KARA
Korea Anti Ransomware Alliance

2023.11.

KARA ransomware trend report

KARA Ransomware Trend Report

■ Ransomware trends

✓ Ransomware trend analysis

In the third quarter, ransomware group's pressure strategy became more sophisticated. The Clop Group's data leak, which was thought to have ended in the second quarter, has continued, and furthermore, the Clop Group is continuing to leak data through ClearNet[1] and Torrent. This can be seen as part of the strategy to compensate for the download speed problem of the existing Tor browser and to pressure victimized companies through broad accessibility. In a similar way, the BlackCat Group began to provide an API that can get detailed information about victimized companies.

The strategies and attack tools for successful attacks have also advanced to the next level. An affiliate of the LockBit Group developed an elaborate strategy of simultaneously preparing not only the LockBit ransomware but also the RaaS-type ransomware called 3AM to infect ransomware, and it was confirmed that when the LockBit ransomware was blocked by the security system, the 3AM ransomware was used to successfully carry out the attack. On the other hand, the BlackCat Group released the Sphynx ransomware with built-in Remcom[2] and Impacket[3], and the Abyss Group and the Monti Group released Linux versions of the ransomware. Ransomware groups target various operating systems and use ransomwares with built-in powerful functions, and sometimes use attack strategies that utilize ransomwares from multiple groups.

1 ClearNet: Publicly accessible Internet
2 Remcom: An open source version of PsExec, a tool that allows remote PC control
3 Impacket: A collection of tools for access testing of network protocols and services

New ransomware and group activities

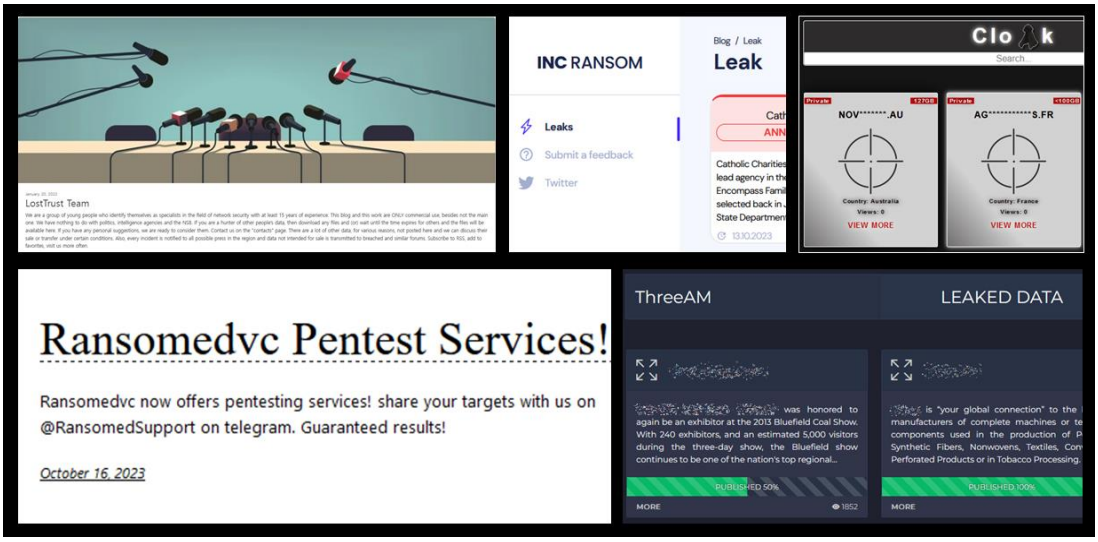


Figure 1. New ransomware and group activities

In the third quarter, 12 ransomware groups, i.e. CyClops, Knight, MetaEncryptor, LostTrust, UnderGround, Cactus, INC, Ransomed, Cloak, 3AM, CiphBit, and CryptBB, were discovered. Among them, the Cyclops Group began its activities in July, and after announcing an affiliate panel and ransomware update at the end of July, it re-emerged by rebranding[4] itself as the Knight Group. Additionally, the LostTrust Group and the MetaEncryptor Group use the same images and phrases on the dark web leak site, and it was confirmed that their codes are similar to those of the Sfile2 ransomware discovered in the first quarter of 2022. The fact that the codes are similar to those of the Sfile2 ransomware, the introductory phrases of the LostTrust Ransomware Group and the MetaEncryptor Ransomware Groups are similar, and the posted victims are all different means that it is not a simple imitation, and the LostTrust Group can be assumed to be a rebrand of the MetaEncryptor Group.

4 Rebranding: Ransomware attackers publicly suspend an operation and then restart it under a new name.

Some groups were confirmed to be related to or have partnerships with other groups. In particular, some say that the Cloak Group discovered in August is connected to the GoodDay Group. This is based on the evidence that the dark web address used by the Cloak Group was written in the ransom note used by the GoodDay Group. In addition, the Ransomed Group is continuing its activities after discontinuing the operation of Ransomed.vc, which is ClearNet, and switching to the dark web. In this process, it emphasized its partnerships with BreachFourn, a dark web forum, and ransomware groups Stormous and Everest through Telegram and interviews. These measures suggest that these groups are not simply engaged in individual activities, but have a win-win relationship in which they cooperate with other groups to carry out more active attacks.

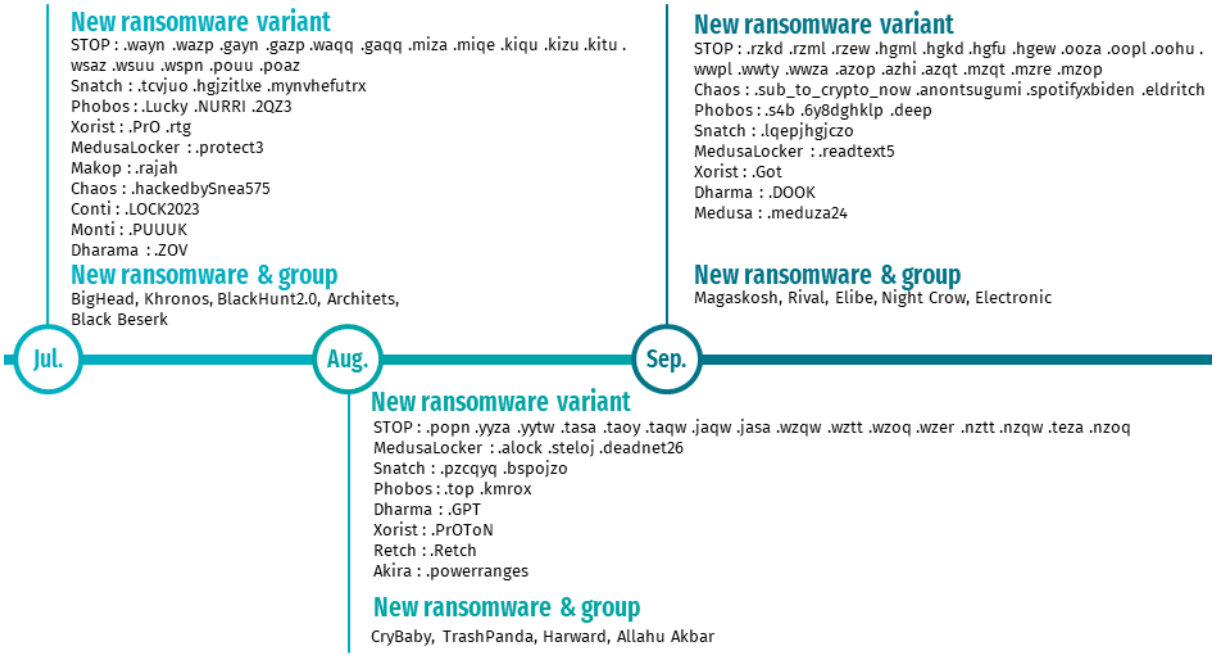


Figure 2. New/variant ransomware activities

Recently, as the LockBit ransomware was blocked by the security system while an affiliate of the LockBit Group was attacking the system, it used the 3AM ransomware to infect the system. This incident revealed the existence of the 3AM Group, but the connection between the 3AM Group and the LockBit Group has not been confirmed to date. What is noteworthy in this incident is that an affiliate of the LockBit Group possessed and selectively used various RaaS[5]-type ransomwares rather than simply one ransomware in order to successfully carry out the attack.

5 RaaS: It's short for Ransomware-as-a-Service. It is a service in which ransomware is provided in exchange for money.

The 3AM ransomware was produced in the Rust language, and similarly ransomwares produced in non-mainstream languages continue to appear. The movement to adopt non-mainstream languages appears to be continuing as it has advantages in fast encryption speed, analysis and detection bypass, and cross-platform[6]. SophosEncrypt, created in the Rust language, impersonates Sophos, an information security company, and includes not only system encryption, a common ransomware behavior, but also RAT functions that can log key input and remotely control the system. Additionally, the Kanti ransomware written in the Nim language was discovered in August.

Ransomware attack group trends

Since the Clop Group's large-scale attack using the MOVEit vulnerability, the number of attacks utilizing vulnerabilities in software used by many companies has been increasing. In particular, it has recently been confirmed that the LockBit Group and the Akira Group attempted attacks targeting companies by exploiting the vulnerabilities of Cisco VPN and Firepower Threat Defense. At the same time, cases of using social engineering techniques to spread ransomwares are also increasing, e.g. Knight disguised as a TripAdvisor e-mail, Magniber disguised as a Windows security update, and BlackCat distributed through normal software sites and Google Ads. This can be seen as a difference in technology between some groups or affiliates, but it can also mean that ransomware groups do not easily change the initially designed strategy.

Through collaboration with IABs[7], the ransomware ecosystem is becoming more organized and sophisticated. RaaS groups look systematic, e.g. hiring affiliates, purchasing initial access paths from IABs to perform attacks, and laundering their revenues through mixing services[8]. Due to these changes, ransomware attacks are possible even without professional knowledge, and damage cases are also increasing. In addition, in the past, ransomware groups mostly requested ransom through data encryption, but groups requesting ransom by disclosing decryption tools or only stealing data to avoid detection are appearing one after another.

Ransomware group activities and statistics

In the third quarter, 1,384 damage cases were confirmed, up by 8% over the previous quarter. This is the result of not only large-scale attacks by the Clop Group and the Malas Group, but also the brisk activities of new groups such as 8Base, NoEscape, LostTrust, and Cactus.

6 Cross-platform: A form that can be operated on various platforms with one language and tool
7 IAB: It's short for Initial Access Broker. A broker who specializes in initial access only
8 Mixing service: A service that mixes cryptocurrency transaction details and is used to avoid tracking virtual assets

The LockBit Group was the most threatening as it caused the most damages in the third quarter too, but around July, when the Clop Group posted a large amount of data, it seemed to be conscious of this and did not post any data, but when Clop's activity decreased, it posted a large amount of data. Considering that the number of attacks in July was 49 and 122 in August, it can be seen that there has been some change in activity. Additionally, in August, it was revealed that affiliates had expressed dissatisfaction or left the organization due to the poor management of the LockBit Group. It was confirmed that the biggest reason was a decrease in reliability due to data posting errors and dark web page errors, absence of developers, and delays in the development of new ransomwares. Meanwhile, cases of damages to domestic companies were confirmed: that is, LockBit posted data from two domestic companies in August and September, and the MetaEncryptor Group and the NoEscape Group posted data from one domestic company each.

Recently, RaaS groups support multi-platforms and provide services to enable attack against various platforms, and cases of attacks exploiting vulnerabilities are continuously discovered. Depending on the impact of the vulnerability, large-scale attacks and damages may occur. So it is necessary to take proactive and preemptive measures by understanding ransomware groups' strategies and tactics in advance.

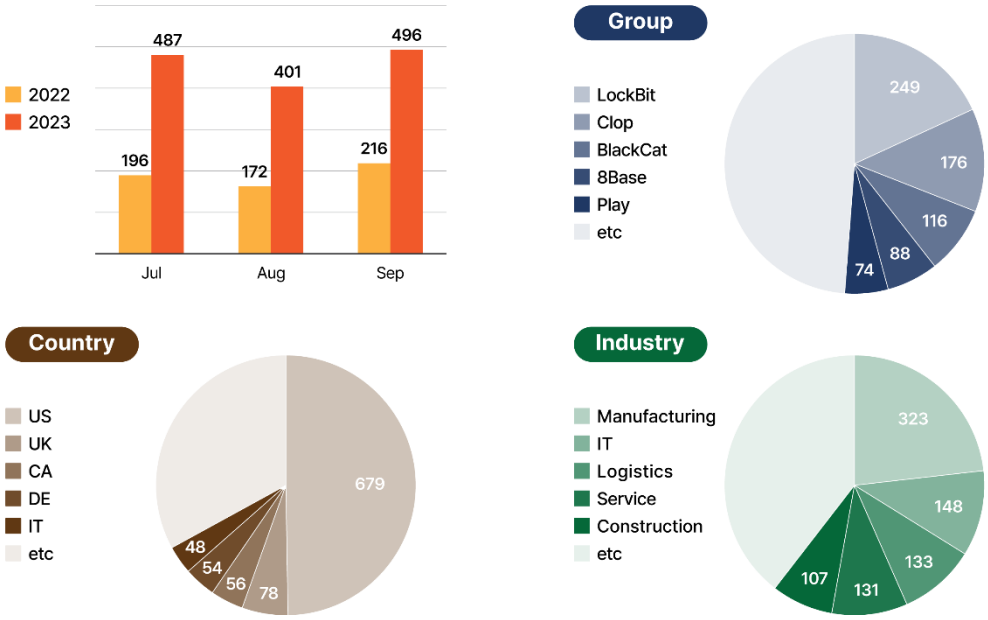


Figure 1. Ransomware group activities

✓ 2 types of ransomwares that can be decrypted

In the third quarter, the decryption script for ransomwares used by KeyGroup was released by EclecticIQ. There was only one sample that could be decrypted, and the ransomware in question was capable of file decryption using the fixed key for file encryption. Additionally, for the Payola ransomware discovered in September, a decryption tool was released to Virus Total, allowing decryption of some ransomwares whose private key and public key match. Like this, cases of ransomwares, which can be decrypted because of mistakes caused by exposure of the encryption key, vulnerability of the encryption algorithm, use of a simple xor operation instead of the encryption algorithm, and leakage of the private key due to the leakage of the decryption tool.

The Ransomware Response Center of SK Shieldus analyzed some variants of the PoliceRecords ransomware used by KeyGroup, and the NoBit ransomware, which is recently operated in the form of RaaS, and confirmed that decryption is possible for some samples confirmed to date. Accordingly, we would like to provide detailed analysis and decryption script for the ransomware.

1. KeyGroup ransomware actively utilizes leaked builder

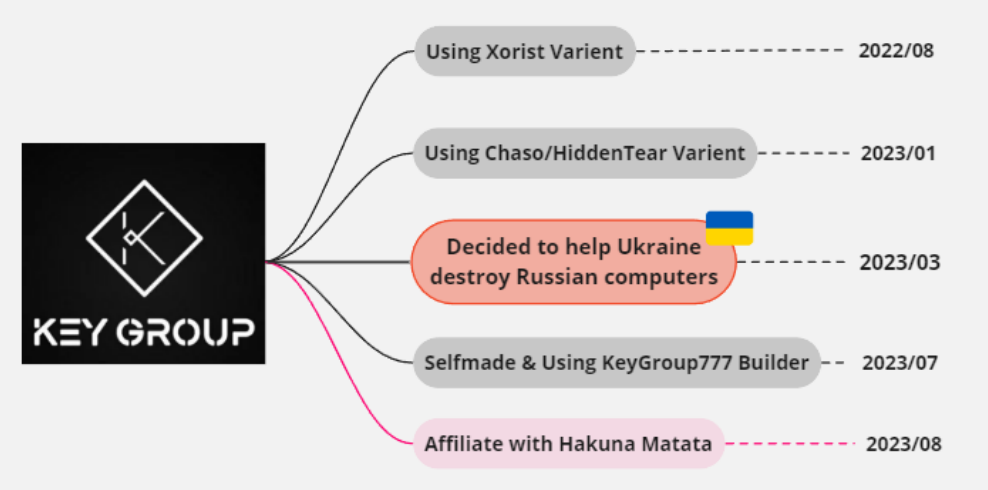


Figure 4. KeyGroup ransomware activities

The KeyGroup ransomware was first discovered in August 2022. The initial version is based on the Xorist ransomware and is confirmed to have attacked mainly Russians. In early January 2023, it began distributing variants using the Chaos 4.0 Builder[9], and in March, it declared through a ransom note, 'We will help Ukraine and destroy Russian computers,' revealing its anti-Russian sentiments. Since April, it has been active in a dark web forum called DarkStore, and is continuing its activities by distributing NjRAT malware and attacking Russian Telegram channels.

Meanwhile, since April of this year, they have been continuously sharing not only the ransomware builder they created, but also various ransomware builders and source codes such as Chaos, HiddenTear, and GoldenEye that were leaked in the past, through Telegram, and the use of the Anabelle, RuRansom, and Cyborg ransomware was confirmed. The situation has been confirmed. Additionally, in August, it was revealed that it was in partnership with the HakunaMatata ransomware. Recently, the number of groups using leaked ransomware builders or source codes has been increasing, and as the source codes of the HelloKitty ransomware were leaked recently, it is expected that variants using these source codes will increase.

The Ransomware Response Center of SK Shieldus analyzed the ransomware used by KeyGroup and confirmed that decryption was possible in some samples. Additionally, the ransomware that can be decrypted is a variant of the PoliceRecords ransomware discovered in May 2022, and it has been confirmed that decryption is also possible in some variants of the ransomware. Accordingly, we would like to provide the analysis contents and decryption script.

9 Builder: A tool that can create or distribute ransomware

1) Feature

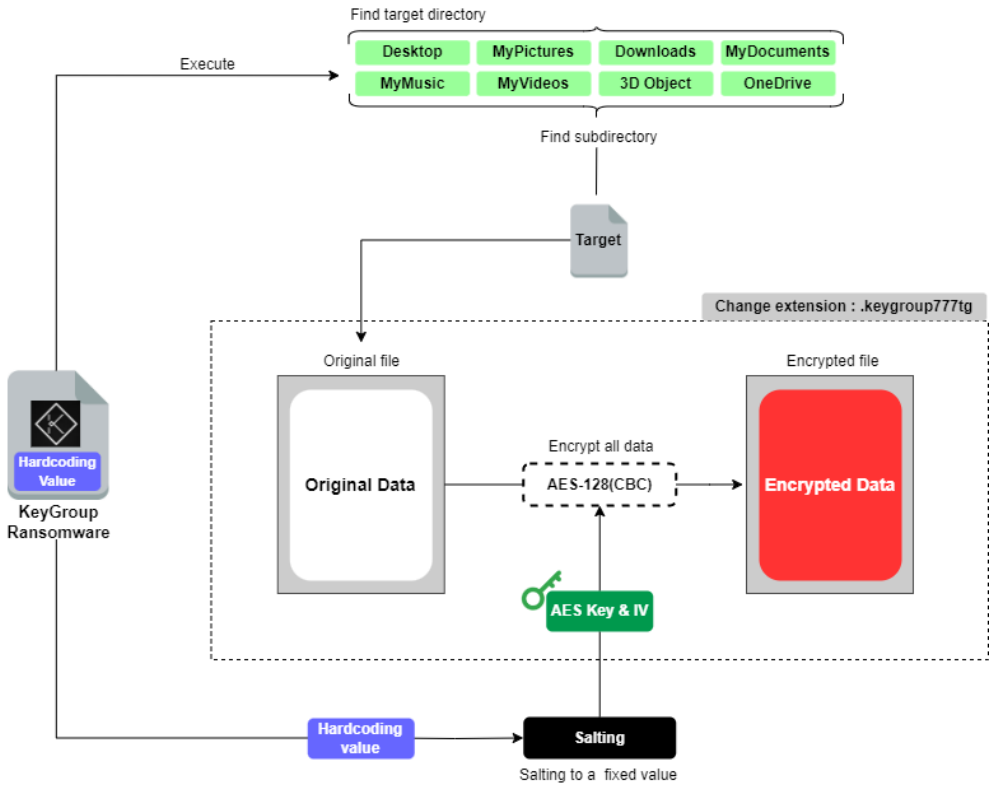


Figure 5. Feature of the KeyGroup ransomware

- The ransomware was discovered on September 14, 2023, and as a ransomware used by KeyGroup, it was confirmed to be a variant of the PoliceRecords ransomware discovered around May 2022.
- All files included in specified folders, such as Desktop, MyPictures, MyMusic, MyVideos, Program Files, and Program Files (x86), are encrypted, and the .keygroup777tg extension is added to the encrypted files.
- The AES-128 (CBC) algorithm is used to encrypt files. The key used at this time is created by applying unicode encoding to the fixed value stored internally, and the key and initial vector use the same value.
- After encryption is performed, the FilterAdministratorToken, EnableLUA, DisableTaskMgr, and DisableRegistryTools values in the SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩System registry to prevent access to the UAC (user account control), task manager, and registry change function.

2) Decryption method

The KeyGroup ransomware applies unicode encoding to a fixed value to generate a key and initial vector to be used in the AES-128 algorithm. In general, high-quality ransomware generates a random key and initial vector value for each file and uses them for file encryption, and uses a hybrid encryption technique, i.e. using an asymmetric key algorithm to protect the key. However, this ransomware encrypted all files after using a fixed value to generate the key value, and as the key was not protected, the files could be decrypted.

Date of discovery	Key value encryption Y/N	Variant
23/08/30	O	Xorist
23/01/06 ~ 23/06/24	O	HiddenTear/Chaos
23/08/03	X	HiddenTear/Chaos
23/08/28	O	Anabelle
23/09/07	O	RURansom
23/09/14	X	PoliceRecords
23/09/19	O	Cyborg
23/09/25	O	UxCryptor

Table 1. Ransomwares used by KeyGroup

Looking at [Table 1], in most of the ransomwares used by KeyGroup, the keys used for encryption were protected through the hybrid encryption technique, but the key was not protected only in the samples discovered on August 3 and September 14, which suggests that the attacker made a mistake in the process of making the ransomware. It is assumed that a mistake was made. In [Table 1], the sample discovered on August 3 disclosed the script in Eclecticiq.

The decryptable sample confirmed by the Ransomware Response Center of SK Shieldus is the sample discovered on September 14. This KeyGroup ransomware was confirmed to be a variant of the PoliceRecords ransomware discovered around May 2022, and it was confirmed that some variants of the PoliceRecords ransomware can be decrypted.

filename	MD5
Police_Records.exe	00d77230603c745c638c5de737d1593e
Police_Records.exe	d7a7df59b8979b97d547972b307a4740
RubberDucky.exe	7C3EADFECFE56137704664A9CBED3544

Table 2. Decryptable ransomware

If the extension of the encrypted file is .CRYPT, or .keygroup777tg, or the name of the ransom note is FAQ.txt or Rubber_Decrypt0r.txt, you can try decryption through the script below. If it is the same as shown in [Table 2], you can use the following script to decrypt it.

```
import pip
import os
import subprocess

print("Download moudles for decrypt")
pip.main(['install','requests'])
pip.main(['install','pycryptodome'])
pip.main(['install','dnfile'])
pip.main(['install','dncil'])
import requests
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

# Download Script(Open source by Mandiant)
def DownloadScript():
    url =
'https://raw.githubusercontent.com/mandiant/dncil/main/scripts/print_cil_from_dn_file.py'
    res = requests.get(url)
    with open('print_cil_from_dn_file.py','w') as f:
        f.write(res.text)

def ExecuteScript(RansomwareFileName):
    result = subprocess.run(f'print_cil_from_dn_file.py {RansomwareFileName} >>
dis.txt',shell=True)

def GetRansomwareFileName():
    RansomwarefileName = input('Input the ransomware sample file name(Full path): ')
    return RansomwarefileName

def FindKey():
    file_path = "dis.txt"
    target_string_1 = "Method: EncryptFile"
    target_string_2 = "nop"
    target_string_3 = "ldstr"

    try:
        with open(file_path, "r") as file:
            lines = file.readlines()
            for i in range(len(lines)):
                if target_string_1 in lines[i]:
                    if target_string_2 in lines[i+1] and target_string_2 in lines[i+2]:
                        if target_string_3 in lines[i+3]:
                            keysource_line = lines[i+3].strip()
                            keysource = keysource_line.split('"')[1]
```

```
                        print("keysource is exist :", keysource)
                        break

    except FileNotFoundError:
        print(f"Cannot found '{file_path}'.")
        exit()
    except Exception as e:
        print(f"Error : {e}")
        exit()

    # Check key length
    if len(keysource)==0:
        print("Key not found")
        exit()

    elif len(keysource)!=8 & len(keysource)!=16 :
        print("Key length is incorrect")
        exit()

    # Unicode encode
    array = bytearray()
    for i in keysource:
        array.append(ord(i))
        array.append(0x00)

    # Get key, IV
    key = array
    iv = array
    print('Key : %s IV : %s'%(key,iv))

    return key,iv

# AES decrypt func
def DecryptFile(file_path,key,iv):

    try:
        with open(file_path, 'rb') as file:
            ciphertext = file.read()
            cipher = AES.new(key, AES.MODE_CBC, iv)
            decrypted_data = unpad(cipher.decrypt(ciphertext), AES.block_size)
        with open(file_path, 'wb') as file:
            file.write(decrypted_data)
        print(f'Decrypted: {file_path}')
```

```
        # Remove encrypted extensions
        decrypted_file_path = os.path.splitext(file_path)[0]

        # Verify that the same file already exists
        while os.path.exists(decrypted_file_path):
            decrypted_file_path += '_copy'
        os.rename(file_path, decrypted_file_path)
        print(f'Renamed to: {decrypted_file_path}')

    except Exception as e:
        print(f'Error decrypting {file_path}: {e}')

# Travel directory
def TravelDirectory(Directory,Extension,key,iv):
    for foldername, subfolders, filenames in os.walk(Directory):
        for filename in filenames:
            if filename.endswith(Extension):
                file_path = os.path.join(foldername, filename)
                if os.path.exists(file_path) and os.path.getsize(file_path)==0:
                    os.remove(file_path)
                    continue
                DecryptFile(file_path,key,iv)

def GetExtension():
    Extension = input('Input the encrypted extension(without comma): ')
    return '.' + Extension

def GetStartDirectory():
    start_directory = input('Input the start directory(without :\\\\): ')
    return start_directory+':\\'

if __name__ == "__main__":
    DownloadScript()
    ExecuteScript(GetRansomwareFileName())
    key, iv = FindKey()
    TravelDirectory(GetStartDirectory(),GetExtension(),key,iv)
```

Script 1. Decryption script

3) IoC

MD5	00d77230603c745c638c5de737d1593e d7a7df59b8979b97d547972b307a4740 7C3EADFECFE56137704664A9CBED3544
File name	Police_Records.exe RubberDucky.exe

2. new RaaS, NoBit ransomware

Figure 6. Recently publicized RaaS ransomware

RaaS ransomwares are mushrooming in invisible places. They are mainly active on Telegram and the dark web, recruiting members and generating revenues. In July, a RaaS ransomware called NoBit appeared on Telegram and the dark web. They introduced the NoBit ransomware as the next-generation ransomware and they are advertising it while emphasizing fast encryption, the function to detect the languages (Korean, English, etc.) in use on the target PC, ease of use, etc. As it is not much different from existing RaaS ransomware, and some samples with exposed hashes can be decrypted, however, doubts are raised about the claim that it is a next-generation ransomware. Currently, the NoBit ransomware builder sells for $200 (KRW270,000), and the entire source codes of the ransomware are traded at around $1000 (KRW1,350,000).

The NoBit ransomware builder has advantages: that is, attackers can easily customize it as it provides various functions such as setting AES-128 key values, modifying ransom notes, changing the displayed ransom amount, stopping encryption when a specific language is used, and specifying extensions to be encrypted. These RaaS ransomwares have a major problem: i.e. even people without hacking expertise can use it by simply paying for it.

1) Feature

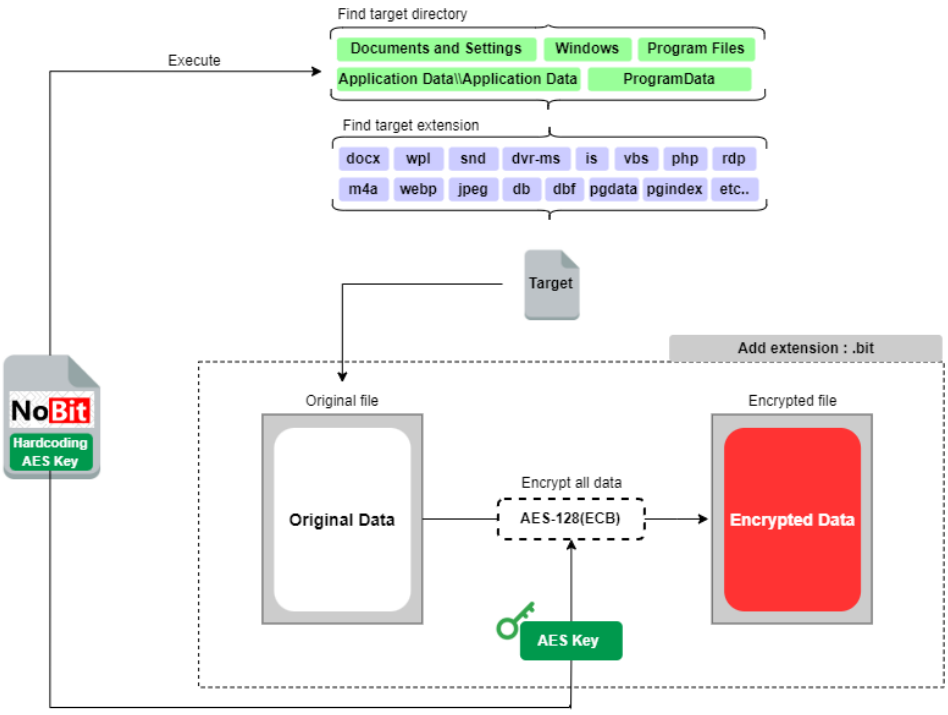


Figure 7. NoBit ransomware Feature

- VSS[10] is deleted for the purpose of interfering with system recovery.
- In the case of directories related to PC execution, such as Documents and Settings, Windows, Program Files, and ProgramData, the files are not encrypted. Additionally, the extension of the file is checked and the file is encrypted only if it matches a specified extension such as docx, wpl, snd, or vbs.
- The AES-128 (ECB mode) algorithm is used for data encryption, and the key value used at this time is hard coded inside the ransomware. For encrypted files, the .bit extension is added to the end of the existing filename.
- Once file encryption is complete, the desktop is changed using the bitmap file stored inside the ransomware. Then, the Decryptor.exe file is created in the desktop path and executed. The file displays the contents of the ransom note and has a function to decrypt the file by receiving the key used for encryption as input.
- The destruct.bat file is created in %Temp% path and executed. The batch file has a function to delete ransomware.

10 VSS: It's short for Volume Shadow Copy. It is a copy or snapshot at a specific point in time.

2) Decryption method

The NoBit ransomware encrypts data with the AES algorithm using a 128-bit key stored inside the file. At this time, the key used for encryption is the same for each file, and decryption is possible because the key value is not protected. However, because NoBit ransomware deletes itself after performing file encryption, it is necessary to secure a hash or sample through investigation of infringement incidents. If the hash is as shown in the table below, file decryption is possible with the matching key value. If the hash is not in the table, file decryption is possible through the key value present in the resource data of the secured sample.

Filename	MD5	Key value (text)
Botnet Virus Remover.exe	cad2d5524d0f66bb1017e206d28d2452	FF2934E360B2F1E6
try.exe	27c00e46185d476e33961c676f07774c	F60074D9D3F5EA5E
232464727	b10033b91ab6d47547871dfe361272bb	6CDF3A165152908D

Table 1. NoBit ransomware

If infected with the NoBit ransomware, you must check whether the ransomware used in the attack matches the hash in [Table 3] or secure an actual sample of the ransomware. If it matches the hash in [Table 3], run the decryption script, and enter the key value corresponding to the hash value and perform decryption.

If the hash of the sample does not exist in [Table 3], you must use the .NET decompile tool such as JetBrains' DotPeek or DnSPy, an open source tool. As the NoBit ransomware stores the key used for encryption in the form of a resource named "key," you can perform decryption by finding the resource data, securing the key value, and then executing the decryption script.

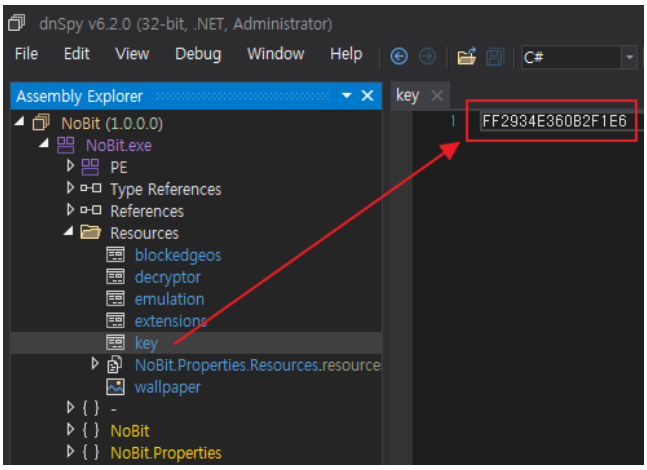


Figure 2. NoBit ransomware key path

```python
import os
import pip
import winreg
pip.main(['install','pycryptodome'])
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

def SetWallpaper():
    regpath = r"Control Panel\Desktop"
    name = "Wallpaper"
    value = r"c:\windows\web\wallpaper\windows\img0.jpg"
    try:
        regkey = winreg.OpenKey(winreg.HKEY_CURRENT_USER, regpath, 0,
                                    winreg.KEY_SET_VALUE)
        winreg.SetValueEx(regkey, name, 0, winreg.REG_SZ, value)
        winreg.CloseKey(regkey)
        return True
    except WindowsError:
        return False

# Get AES Key
def GetKey():
    key = bytes(input('Input the AES Key(in text) : '),'utf-8')
    return key

# AES decrypt
def decrypt_aes(ciphertext, key):
    cipher = AES.new(key, AES.MODE_ECB)
    plaintext = unpad(cipher.decrypt(ciphertext), AES.block_size)
    return plaintext

# Find and decrypt .bit files in a directory
def decrypt_bit_files(directory,key):
    for foldername, subfolders, filenames in os.walk(directory):
        for filename in filenames:
            if filename.endswith('.bit'):
                file_path = os.path.join(foldername, filename)
                with open(file_path, 'rb') as file:
                    encrypted_data = file.read()
                    decrypted_data = decrypt_aes(encrypted_data, key)
                # Create a filenmae with the .bit extension removed
                new_filename = os.path.splitext(filename)[0]
                new_file_path = os.path.join(foldername, new_filename)
                with open(new_file_path, 'wb') as file:
```

```
                    file.write(decrypted_data)
                # Delete an existing .bit file
                os.remove(file_path)
                print(f'Decrypted and renamed: {new_file_path}')

# Setting the start directory
def GetStartDirectory():
    start_directory = input('Input the start directory(without :\\\\) : ')
    return start_directory + ':\\'

# Main function
if __name__ == "__main__":
    decrypt_bit_files(GetStartDirectory(),GetKey())
    SetWallpaper()
    print('decrypt done')
```

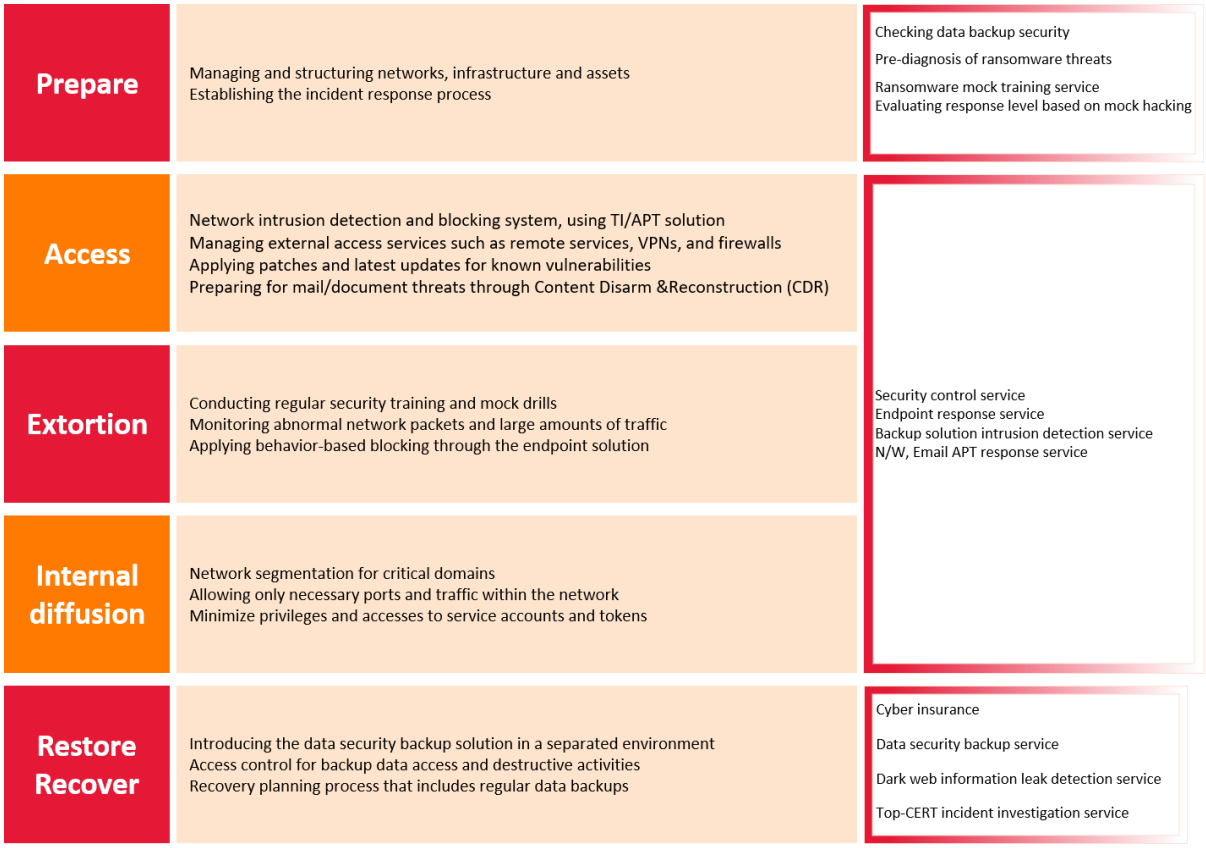
Script 2. Decryption script

3) IoC

MD5	cad2d5524d0f66bb1017e206d28d2452 27c00e46185d476e33961c676f07774c b10033b91ab6d47547871dfe361272bb
File name	Botnet Virus Remover.exe try.exe 232464727

Ransomware mitigations

The Ransomware Response Center of SK Shieldus analyzed in detail two types of decryptable ransomwares, i.e. KeyGroup and NoBit, through the 3rd quarter ransomware trend report and distributed decryption scripts. These ransomwares encrypt the hash file using a key value hard coded inside the file, and do not protect the key. So hash file decryption is possible only when a sample or sample hash exists. As ransomware groups use a double extortion strategy, i.e. not only encrypting files but also stealing data and demanding money, however, in order to prevent damage, it is necessary to be ready for targeted APT attacks and prepare security elements and processes appropriate at each stage, and detect and block intrusions before attacker groups achieve their goals.



Technology for Everyday Safety | SK shieldus

23, Pangyo-ro 227beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea
https://www.skshieldus.com

Publisher : SK shieldus EQST Business Group & KARA (Korea Anti Ransomware Alliance)
Producer : SK shieldus Communication Group