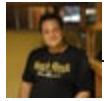


(Ab)using Adobe Acrobat Sign to distribute malware

 blog.avast.com/adobe-acrobat-sign-malware



Luis Corrons 15 Mar 2023

What if an attacker could manage to make a well-known company distribute an email on their behalf?

Bad actors have been distributing malware through email for decades. Over time, security technology has evolved and improved greatly, making this task harder for cybercriminals. 20 years ago, we witnessed the frequent distribution of email worms, which caused inboxes to be flooded with them and mail servers to collapse. Although the prevalence of email worms is much lower these days, email phishing is the new prevalent threat users have to face today, despite email being a great tool used by most internet users.

Not only have the different protection mechanisms have evolved – individuals have also grown more tech-savvy, and it has become increasingly more difficult to fool them. Don't get me wrong, though: Modern bad actors are professionals that make a living out of cybercrime, and they invest a lot in making their tricks (they sometimes deliver them in messages that make their way past seasoned security professionals). In any case, we can't underestimate the ability of these cybercriminals to carry out malicious activities.

What if an attacker could manage to make a well known company distribute an email on his behalf? What if the only link in that email takes the reader to a website belonging to the same company? In this message, there aren't any suspicious senders, suspicious URLs, or the inclusion of other websites – everything is legit. Chances are that this type of email will not only bypass all cybersecurity layers, but it will also fool the final user.

How today's cybercriminals are making use of this innovative technique

Adobe offers a cloud service to sign documents online called Acrobat Sign, which users can register for and start using it right away. Adobe Acrobat Sign allows registered users to send a document signature request to anyone. When doing so, an email will be generated and sent to the intended recipients. The email includes a link to the document (which can be a PDF, Word document, HTML file, and so on) that will be hosted on Adobe itself.

The sender can add text that they'd like to be shown in the email, which is an important detail, as it can easily be abused by cybercriminals.

This is one of the messages that our team has captured:

Subject: Signature requested on "Copyright infringement report #3047"



UK Copyright Service - Content Protection <adobesign@adobesign.com>
to [redacted]@[redacted].com

 **Adobe Acrobat Sign**



UK Copyright Service - Content Protection requests
your signature on
[Copyright infringement report #3047](#)

[Review and sign](#)

Notice of Copyright Infringement:
Request for Removal of Infringing Material.

UK COPYRIGHT SERVICE - CONTENT PROTECTION
check@9music.company

After you sign [Copyright infringement report #3047](#), all parties will receive a final PDF copy by email.

 Powered by
Adobe Acrobat Sign

By proceeding, you agree that this agreement may be signed using electronic or handwritten signatures.

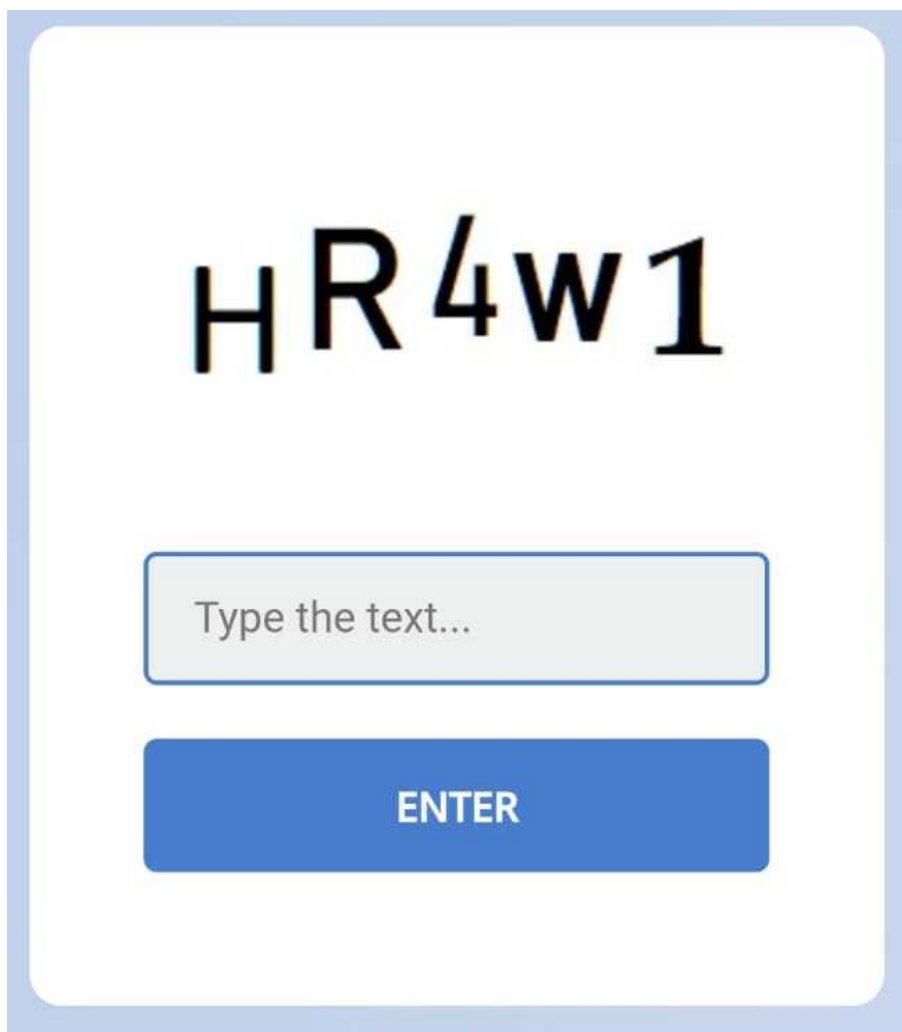
To ensure that you continue receiving our emails, please add adobesign@adobesign.com to your address book or safe list.

[Terms of Use](#) | [Report Abuse](#)

The sender's address displays as adobesign@adobesign.com, which is a legitimate email address.

When the victim clicks on the "Review and sign" button, it takes them to a page hosted in "eu1.documents.adobe.com/public/", which is another legitimate source that belongs to Adobe. As I mentioned earlier, people using this service can upload a broad variety of file types to Adobe Acrobat Sign, which will be displayed in the email with the option to sign them.

Cybercriminals include text with a link in a document that gives the victim the idea that they'll be through the content before signing it. When clicking on the link, the victim is redirected to another site where they're asked to enter a hardcoded CAPTCHA.



HR4W1

Once entered, the victim will be asked to download a ZIP file that contains a Redline Trojan variant that's designed to steal passwords, crypto wallets, and more.


In the example above, the target of the attack owns a YouTube channel with hundreds of thousands of subscribers, so the topic of the message fits pretty well with that profile. Fortunately, the victim realized that there was something “phishy” about the message and didn't click on the link.

Not ready to face defeat, however, the attacker tried to carry out the attack again a few days later. In order to increase the chances of having the malware installed, they also added another link into the email sent by Adobe.

UK Copyright Service -
Regulations Report
requests your signature
on
**Copyright infringement
report**

[Review and sign](#)

Notice of Copyright
Infringement:
Request for Removal of
Infringing Material.
Copy of the report -
<https://dochub.com/copyright->



**UK COPYRIGHT SERVICE -
REGULATIONS REPORT**
call@9music.company

When clicking on that link, the following page will be loaded in the browser:

Hello,

We have detected a copyright infringement such as a video clip or background sound belonging to UK Music on Youtube video hosting platform.

Music copyright designates legal ownership of a musical composition or sound recording. This ownership includes exclusive rights to redistribute and reproduce the work, as well as licensing rights.

Full infringement report: https://reported.digital/youtube_1TGv4
[REDACTED]report.docx

Please remove infringing third party content to avoid a complaint directly to Youtube video hosting platform.

If you believe this notification is in error, you may file a counter-notification of the alleged infringement.

UK Music team.
Copyright Office.



Infringement Notice #3047.



SOUND UK



This page is hosted on dochub.com, which is another company that offers electronic document signing. However, in case the victim clicks on the “Review and sign” button within the email, it will take them to Adobe and will show the very same document to be signed

(that also contains the same link in it).

**Adobe Acrobat Sign**

**1 required field remaining**

Hello,

We have detected a copyright infringement such as a video clip or background sound belonging to UK Music on Youtube video hosting platform.



Music copyright designates legal ownership of a musical composition or sound recording. This ownership includes exclusive rights to redistribute and reproduce the work, as well as licensing rights.


Full infringement report:https://reported.digital/youtube_1TGv4report.docx

Please remove infringing third party content to avoid a complaint directly to Youtube video hosting platform.

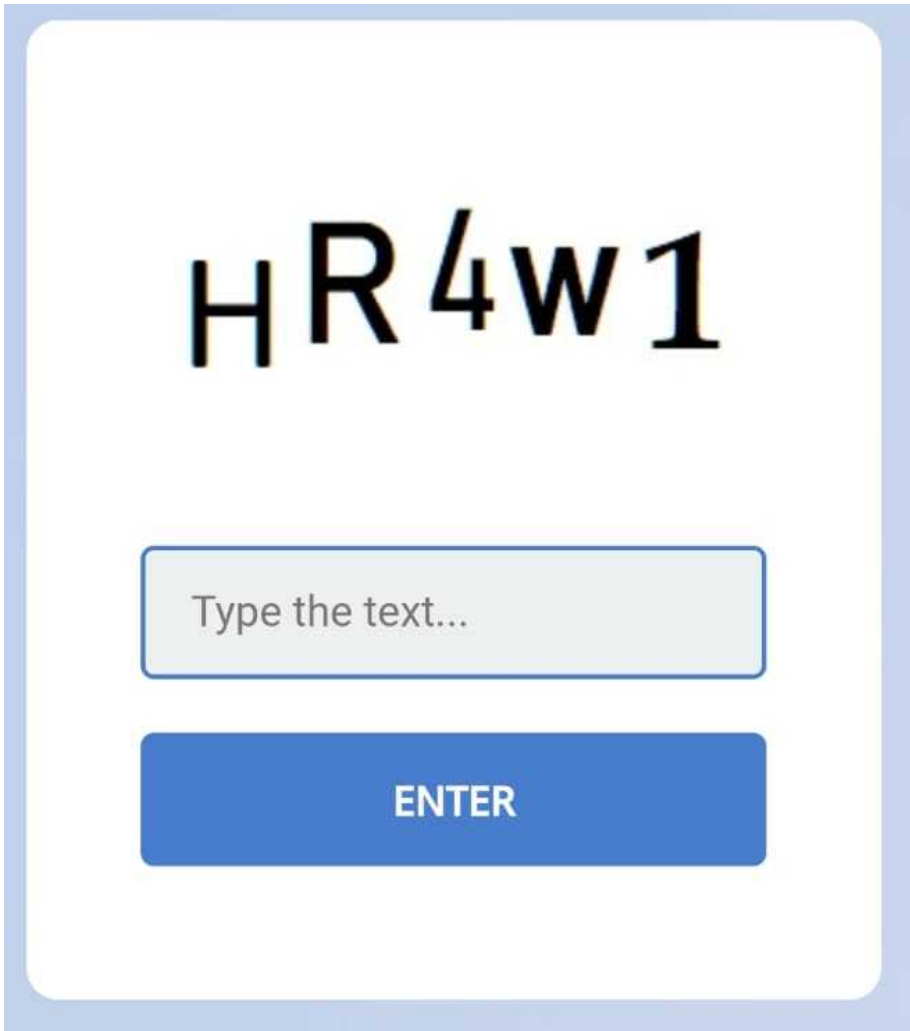
If you believe this notification is in error, you may file a counter-notification of the alleged infringement.

UK Music team.
Copyright Office.
Infringement Notice #3047.



Signature: *  Sign here
Email: 

The link in the documents that's loaded on both dochub.com and adobe.com takes the victim to the same CAPTCHA (which is hardcoded):



When entered correctly, it takes the victim to the download of the malware, which was another Redline Trojan variant. In this instance, the ZIP file also contained some other non-malicious executables belonging to the Grand Theft Auto V game.

One of the characteristics of the two variants of Redline that these cybercriminals used in these attacks is that they've artificially increased the size of the Trojan to more than 400MB. This is not noticeable by the victim during the download, as the file is compressed and most of that artificial size has just been filled with zeros. The reason for this is unknown; it's possible that the cybercriminals are using it in the hope of bypassing some antivirus engines that could behave differently with big files.

This abuse of Adobe Acrobat Sign to distribute malware is a new technique used by attackers that's targeted to a specific victim. Our team has yet to detect other attacks using this technique; nevertheless, we fear that it may become a popular choice for cybercriminals in the near future. This is because it may be able to avoid different anti-malware filters, which increases its chances of reaching the victims. In any case, we have already contacted both Adobe and dochub.com and shared all the information of the incidents with them.

How you can protect yourself

- Don't click on email links from unknown senders. Pay extra close attention to anything that you receive from those you don't know.
- Check your sources. Before clicking on a link, ask yourself why you've received it and if it can be considered to be legitimate.
- Use security software. Security software, or antivirus, acts as a safety net, protecting even the most tech-savvy internet users.