Flash Report: Colossus Ransomware

zerofox.com/blog/flash-report-colossus-ransomware/

September 24, 2021

BLOG

September 24, 2021 | by ZeroFox Research

6 minute read

On Friday, September 24, 2021, the ZeroFox Threat Intelligence team discovered a variant of ransomware called Colossus that affects machines running Microsoft Windows operating systems. The sample has a number of features including binary packing via Themida and sandbox evasion capabilities. The ransomware has a support website for setting up communications with victims, which most likely was launched on September 20, 2021. The ransomware shares a similar ransom note structure to EpsilonRed, BlackCocaine, and some Sodinokibi/REvil notes. As of September 24, 2021, Colossus has one known victim currently in active negotiations, an automotive group based in the United States. The operators appear at least highly familiar if not directly associated with other existing ransomware-as-a-service (RaaS) groups based on their tactics, techniques, and procedures (TTPs).

Details

As part of routine monitoring, ZeroFox detected and extracted a ransom note titled “HOW_TO_RECOVER_FILES.Colossus.txt” from a malware sample uploaded to the Hatching Triage malware analysis service on September 24, 2021. The note contained a link with the domain colossus[.]support and a victim key to access a private “Support Room” page to engage the attacker. The page notes a U.S.-based automotive group of dealerships as the target and threatens to dump 200 GB of exfiltrated data if an amount of USD 400,000 is not paid. A countdown timer shows the ransom is scheduled to increase to USD 600,000 in about 3 days. A suspected representative of the targeted company with the anonymous

username “USER912058085” appears to have entered the chat room and initiated negotiations. At this time, the attacker has shared four sample files of stolen data hosted at the file sharing service ibb[.]co and is awaiting a further response.

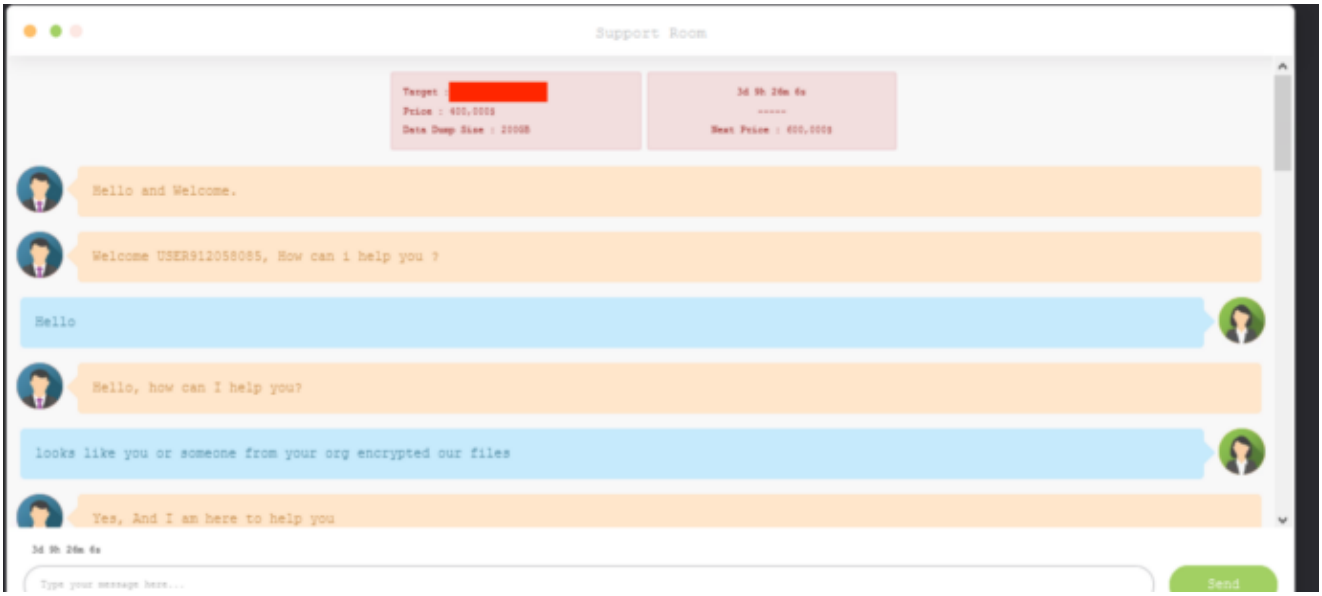


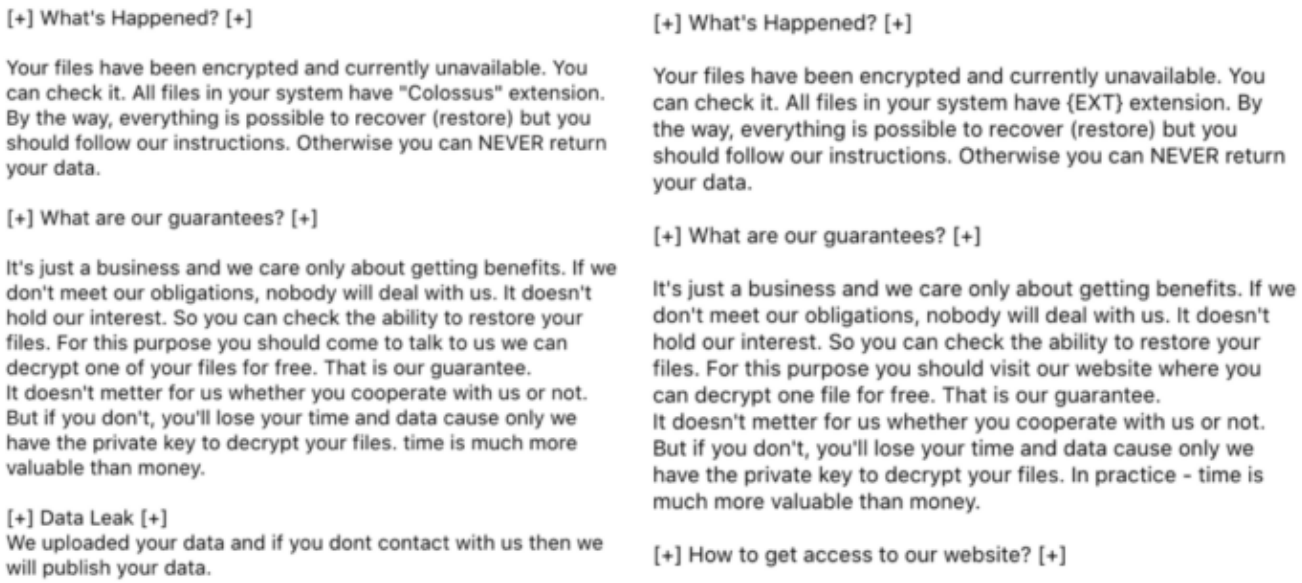
Figure 1: Private negotiation page for Colossus ransomware target
Source: ZeroFox Threat Intelligence

Figure 2: Colossus ransomware actor sharing samples of stolen data
Source: ZeroFox Threat Intelligence

Ransomware groups tend to host a support page on a 1-1 basis with their victims (a unique page), or they run a support portal. In the case of Colossus, they registered the domain for their support portal on 9/19/2021. The domain is registered via Tucows, and the nameserver responding to DNS lookups is dnspod, a popular DNS provider for cybercriminals. Dnspod has hosted a number of other ransomware support pages. This does not mean there is a definitive link between Colossus and other groups that have used dnspod; rather, it shows that there is a playbook that ransomware operators follow for operational security reasons.

Passive DNS of the support domain shows successful support page resolutions starting on 9/20/2021 to a web server hosted in Riga, Latvia. This webserver is hosted by PINVDS, a Russian-based VPS provider.

ZeroFox has not observed any related deep and dark web chatter specifically on a Colossus ransomware product or Colossus ransomware affiliate program. However, these operators appear to be at least highly familiar if not directly associated with other existing ransomware-as-a-service (RaaS) groups based on their tactics, techniques, and procedures (TTPs). Their ransom note is similar in structure and content to other known ransomware products, including some EpsilonRed/BlackCocaine and REvil/Sodinokibi samples. This could indicate using a similar builder for the ransomware files, and follows a pattern of ransomware groups disappearing and reappearing with a rebranded name and similar toolsets.



[+] What's Happened? [+]

Your files have been encrypted and currently unavailable. You can check it. All files in your system have "Colossus" extension. By the way, everything is possible to recover (restore) but you should follow our instructions. Otherwise you can NEVER return your data.

[+] What are our guarantees? [+]

It's just a business and we care only about getting benefits. If we don't meet our obligations, nobody will deal with us. It doesn't hold our interest. So you can check the ability to restore your files. For this purpose you should come to talk to us we can decrypt one of your files for free. That is our guarantee.
It doesn't metter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data cause only we have the private key to decrypt your files. time is much more valuable than money.

[+] Data Leak [+]
We uploaded your data and if you dont contact with us then we will publish your data.

[+] What's Happened? [+]

Your files have been encrypted and currently unavailable. You can check it. All files in your system have {EXT} extension. By the way, everything is possible to recover (restore) but you should follow our instructions. Otherwise you can NEVER return your data.

[+] What are our guarantees? [+]

It's just a business and we care only about getting benefits. If we don't meet our obligations, nobody will deal with us. It doesn't hold our interest. So you can check the ability to restore your files. For this purpose you should visit our website where you can decrypt one file for free. That is our guarantee.
It doesn't metter for us whether you cooperate with us or not. But if you don't, you'll lose your time and data cause only we have the private key to decrypt your files. In practice - time is much more valuable than money.

[+] How to get access to our website? [+]

Figure 3: Side-by-side comparison of Colossus (left) and REvil/Sodinokibi (right) ransom notes
Source: ZeroFox Threat Intelligence

Additionally, this Colossus ransomware group is engaging in the double extortion method of encrypting then threatening to leak stolen data on the dark web in a similar manner to over 50 other ransomware and digital extortion groups tracked by ZeroFox so far this year. A public Colossus-specific ransomware leak site is likely to arise in the coming weeks out of this first known operation to leak data. Finally, it is noteworthy to see unique usernames being assigned to any visitors to the private “Support Room” page as a form of enhanced operational security. Other ransomware groups have struggled with security researchers and other malicious actors advertising on social media or even directly hijacking victim chat communications, most recently the BlackMatter ransomware group targeting of NEW Cooperative.

Colossus Ransomware Analysis

Similar to other ransomware samples, once the binary executes on the target environment, it begins the infection process. The sample of Colossus leverages PowerShell to facilitate the ransomware infection. However, ransomware operators packed Colossus with the Themida application. Themida is a packer that, when used to protect a binary, modifies the underlying code before running the application inside a custom virtual machine, making analysis of the binary significantly challenging.

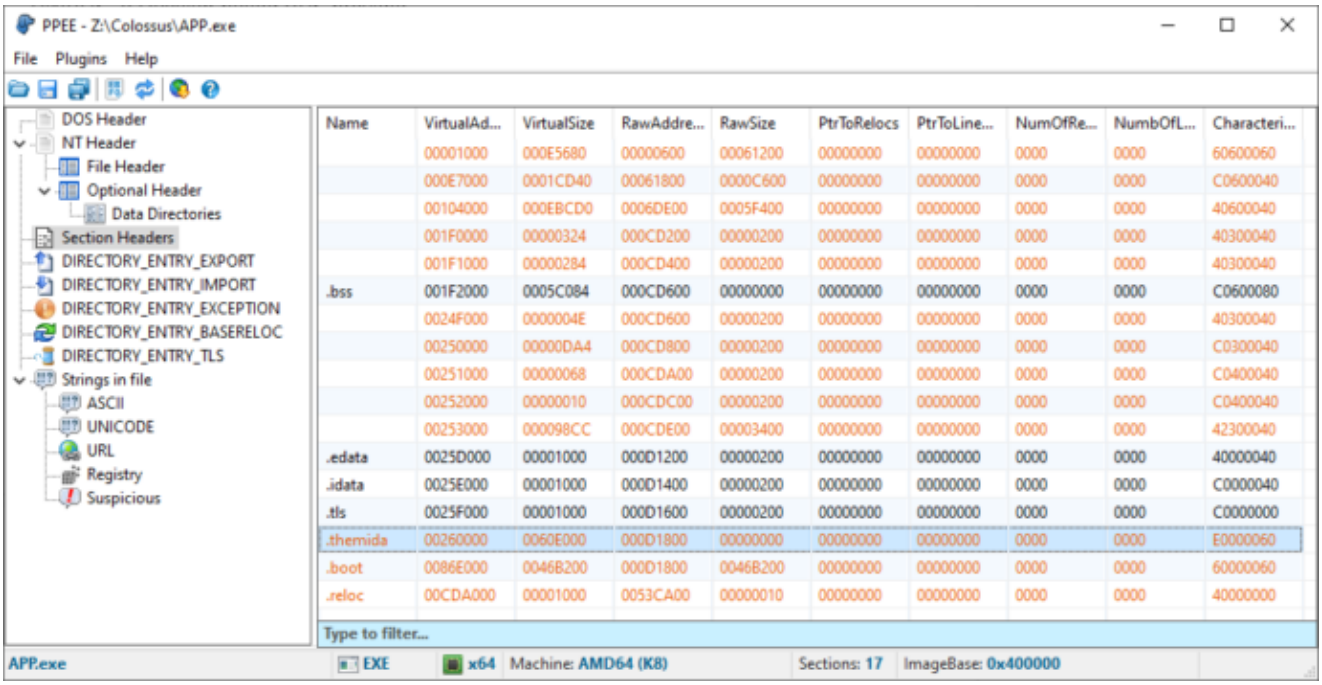


Figure 4: Screenshot depicting a Colossus (APP[.]exe) sample packed by Themida
Source: ZeroFox Threat Intelligence

During the infection cycle, the ransomware will begin the encryption process by encrypting all files, documents, and images on the target machine. After encryption, a ransom note will be available for the victim that contains decryption and negotiation instructions. The operators inform the victim to visit the Colossus website and contact the operators at the provided email address.

Indicators of Compromise

Hashes

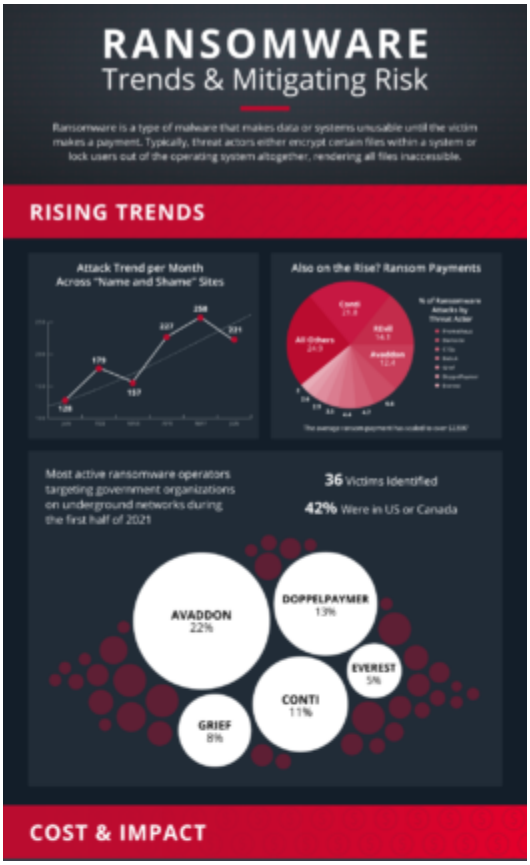
```
SHA256 - b70b9039ec4b33987a991c5c20729eb3310d7406b8d15161037df3b21fd968bb

MD5 - 4f3669edb010f5db21b13a088182b8fe

SHA-1 - 892447e55ff7a3ac5d26c573bb8eb4607b41ba1e
```

Recommendations

- Ensure antivirus and intrusion detection software is up-to-date with all patches and rule sets.

- Enable 2-factor authentication for all of your organizational accounts.
- Utilize account permissions best practices such as role-based access control, least privilege, and restricting root/admin permissions.
- Segment critical network resources using zero-trust configurations.
- Maintain regularly scheduled backup routines, including off-site storage and integrity checks.
- Limit file egress by size and type.
- Log and monitor all administrative actions as much as possible. Alert on any suspicious activity.
- Consider disabling, or at least logging, all network activity outside of normal business hours for most users where possible.
- Monitor usage of dual purpose tools such as Powershell for abnormal behaviors.
- Disable port echoing on all Internet-facing devices.
- Use a VPN for internal network connections.
- Avoid opening unsolicited attachments and never click suspicious links.

Learn more about ZeroFox's Threat Intelligence team, including how to access finished intelligence like this flash report here. If you need a refresher on just a few of the costs and impacts both malware and ransomware attacks can have, click on the infographic below. Included in the infographic are top recommendations to get a leg up on establishing a security plan to ensure your enterprise is prepared and protected. In tandem, the ZeroFox Threat Research team has also released a more detailed report on ransomware trends and ways you can start preparing for what's to come.



Click to View Full Ransomware Infographic

Source: ZeroFox Threat Research