New Nokoyawa Ransomware Possibly Related to Hive

: 9-3-2022

In March 2022, we came across evidence that another, relatively unknown, ransomware known as Nokoyawa is likely connected with Hive, as the two families share some striking similarities in their attack chain, from the tools used to the order in which they execute various steps.

By: Don Ovid Ladores, Ian Kenefick March 09, 2022

Hive, which is one of the more notable ransomware families of 2021, made waves in the latter half of the year after breaching over 300 organizations in just four months — allowing the group to earn what could potentially be millions of US dollars in profit. In March 2022, we came across evidence that another, relatively unknown, ransomware known as Nokoyawa is likely connected with Hive, as the two families share some striking similarities in their attack chain, from the tools used to the order in which they execute various steps. Currently, the majority of Nokoyawa's targets are located in South America, primarily in Argentina.

Attack chain similarities and differences

Some of the indicators we've observed being shared by both Nokoyawa and Hive include the use of Cobalt Strike as part of the arrival phase of the attack, as well as the use of legitimate, but commonly abused, tools such as the anti-rootkit scanners GMER and PC Hunter for defense evasion. Other steps, such as information gathering and lateral deployment, are also similar.

The operators of the Hive ransomware are known to use other tools — such as NirSoft and MalXMR miner — to enhance their attack capabilities depending on the victim environment. Based on our analysis, Nokoyawa also does the same thing based on its victims. We've observed the ransomware leverage other tools such as. Mimikatz, Z0Miner, and Boxter

We also found evidence based on one of the IP addresses used by Nokoyawa that the two ransomware families share the same infrastructure.

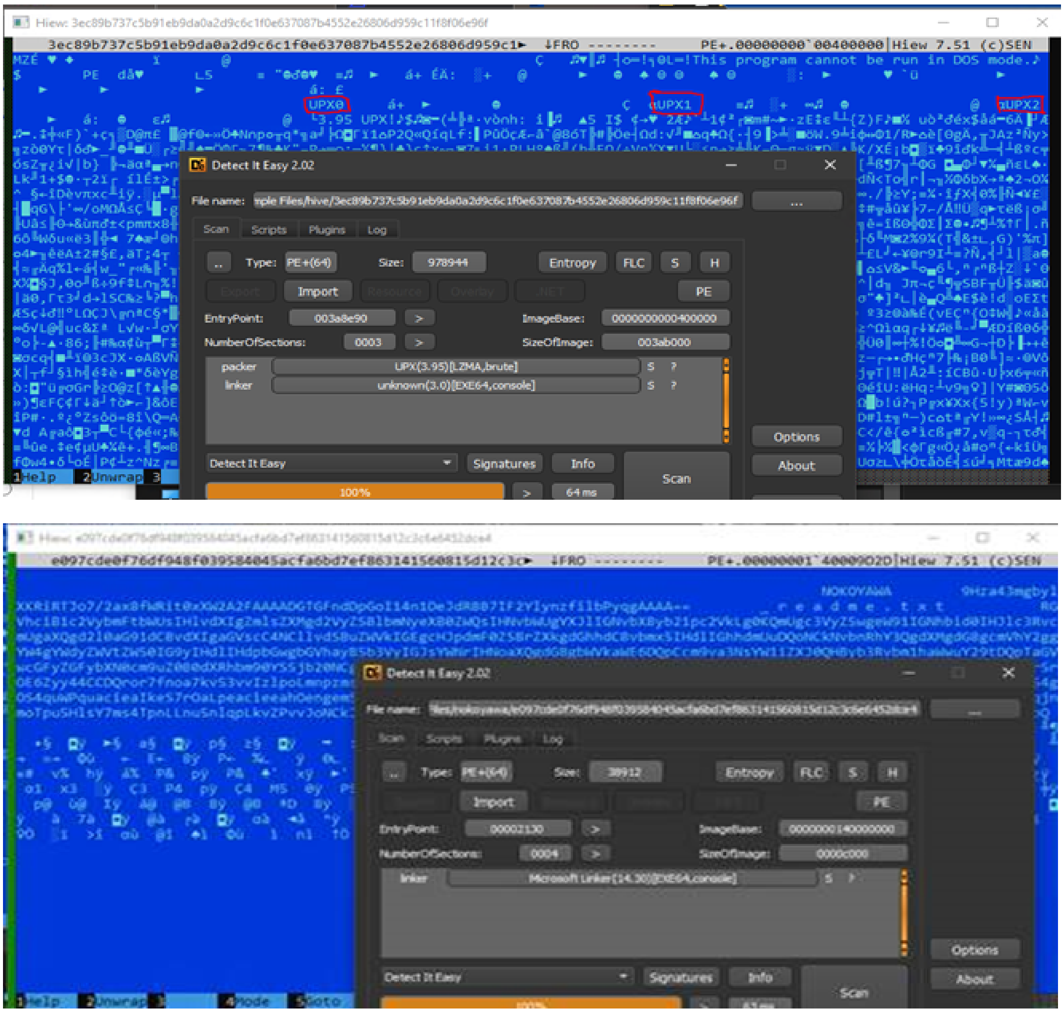
Although we are not certain how Nokoyawa is delivered to its victims, given the similarities with Hive, it's likely that it uses similar methods such as phishing emails for arrival.

Indicator	Hive	Nokoyawa
Cobalt Strike (arrival)	Yes	Yes
Coroxy malware (deployment of PowerShell commands and scripts)	Other researchers have flagged this malware as being related to Hive, though we have not confirmed this ourselves	Yes
GMER (defense evasion)	Yes	Yes
PC Hunter (info gathering and defense evasion)	Yes	Yes
PowerShell Scripts (info gathering)	Yes	Yes
PsExec (lateral deployment of Ransomware)	Yes	Yes
Filename for Ransom Payload (xxx.exe)	Yes	Yes

Table 1. Similarities in the attack chain of Hive and Nokoyawa

Taking each individual step into account, the similarities might not seem as apparent — for example, Cobalt Strike is a very popular post exploitation tool that has been used by other ransomware gangs — but when taking the whole picture into account, it's clear to see that the two ransomware families are connected.

Despite their similarities, the two ransomware families still have a few differences. For example, the majority of the Hive ransomware variants that we have observed were packed using UPX, while the Nokoyawa sample we analyzed did not use any packer for the binary sample, leaving strings from the file bare and easy to analyze.



Hiew: 3ec89b737c5b91eb9da0a2d9c6c1f0e637087b4552e26806d959c11f8f06e96f

Detect It Easy 2.02

File name: mple Files/hive/3ec89b737c5b91eb9da0a2d9c6c1f0e637087b4552e26806d959c11f8f06e96f

Type: PE+(64)
Size: 978944
EntryPoint: 003a8e90
ImageBase: 0000000000400000
NumberOfSections: 0003
SizeOfImage: 003ab000
packer: UPX(3.95)[LZMA,brute]
linker: unknown(3.0)[EXE64,console]

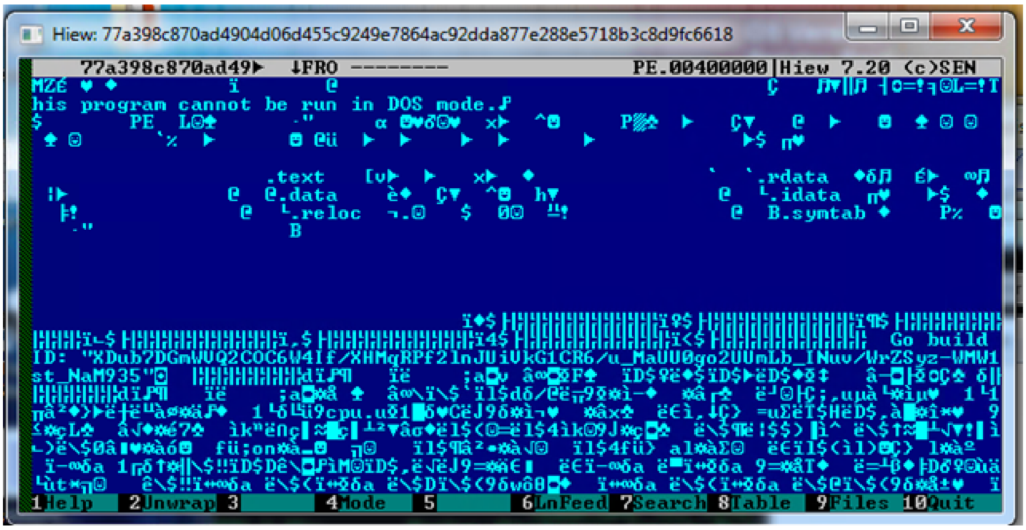
Detect It Easy 2.02

File name: files/nokoyawa/e097cde0f76df948f039584045acfa6bd7ef863141560815d12c3c6e6452dca4

Type: PE+(64)
Size: 38912
EntryPoint: 00002130
ImageBase: 0000000140000000
NumberOfSections: 0004
SizeOfImage: 0000c000
linker: Microsoft Linker(14.30)[EXE64,console]

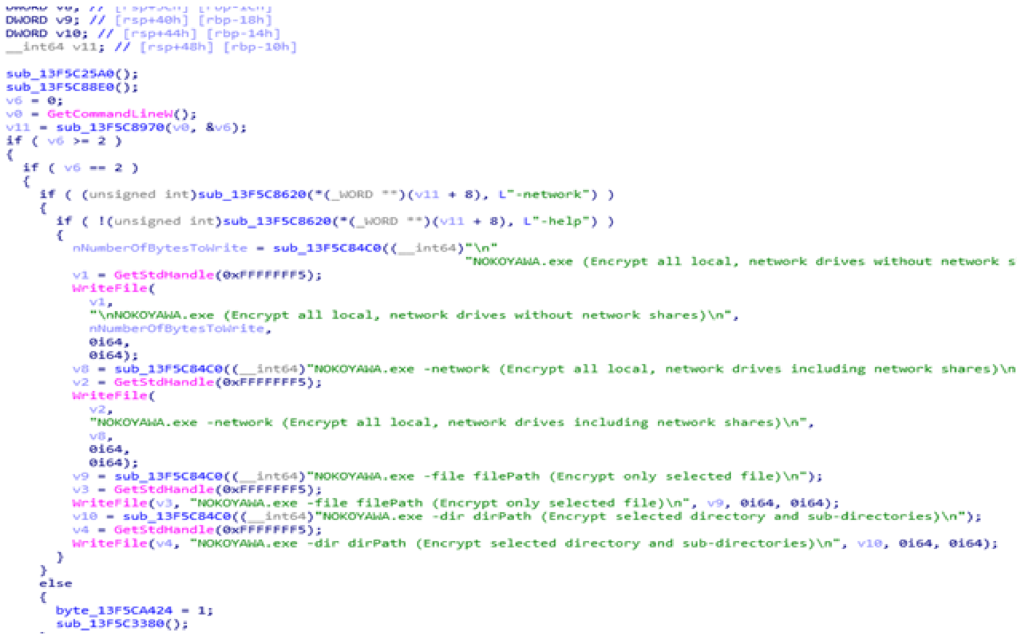
Figure 1. A Hive variant packed using UPX compared to the Nokoyawa sample we analyzed

Another difference is in the compiler — Hive's binary was compiled using GoLang script, while Nokoyawa uses another language to compile its binary, again making it easier to disassemble and analyze.



Hiew: 77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618

```
77a398c870ad49►  ↓FRO --------          PE.00400000|Hiew 7.20 (c)SEN
his program cannot be run in DOS mode.
.text  .data  .reloc  .rdata  .idata  B.symtab
Go build ID: "XDub7DGmWUQ2COC6W4If/XHMqRPf21nJUiUkG1CR6/u_MaUU0go2UUmLb_INuv/WrZSyz-WMW1st_NaM935"
```



```
DWORD v8; // [rsp+3Ch] [rbp-1Ch]
DWORD v9; // [rsp+40h] [rbp-18h]
DWORD v10; // [rsp+44h] [rbp-14h]
__int64 v11; // [rsp+48h] [rbp-10h]

sub_13F5C25A0();
sub_13F5C88E0();
v6 = 0;
v0 = GetCommandLineW();
v11 = sub_13F5C8970(v0, &v6);
if ( v6 >= 2 )
{
  if ( v6 == 2 )
  {
    if ( (unsigned int)sub_13F5C8620(*(_WORD **)(v11 + 8), L"-network") )
    {
      if ( !(unsigned int)sub_13F5C8620(*(_WORD **)(v11 + 8), L"-help") )
      {
        nNumberOfBytesToWrite = sub_13F5C84C0((__int64)"\n"
                                                         "NOKOYAWA.exe (Encrypt all local, network drives without network s
        v1 = GetStdHandle(0xFFFFFFF5);
        WriteFile(
          v1,
          "\nNOKOYAWA.exe (Encrypt all local, network drives without network shares)\n",
          nNumberOfBytesToWrite,
          0i64,
          0i64);
        v8 = sub_13F5C84C0((__int64)"NOKOYAWA.exe -network (Encrypt all local, network drives including network shares)\n
        v2 = GetStdHandle(0xFFFFFFF5);
        WriteFile(
          v2,
          "NOKOYAWA.exe -network (Encrypt all local, network drives including network shares)\n",
          v8,
          0i64,
          0i64);
        v9 = sub_13F5C84C0((__int64)"NOKOYAWA.exe -file filePath (Encrypt only selected file)\n");
        v3 = GetStdHandle(0xFFFFFFF5);
        WriteFile(v3, "NOKOYAWA.exe -file filePath (Encrypt only selected file)\n", v9, 0i64, 0i64);
        v10 = sub_13F5C84C0((__int64)"NOKOYAWA.exe -dir dirPath (Encrypt selected directory and sub-directories)\n");
        v4 = GetStdHandle(0xFFFFFFF5);
        WriteFile(v4, "NOKOYAWA.exe -dir dirPath (Encrypt selected directory and sub-directories)\n", v10, 0i64, 0i64);
      }
    }
    else
    {
      byte_13F5CA424 = 1;
      sub_13F5C3380();
```

Figure 2. Comparing the compilers of Hive (top) and Nokoyawa (bottom)

The third difference is in the encryption routine. Hive generates a random key to be used for the encryption process based on RTLGenRandom API, which will be initially saved in memory. This key is then used through what seems to be a custom encryption implementation to encrypt the files. The key is then also encrypted using RSA via GoLang's implementation of RSA encryption, which it accomplishes using a list of public keys embedded in the binary and the saved as <random>.key.<extension> on the encrypted drive. Finally, the generated key will be wiped from memory so that the encrypted key will be the only copy of the key used for decryption.

In contrast, Nokoyawa ransomware generates a random key to be used for the encryption process using the BCryptGenRandom API. Each value is created for each file. It uses a hardcoded nonce for the encryption, "lvcelcve" and Salsa to encrypt the files, which is generated for every file. Then, it will encrypt the key using ECDH key pair.

What the information gathered implies is that the Hive ransomware's operators have likely begun using another ransomware family — perhaps as a new Ransomware-as-a-Service (RaaS) operation. It's also possible that they are using the same infection chain as before, but with a different ransomware payload.

Note that we have not found any evidence that Nokoyawa has been using the double extortion technique — where the ransomware operator threatens to release critical information on a leak site in addition to encoding files — unlike Hive, which has been found to be integrating it in its attacks.

Defending against ransomware attacks

Ransomware is one of the most destructive malware types in the wild today due to its ability to compromise and leak critical data. Therefore, organizations should ensure that their information is as safe as possible from ransomware attacks. These security recommendations can help maximize their security implementation with relatively little costs:

- Enabling multifactor authentication can prevent malicious actors from compromising user accounts as part of their infiltration process.
- Users should be wary of opening unverified emails. Embedded links should never be clicked and attached files should never be opened without the proper precautions and verification as these can kickstart the ransomware installation process.
- Organizations should always adhere to the 3-2-1 rule: Create three backup copies on two different file formats, with one of the backups in a separate location.
- Patching and updating software and other systems at the soonest possible time can minimize the chance of a successful vulnerability exploitation that can lead down the road to a ransomware infection.
- Organizations can better protect themselves from ransomware attacks if they implement multilayered security setups that combine elements such as the automated detection of files and other indicators with constant monitoring for the presence of weaponized legitimate tools in their IT environment.

Correlating two different attacks, such as the one we’ve done in this blog entry with Hive and Nokoyawa, are made much easier with multilayered detection and response solutions such as Trend Micro Vision One™, which is a purpose-built threat defense platform that provides added value and new benefits beyond extended detection and response (XDR) solutions. This technology provides powerful XDR capabilities that collect and automatically correlate data across multiple security layers — email, endpoints, servers, cloud workloads, and networks — to prevent attacks via automated protection while also ensuring that no significant incidents go unnoticed.

Indicators of Compromise

URLs

- hxxp://185.150.117[.]186:80/asdfgsdhsdfgsdfg (Cobalt Strike download)

SHA256

Malware	**SHA256**	**Detection**
Exploit Agent	a70729b3241154d81f2fff506e5434be0a0c381354a84317958327970a125507	Trojan.Win64.NEKTO.YACCA
Coroxy Dropper	2ef9a4f7d054b570ea6d6ae704602b57e27dee15f47c53decb16f1ed0d949187	Trojan.Win32.COROXY.SMY
Coroxy	c170717a69847bb7b050832c55fcd2a214e9180c8cde5f86088bd4e5266e2fd9	Backdoor.Win64.COROXY.YA
DataSpy	a290ce75c6c6b37af077b72dc9c2c347a2eede4fafa6551387fa8469539409c7	TrojanSpy.PS1.DATASPY.B
Nokoyawa	e097cde0f76df948f039584045acfa6bd7ef863141560815d12c3c6e6452dce4	Ransom.Win64.NOKO.YACB