMd8IhIbmo6Tw/Um1KYzSeg1zw1X8mBPf5/lvis1/ygeKt8khOgM4BBTfc2uLfTnmfIfBc1NSbgE16FCV/RquAjf6
5cIhxcT1jsm5h4A0tdh0whxFz1nvTJquE7+f93h/YVG1TJH74nrirZ4sEcpe5lugtOyOQLYIHXK12pw2UF8HpI7PT3hkU113Zvx/O90potWGG5hRJP5XU8fydk7bv8W6hHC8i3rKAE6zr63v49TKH9zAa0kVY+txns2t4hxUySSmjfDyE58mY5
---EGREGOR---
```

Egregor ransom note (Source: Recorded Future)

Egregor Payload

- Borrows heavily from Sekhmet code, similar:
  - Processes terminated
  - Extensions/filenames to avoid encryption
  - Ransom note name (RECOVER-FILES.txt)
  - File renaming scheme
  - String encryption method
  - Method of code obfuscation
  - Highly similar first stage packer



```
  call_decrypt_--target_z                                                  XREF[1]:     100
02 10                         PUSH       key_--target
ff ff                         CALL       string_decrypt_z
00 10                         PUSH       does_jmp_decrypt_--append_and_--norename_z
                              RET
```

```
  check_--nomimikatz_z                                                   XREF
                                ADD        ESP,0x8
                                TEST       EAX,EAX
f6 ff ff                        JZ         --nomimikatzcheck_eitherway_z
f6 ff ff                        JNZ        --nomimikatzcheck_eitherway_z
```

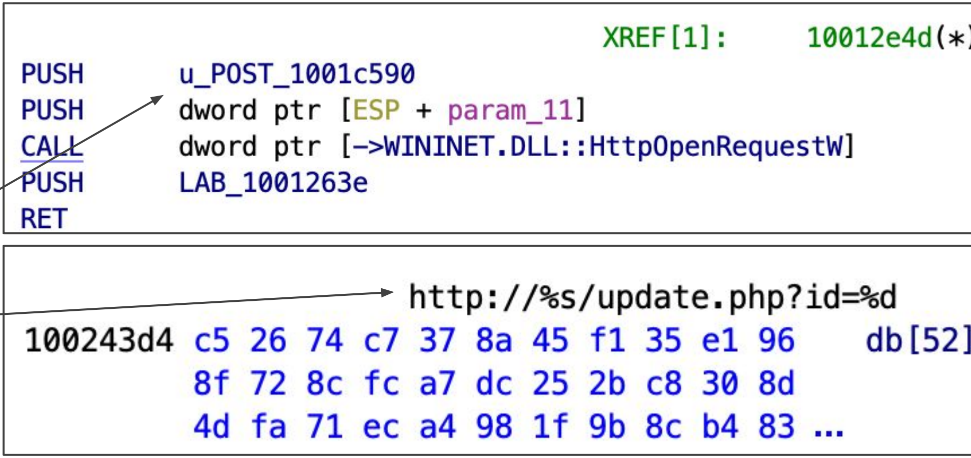
Code obfuscation used in Egregor and Sekhmet (Source: Recorded Future)

```
while k < len(to_decrypt):
    save = []
    for i < 0x10:
        v = xorkey[i] ^ 0x2
        if i = 0:
            save.append(v)
        xorval = xorkey[i]
        d = ((v + i) * 0x8081) >> 0x17
        v = v + d + i
        if i != 0:
            save.append(v)
        decrypted = to_decrypt[i] ^ xorval
        k++
    xorkey = save
```

Pseudocode for Egregor and Sekhmet string obfuscation (Source: Recorded Future)

Sekhmet++

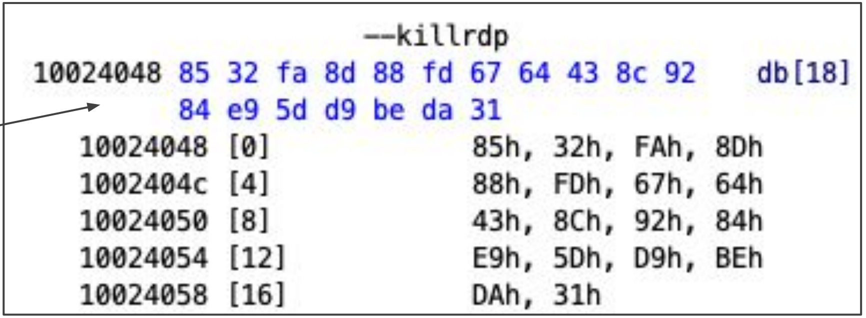
- A few key differences
  - Egregor contains code for HTTP POST request that does not appear to be triggered (functional in Sekhmet)
  - Sekhmet has 2 “stages” only - and no password required!
  - Adds command line parameters: --samba (LNK files will not have "DELETE_ON_CLOSE") , --killrdp
  - Dropped filenames
    - dtb.dat (Egregor)
    - %ProgramData%\syscfg.db (Sekhmet)



```
                                        XREF[1]:     10012e4d(*
PUSH        u_POST_1001c590
PUSH        dword ptr [ESP + param_11]
CALL        dword ptr [->WININET.DLL::HttpOpenRequestW]
PUSH        LAB_1001263e
RET
```

```
                        http://%s/update.php?id=%d
100243d4 c5 26 74 c7 37 8a 45 f1 35 e1 96    db[52]
         8f 72 8c fc a7 dc 25 2b c8 30 8d
         4d fa 71 ec a4 98 1f 9b 8c b4 83 ...
```

“Vestigial” source code in Egregor payload (Source: Recorded Future)



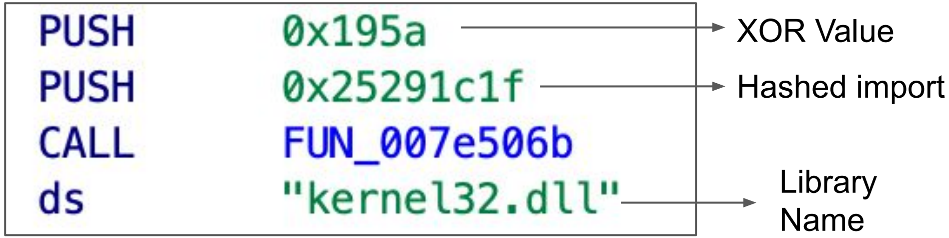
```
                     --killrdp
10024048 85 32 fa 8d 88 fd 67 64 43 8c 92    db[18]
         84 e9 5d d9 be da 31
   10024048 [0]              85h, 32h, FAh, 8Dh
   1002404c [4]              88h, FDh, 67h, 64h
   10024050 [8]              43h, 8Ch, 92h, 84h
   10024054 [12]             E9h, 5Dh, D9h, BEh
   10024058 [16]             DAh, 31h
```

“--killrdp” bytes in Egregor payload (Source: Recorded Future)

Recorded Future®

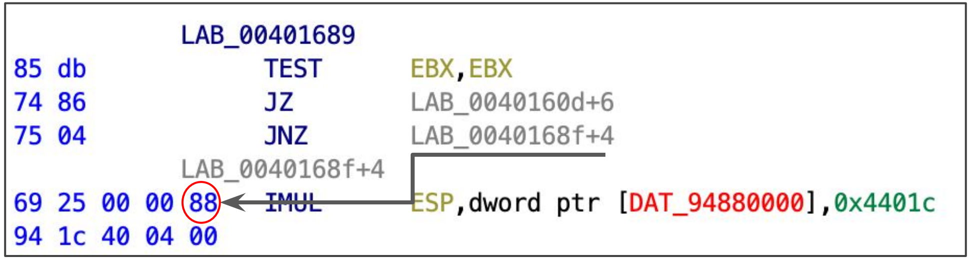
Maze--

- Uses substantially different obfuscation techniques than Maze ransomware
- Packers/first stages are very different
  - Wide variety used with Maze
- Different code obfuscation techniques
  - Absolute conditional jump
  - Indirect absolute jump to call
  - And more!
- Pretty similar looking country check
  - Not a “smoking gun” imho



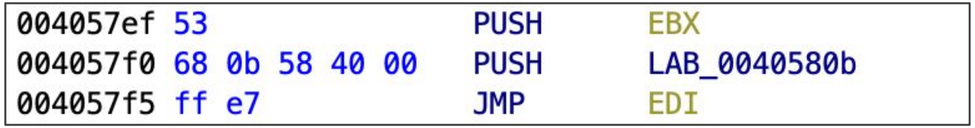
```
PUSH        0x195a
PUSH        0x25291c1f
CALL        FUN_007e506b
ds          "kernel32.dll"
```

Maze import hashing technique (Source: Recorded Future)



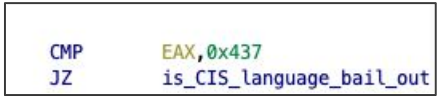
```
              LAB_00401689
85 db              TEST       EBX,EBX
74 86              JZ         LAB_0040160d+6
75 04              JNZ        LAB_0040168f+4
              LAB_0040168f+4
69 25 00 00 88     IMUL       ESP,dword ptr [DAT_94880000],0x4401c
94 1c 40 04 00
```

Maze code obfuscation technique - absolute conditional jump (Source: Recorded Future)



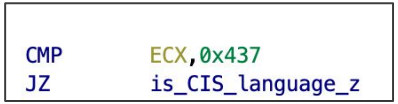
```
004057ef 53                PUSH     EBX
004057f0 68 0b 58 40 00    PUSH     LAB_0040580b
004057f5 ff e7             JMP      EDI
```

Maze code obfuscation technique - indirect absolute jump (Source: Recorded Future)



```
CMP       EAX,0x437
JZ        is_CIS_language_bail_out
```

Egregor language check



```
CMP       ECX,0x437
JZ        is_CIS_language_z
```

Maze language check

Ok, so that's just code, what else?

Really, as ransomware affiliates move to new variants, new operations spin up and spin down, cartels form and commodity tools get used, obvious hallmarks of specific threat actors or variants become blurred - **we need to look at contextual information as well**

- Chainalysis believes "Blockchain analysis suggests affiliate overlap and other possible connections between Maze, Egregor, SunCrypt, and Doppelpaymer"
- Cobalt Strike used in 70% of Big Game Hunting incidents in 2020
- RDP is the most common attack vector employed to install ransomware
- VPN vulnerabilities are popular as well
- Everyone uses phishing!

Mostly just suggestive of "Big Game Hunting" in general, at a broad technical level

What does this mean for defenders?

- Good news: many of the same TTPs used between ransomware actors!
  - Focus detections/mitigations on common issues
  - Aware of vulnerable products and tools
  - FBI advised patching several RDP vulnerabilities from 2019 and 2020
- Bad news: they're still succeeding using these TTPs
  - Phishing is an eternal problem
  - Patching takes resources, may fall by the wayside
  - Separating "good" vs. "bad" use of tools is difficult
- Worst news: they will evolve their TTPs if they need
  - There is big money in Big Game Hunting
  - Remember the affiliates!

Tracking Egregor

- Monitor for unexpected commodity/openly available tool use: Qakbot, Cobalt Strike especially
  - Not Egregor-specific, commonly used with ransomware deployments
  - Often a precursor to many kinds of unsavory behavior
  - Recorded Future has created Sigma rules and YARA rules for some of these

- Based on “unique” technical aspects
  - Second stage is extremely consistent between samples - even bytewise
  - String encryption technique used in final payload
  - First-stage decryption process - XOR, ChaCha cipher, MZ/PE check, Sleep if fail

What’s Next?

- With the arrest of affiliates, the “Egregor” operation is very likely dead
  - Likely that the operators will move to a new operation
  - Possible to see TTPs carry over to new operation

- Ransomware is not going away anytime soon
  - Big Game Hunting is big business!
  - “Name and shame” will likely remain popular
  - “Cartels” as well

Thank you!

lindsay.kaye@recordedfuture.com

@theQueenofELF

Recorded Future®