# Malicious Actors Target Comm Apps such as Zoom, Slack, Discord

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malicious-actors-target-comm-apps-such-as-zoom-slack-discord

In our 2020 midyear report, we discussed how the Covid-19 pandemic had forced many organizations to shift from physical offices to virtual ones — a change that also led to the rise of messaging and video conferencing apps as indispensable tools for communication. While these apps have provided businesses a way of maintaining communication between employees, they have also caught the eye of malicious actors who are always looking to integrate new techniques in their malicious activities.

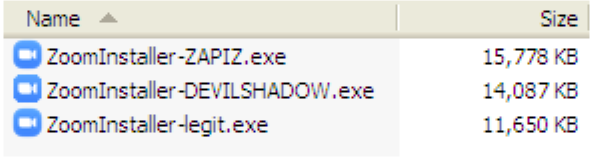
## Zoom-based attacks have remained consistent

No other software has defined 2020 as much as the video conferencing app Zoom, which has exploded in popularity since the start of the pandemic. Given its high usage rate among schools, businesses, and individuals, it's no surprise that cybercriminals have been focusing their efforts on Zoom-based attacks.

The most well-known malicious activity involving Zoom is probably "Zoombombing," which involves pranksters crashing a meeting and then performing disruptive actions, such as spamming pornographic content or even just generally being a nuisance.

While annoying, Zoombombing is typically harmless in terms of security. On the other hand, we've encountered Zoom-related attacks that involve actual malware, which can potentially be more damaging to organizations and individuals. The most common Zoom-related attack technique is the use of Zoom installers bundled with malware.

In some cases, the attackers use fake Zoom installers to trick users into installing them on their machines. We encountered an example of this in May, after we found samples of malware files that were disguised as fake Zoom installers. While it could be difficult for the average user to distinguish the legitimate Zoom app from the fake ones, closer inspection shows that the malicious versions have significantly larger file sizes.



| Name | Size |
|---|---|
| ZoomInstaller-ZAPIZ.exe | 15,778 KB |
| ZoomInstaller-DEVILSHADOW.exe | 14,087 KB |
| ZoomInstaller-legit.exe | 11,650 KB |

Figure 1. The file size of malicious Zoom copies compared with that of the legitimate installer

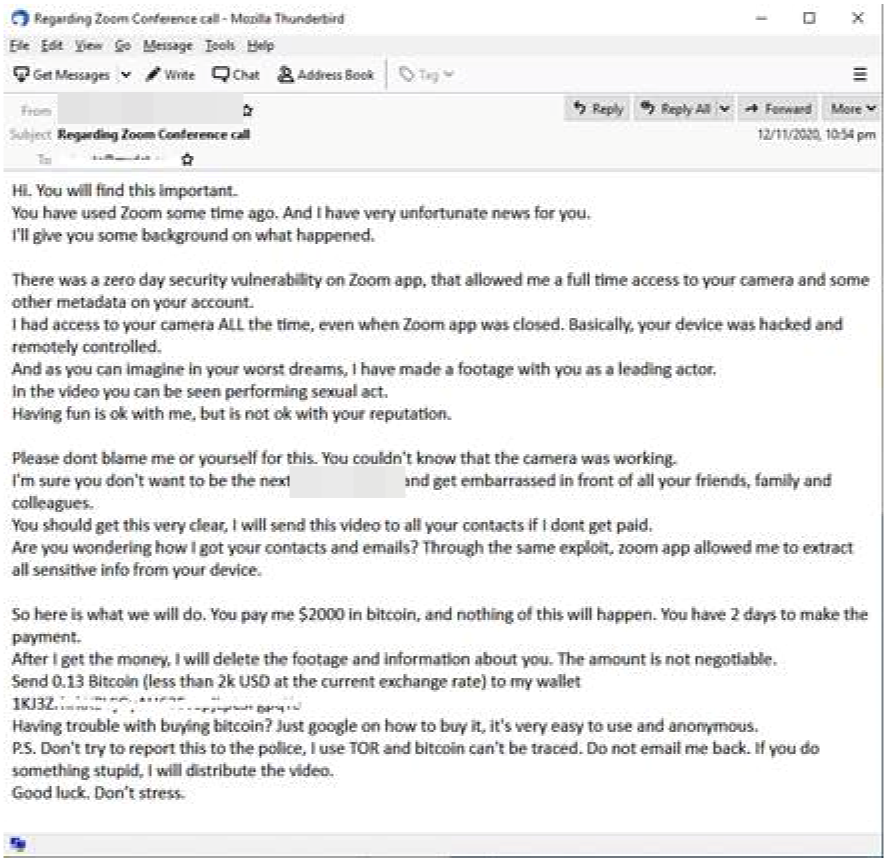
One of the malware samples (Trojan.Win32.ZAPIZ.A) is a backdoor with remote access features, allowing the attacker to gain access to the infected machine to perform malicious actions, such as stealing information. The other sample (Backdoor.Win32.DEVILSHADOW.THEAABO) has an installer that consists of a file containing malicious commands. Interestingly, both compromised installers installed a legitimate version of Zoom, likely to hide evidence of malicious activity from the user.

Aside from using compromised installers, we also found instances where malicious actors bundled legitimate installers with malware files. In April, we discovered an attack that used real Zoom installers that came with the RevCode WebMonitor RAT (Backdoor.Win32.REVCODE.THDBABO). This malware variant allows its operator to execute commands remotely, such as adding or deleting files, recording keystrokes, and gathering information.

Another example of this is the ZAPIZ malware (Trojan.Win32. ZAPIZ.A), a trojan that also comes bundled with a legitimate Zoom installer. Once downloaded, it will kill all running remote utilities, after which it will use PORT =5650/TCP for remote inbounding.

Based on our analysis, ZAPIZ will perform information theft, gathering the target machine's usernames and its machine name — perhaps as a prelude to further attacks.

We also found an email sample where a malicious actor tried to extort money from the victim by threatening them with the release of compromised video footage — allegedly acquired via a hacked camera.


Regarding Zoom Conference call - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More

From [redacted]
Subject Regarding Zoom Conference call
To [redacted]
12/11/2020, 10:54 pm

Hi. You will find this important.
You have used Zoom some time ago. And I have very unfortunate news for you.
I'll give you some background on what happened.

There was a zero day security vulnerability on Zoom app, that allowed me a full time access to your camera and some other metadata on your account.
I had access to your camera ALL the time, even when Zoom app was closed. Basically, your device was hacked and remotely controlled.
And as you can imagine in your worst dreams, I have made a footage with you as a leading actor.
In the video you can be seen performing sexual act.
Having fun is ok with me, but is not ok with your reputation.

Please dont blame me or yourself for this. You couldn't know that the camera was working.
I'm sure you don't want to be the next [redacted] and get embarrassed in front of all your friends, family and colleagues.
You should get this very clear, I will send this video to all your contacts if I dont get paid.
Are you wondering how I got your contacts and emails? Through the same exploit, zoom app allowed me to extract all sensitive info from your device.

So here is what we will do. You pay me $2000 in bitcoin, and nothing of this will happen. You have 2 days to make the payment.
After I get the money, I will delete the footage and information about you. The amount is not negotiable.
Send 0.13 Bitcoin (less than 2k USD at the current exchange rate) to my wallet
1KJ3Z.[redacted]
Having trouble with buying bitcoin? Just google on how to buy it, it's very easy to use and anonymous.
P.S. Don't try to report this to the police, I use TOR and bitcoin can't be traced. Do not email me back. If you do something stupid, I will distribute the video.
Good luck. Don't stress.

Figure 2. Email threatening the victim with release of compromised video footage

## Abuse of other communication apps such as Discord and Slack

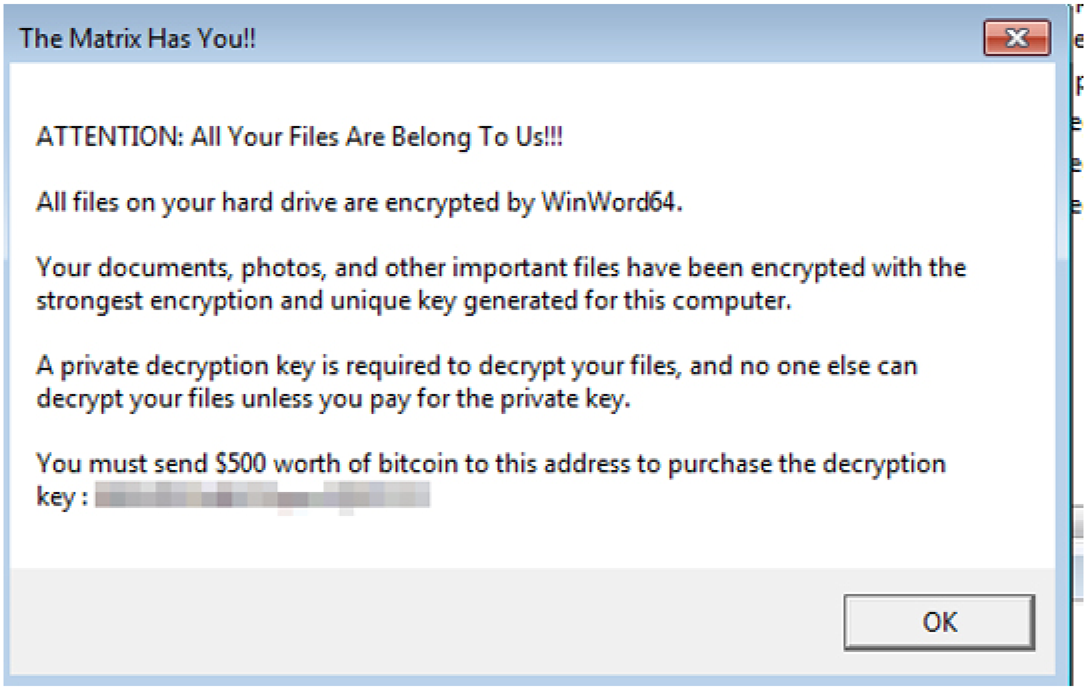
While Zoom remains perhaps the most popular communication app during the pandemic, it's not the only one that cybercriminals have abused. We found evidence of attacks that integrate other communication services — specifically Slack and Discord — into their routines.

Slack has earned a loyal following over the years, with over 10 million daily active users as of 2019. However, we also found evidence of malicious actors making use of some of its features.

We recently found a ransomware variant (Ransom.Win32.CRYPREN.C) that, on the surface, seems fairly standard in terms of capabilities. It encrypts files with the following extensions (after which it will append the .encrypted suffix):

- .bmp
- .doc
- .docx
- .gif
- .jpeg

- .jpg
- .m2ts
- .m4a
- .mkv
- .mov
- .mp3
- .mp4
- .mpeg
- .mpg
- .pdf
- .png
- .ppt
- .pptx
- .txt
- .xls
- .xlsx



ATTENTION: All Your Files Are Belong To Us!!!

All files on your hard drive are encrypted by WinWord64.

Your documents, photos, and other important files have been encrypted with the strongest encryption and unique key generated for this computer.

A private decryption key is required to decrypt your files, and no one else can decrypt your files unless you pay for the private key.

You must send $500 worth of bitcoin to this address to purchase the decryption key : [redacted]

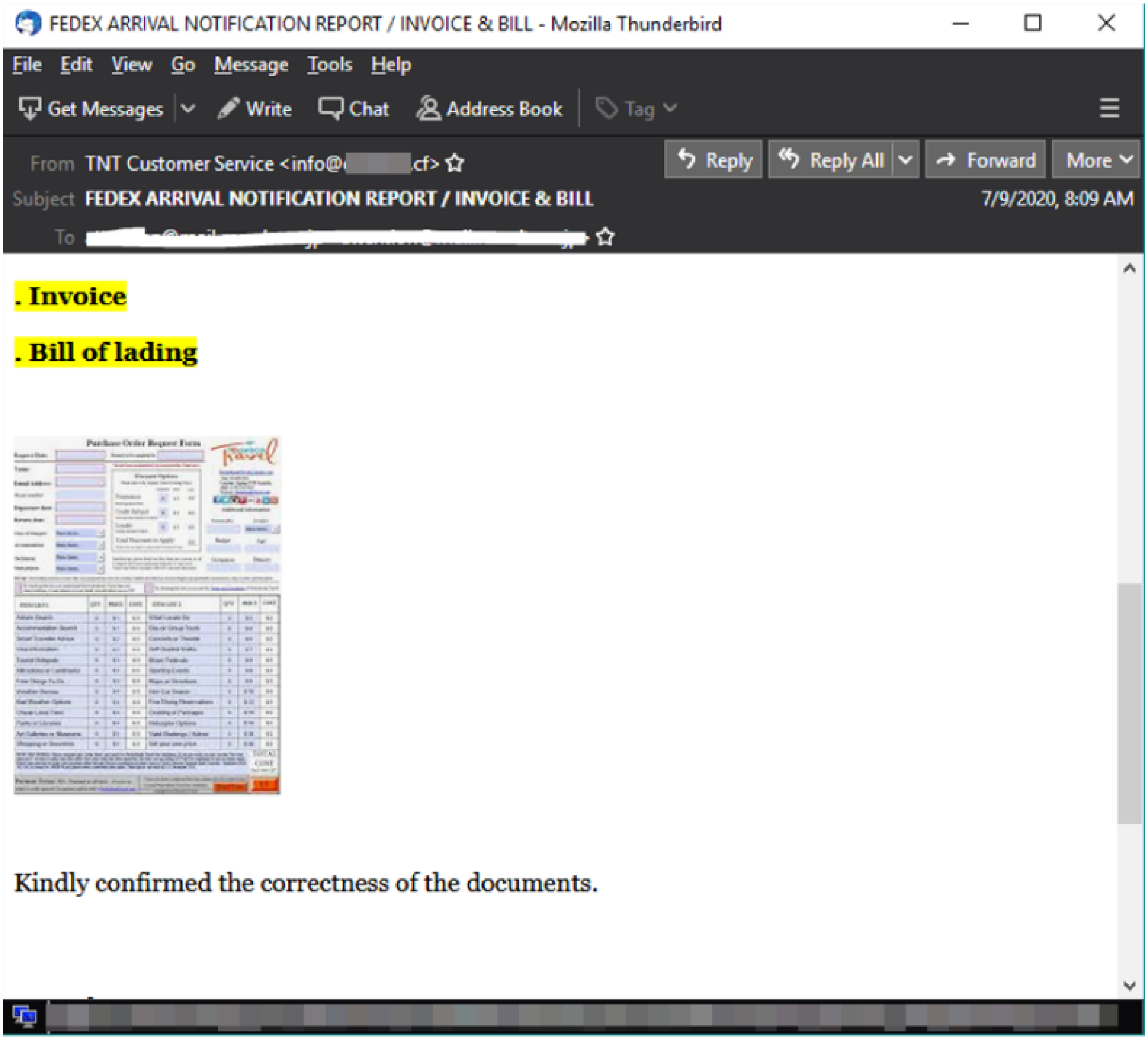
Figure 3. The ransom note for the Crypren ransomware

What makes Crypren interesting is its use of Slack webhooks to report its victims' encryption status back to its command-and-control (C&C) server — a technique we haven't encountered before.

Currently, it only sends back a minimal amount of data, namely computer and user names, the number of infected files, and the infection timestamp — indicating that the use of Slack for infection status reporting might still be in its testing phase.

Discord is another communication software that shares similar features with Slack (while also being notable for its widespread use in gaming communities). We found samples that show how malicious actors are using Discord as part of a campaign involving malicious spam emails that eventually end in an AveMaria or AgentTesla malware infection. We first observed the use of malicious spam to deliver these malware families in 2019 — however, the addition of Discord as part of its attack routine is relatively recent.

The malicious emails are typically either postal delivery notifications or invoices with an included DHL or TNT-themed attachment:


FEDEX ARRIVAL NOTIFICATION REPORT / INVOICE & BILL - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Reply
Reply All
Forward
More

From TNT Customer Service <info@[redacted].cf>

Subject FEDEX ARRIVAL NOTIFICATION REPORT / INVOICE & BILL

7/9/2020, 8:09 AM

To [redacted]

**. Invoice**

**. Bill of lading**

Kindly confirmed the correctness of the documents.

Figure 4. Spam mail sample

These emails come with embedded links — either in the images or the text — that point to a Discord URL with the following format: hxxps://cdn[.]discordapp[.]com/attachments/{ChannelID}/{AttachmentID}/example[.]exe. These URLs are used to host AveMaria and AgentTesla, which will then infect the users' machines once they click on the executable.

The use of legitimate apps such as Slack and Discord as part of an attack may come down to a few simple reasons: they're well-known, widely used, free, and provide some form of anonymity. Furthermore, users are not even required to have the apps installed to download files from them, making the process streamlined and efficient. Another possible reason that explains these programs' use is that they can pass off as normal legitimate network communication. Their popularity also amounts to a high chance that employees and end-users are already using these services.

## Defending against attacks that abuse communication apps

Fortunately, defending against these types of attacks is relatively straightforward. In the case of the Zoom installers, the commonality between the attacks is that they are downloaded from places other than the official Zoom download page. The simplest way to avoid infection is to download communications apps (and all apps in general) only from official channels. This will ensure that the software is free from tampering.

Users should also avoid clicking on any links or downloading attachments from suspicious or unverified emails. If unsure, it would be a good idea to double-check with the alleged sender to confirm if they were the ones who sent the email.

HIDE

**Like it? Add this infographic to your site:**
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats