Nokoyawa is a new Windows ransomware that appeared earlier this year. The earliest samples collected by FortiGuard researchers were compiled in February 2022 and share substantial code similarities with Karma, another ransomware that traces its lineage to Nemty through a long string of variants. Nemty is a ransomware family that FortiGuard Labs researchers reported on back in 2019.

Recently, FortiGuard Labs encountered a new variant of this ransomware campaign and observed that it has been improving itself by reusing code from publicly available sources. In this article, we discuss the general behavior of Nokoyawa Ransomware as well as the new features it recently added to maximize the number of files that can be encrypted.

Affected Platforms: Windows Impacted Parties: Windows users Impact: Potential loss of files Severity Level: Medium

Nokoyawa Ransomware Overview

A general overview of how Nokoyawa works is provided here to avoid rehashing information previously presented by other researchers. Links to prior research can be referenced near the bottom of this article.

Curiously, unlike its alleged ransomware predecessor Karma, that runs on both 32-bit and 64-bit Windows, FortiGuard Labs has only observed samples compiled to run exclusively on 64-bit Windows.

Nokoyawa provides several command line options for customized executions:

- -help: Print the list of command line options
- -network: Encrypt files on all drives and volumes (both local and networked)
- -file filePath: Encrypt a single file
- -dir dirPath: Encrypt all files in specified directory and sub-directories

If no argument is provided, Nokoyawa encrypts all local drives and volumes by default. The "-help" argument is interesting as it suggests that the ransomware developers might be a separate team from the operators deploying and executing the ransomware on infected machines.

For speed and efficiency, Nokoyawa creates multiple threads for encrypting files that do not end with .exe, .dll, or .lnk extensions. Files with NOKOYAWA in their names are also skipped. In addition, some directories and their sub-directories are excluded from encryption by comparing the hash of their names with a list of hardcoded hashes.

For each sample, the ransomware operators generate a fresh pair of Elliptic-Curve Cryptography (ECC) public and private keys (aka keypair) and then embed the public key into the ransomware binary. This pair of keys can be considered as "master" keys necessary for decrypting the files upon ransom payment. Assuming that each sample is deployed for a different victim, the ransomware operators eliminate the possibility of victims using a decryptor provided to another victim since each victim is linked to a separate "master" keypair.

Before encrypting each file, Nokoyawa creates a new ephemeral keypair (victim file keys) unique to each file. Using the victim file's private key and the "master" public key from the threat actors, a 64-byte shared secret is generated with Elliptic-Curve Diffie-Hellmann (ECDH). The first 32 bytes of this shared secret are used as a Salsa20 key together with the hardcoded nonce 'lvcelvce' for encrypting the contents of each file.

A SHA1 hash is generated based on the previously generated shared secret and the file content and is appended at the end of each encrypted file together with the victim file's public key and the string "NOKOYAWA". This hash is likely to be used for checking data integrity during decryption.

Consequently, the victim file's public key and the "master" private key owned by the ransomware operator are required to regenerate the Salsa20 key for decrypting each encrypted file.

Files encrypted by the ransomware are appended with a .NOKOYAWA extension. The ransom note is written into NOKOYAWA_readme.txt in every directory included for encryption.

Ransomware Development Cheat Codes

The April 2022 samples we collected contain three new features to maximize the number of files that can be encrypted by Nokoyawa. These features were already present in contemporary ransomware families and their addition simply suggests an attempt by Nokoyawa developers to catch up with other operators in terms of technical capabilities.

FortiGuard Labs researchers were able to determine that most of the added code was copied verbatim from publicly available sources, including the source of the now-defunct Babuk ransomware leaked in September 2021.

One example of such blatant copying is the inclusion of functions to terminate processes and services to reduce the number of files locked by other programs so the encryption code can encrypt those files. The code (including the list of processes and service names) exactly matches the implementation in Babuk. The image in Figure 1 shows a side-by-side comparison of the service killer functions taken from Babuk's leaked source code (left) and Nokoyawa's decompiled code (right).

Figure 1. Service killer functions from Babuk and Nokoyawa

The applications and services impacted by Nokoyawa include Microsoft Office applications, email clients, browsers, backup programs, security products, and database servers. Please refer to Appendix A for a complete list of the affected processes and services.

It also includes code to enumerate and mount volumes to encrypt the files on these volumes, again reusing the exact code copied from the leaked Babuk source.

In the latest samples we collected, it deletes volume snapshots by resizing the allocated space for snapshots of volume shadow copies to 1 byte via the DeviceIoControl API using the IOCTL_VOLSNAP_SET_MAX_DIFF_AREA_SIZE (0x53c028) control code. This size would be too small to store snapshots, resulting in Windows deleting them. This technique was previously reported by Fortinet and the implementation appears to be copied from a publicly available PoC. Previous samples did not delete volume shadow copies.

For the above functionality to operate correctly, administrator privileges are required. Since we did not observe any Windows User Access Control (UAC) bypass being performed by the sample, it is likely that the operators use other means to escalate or obtain administrative privileges prior to executing the ransomware.

New Ransom Note with Onion URL

The ransom note and the way victims communicate with the perpetrators have also undergone a major change in the new variants.

In the older samples from February, victims were instructed to contact the ransomware operators via email, as shown in Figure 2.

Figure 2. Previous ransomware note with redacted emails

In the Apr 2022 samples, however, the email addresses were removed. They were replaced with instructions to contact the ransomware operators through a .onion URL via a TOR browser. Each sample uses the same .onion domain in the ransom notes but the id parameter, which we presume to be the victim identifier, is unique for each sample (Figure 3).

Figure 3. New ransomware note with the Onion URL

New Ransom Payment Page

Visiting the Onion URL leads to a page with an online chat box for communicating with the operators for negotiating and paying the ransom. FortiGuard Labs researchers observed an ongoing conversation between a possible victim (Company) and the ransomware operator (User). Based on this chat history, the threat actors offer free decryption of up to 3 files to prove that they can decrypt the victim's files (Figure 4).

Figure 4. New payment page with chat box

The "Instructions" page shows the ransom amount, in this case a hefty 1,500,000 (presumably in USD), that could be paid in either BTC (Bitcoin) or XMR (Monero). After payment, the operators claim to provide the tool to decrypt the victim's files (Figure 5).

Figure 5. Ransom payment instruction page

Given the increasing professionalization of some ransomware campaigns, this TOR website may be an attempt to improve "branding" or it may be a way to have a separate team handle ransom negotiations.

Oddly enough, the ransom note includes the following message "Contact us to reach an agreement or we will leak your black s**t to media," which suggests that the victim's data might have been exfiltrated during the infection. However, FortiGuard Labs researchers did not find such capabilities in the Nokoyawa samples. In fact, apart from the enumeration of networked drives, no network-related behaviors were observed at all. It may be possible that data exfiltration is performed separately by the operators, or they might be bluffing to further pressure victims into paying the ransom.

Conclusion

In this article, we highlighted the improvements that have been made to the new variant of Nokoyawa Ransomware. It also shows how threat actors can quickly add new capabilities to their malware with minimal effort by reusing publicly available code.

FortiGuard Labs will continue to monitor Nokoyawa and emerging trends in the ransomware threat landscape.

Fortinet Protections

The FortiGuard Antivirus service detects and blocks this threat as W64/Filecoder.EV!tr.

Fortinet customers are protected from this malware through FortiGuard's Web Filtering, Antivirus, and CDR (content disarm and reconstruction) services and FortiMail, FortiClient, and FortiEDR solutions.

Due to the ease of disruption, damage to daily operations, potential impact to the reputation of an organization, and the unwanted destruction or release of personally identifiable information (PII), etc., it is important to keep all AV and IPS signatures up to date.

Since the majority of ransomware is delivered via phishing, organizations should consider leveraging the Fortinet solutions designed to train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

We also suggest that organizations have their end users go through our free NSE training: NSE 1 — Information Security Awareness. It includes a module on Internet threats that is designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

IOCs

Files (SHA256)

A32b7e40fc353fd2f13307d8bfe1c7c634c8c897b80e72a9872baa9a1da08c46

304e01db6da020fc1e0e02fdaccd60467a9e01579f246a8846dcfc33c1a959f8

The existence of the following files might also indicate an infection:

- NOKOYAWA_readme.txt
- Filenames with ".NOKOYAWA" extension

References

- https://www.sentinelone.com/labs/nokoyawa-ransomware-new-karma-nemty-variant-wears-thin-disguise
- https://www.trendmicro.com/en_us/research/22/c/nokoyawa-ransomware-possibly-related-to-hive-.html
- https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/
- https://securelist.com/evolution-of-jsworm-ransomware/102428/

Appendix A

List of process names

- sql.exe
- oracle.exe
- ocssd.exe
- dbsnmp.exe
- synctime.exe
- agntsvc.exe
- isqlplussvc.exe
- xfssvccon.exe

- mydesktopservice.exe
- ocautoupds.exe
- encsvc.exe
- firefox.exe
- tbirdconfig.exe
- mydesktopqos.exe
- ocomm.exe
- dbeng50.exe
- sqbcoreservice.exe
- excel.exe
- infopath.exe
- msaccess.exe
- mspub.exe
- onenote.exe
- outlook.exe
- powerpnt.exe
- steam.exe
- thebat.exe
- thunderbird.exe
- visio.exe
- winword.exe
- wordpad.exe
- notepad.exe

List of service names

- vss
- sql
- svc$
- memtas
- mepocs
- sophos
- veeam
- backup
- GxVss
- GxBlr
- GxFWD
- GxCVD
- GxCIMgr
- DefWatch
- ccEvtMgr
- ccSetMgr
- SavRoam
- RTVscan
- QBFCService
- QBIDPService
- Intuit.QuickBooks.FCS
- QBCFMonitorService
- YooBackup
- YooIT
- zhudongfangyu
- sophos
- stc_raw_agent

- VSNAPVSS
- VeeamTransportSvc
- VeeamDeploymentService
- VeeamNFSSvc
- veeam
- PDVFSService
- BackupExecVSSProvider
- BackupExecAgentAccelerator
- BackupExecAgentBrowser
- BackupExecDiveciMediaService
- BackupExecJobEngine
- BackupExecManagementService
- BackupExecRPCService
- AcrSch2Svc
- AcronisAgent
- CASAD2DWebSvc
- CAARCUpdateSvc

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.