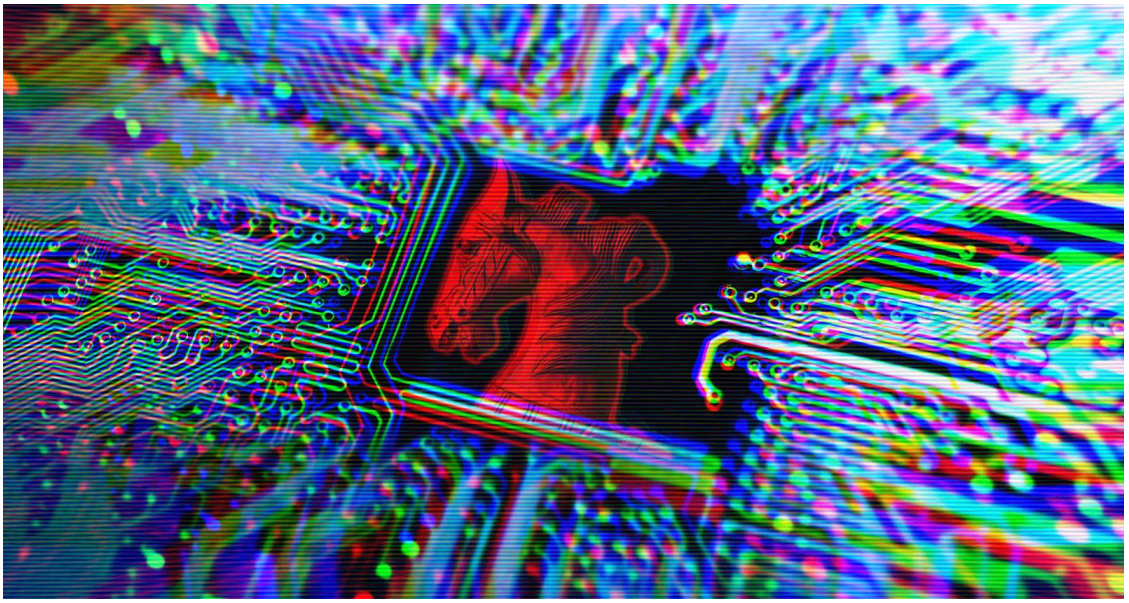
Fake DMCA and DDoS complaints lead to BazaLoader malware

By Ionut Ilascu

Published: 2021-08-27 · Archived: 2026-04-06 00:53:08 UTC

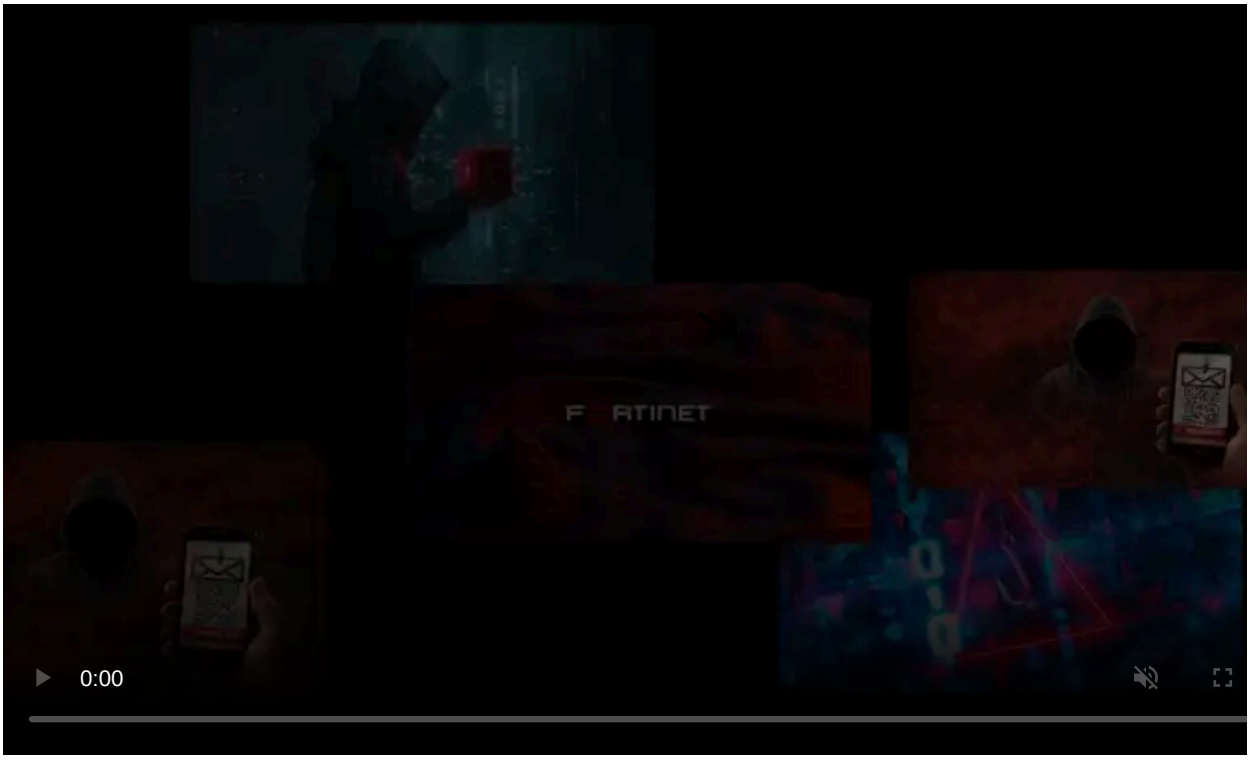


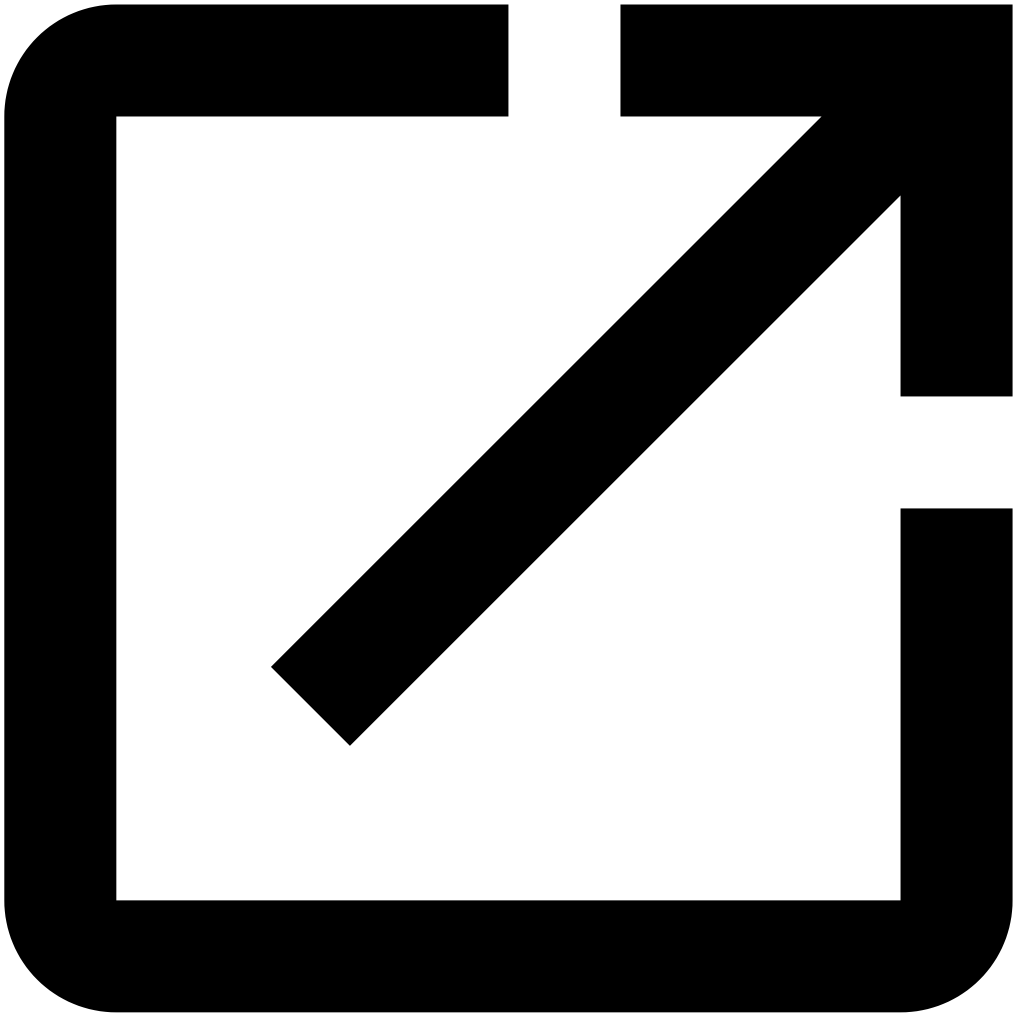
Cybercriminals behind the BazaLoader malware came up with a new lure to trick website owners into opening malicious files: fake notifications about the site being engaged in distributed denial-of-service (DDoS) attacks.

The messages contain a legal threat and a file stored in a Google Drive folder that allegedly provides evidence of the source of the attack.

Fake legal threats

The DDoS theme is a variation of another lure, a Digital Millennium Copyright Act (DMCA) infringement complaint linking to a file that supposedly contains evidence about stealing images.


F RTINET
0:00



In submissions seen by BleepingComputer, the threat actor used Firebase URLs to push BazaLoader. The goal is the same though: use contact forms to deliver BazaLoader malware that often drops Cobalt Strike, which can lead to data theft or a ransomware attack.

Microsoft has warned about this delivery method in April, when cybercriminals used it to deliver IcedID malware. The recent campaigns are similar, only the payload and the lure have changed.

Website developer and designer Brian Johnson posted last week about two of his clients getting legal notifications about their websites being hacked to run DDoS attacks against a major company (Intuit, Hubspot).

The sender threatened with legal action unless the recipients didn't "immediately clean" their website of the malicious files that helped deploy the DDoS attack.

"I have shared the log file with the recorded evidence that the attack is coming from [example.com] and also detailed guidelines on how to safely deal with, find and clean up all malicious files manually in order to eradicate the threat to our network," reads the fake notification.

The malicious sender also included a link to a file hosted in Google Drive claiming to provide evidence of the DDoS attack and its origin.

Hello,

This message was written to you in order to notify, that we are currently experiencing serious network problems and we have detected a DDoS attack on our servers coming from the your website or a website that your company hosts (example.com). As a consequence, we are suffering financial and reputational losses.

We have strong evidence and belief that your site was hacked and your website files were modified, with the help of which the DDoS attack is currently taking place. It is strictly advised for you as a website proprietor or as a person associated with this website take immediate action to fix this issue.

To fix this issue, you should immediately clean your website from malicious files that are used to carry out the DDoS attack.

I have shared the log file with the recorded evidence that the attack is coming from example.com and also detailed guidelines on how to safely deal with, find and clean up all malicious files manually in order to eradicate the threat to our network.

Click on the link below to download DDos Attack evidence and follow the instructions to fix the issue:

https://drive.google.com/uc?export=download&id=removed

Please be aware that failure to comply with the instructions above or/and if DDoS attacks associated with example.com will not stop within the next 24 hour period upon receipt of this message, we will be entitled to seek legal actions to resolve this issue.

If you will experience any difficulties trying to solve the issue, please reply immediately with your personal reference case number (included in the log report and instructions mentioned above) and I will do my best to help you resolve this problem asap.

Austin Nguyen
intuit.com IT security team

Proofpoint security researcher Matthew Mesa notes in a tweet that these messages are sent through the website's contact form and deliver the BazaLoader malware hosted on a Google site.

The researcher also says that the lure is a variation of the copyright infringement theme, also submitted through the website's contact form.

BleepingComputer has received several of these infringement notifications over the past few months with allegations of using protected images without the owner's consent.

The message provides a link to a file that supposedly lists the images used without permission. The data is hosted in Google's Firebase cloud storage.

To make the matter seem urgent, the sender also says that the website owner is "possibly be liable for statutory damage as high as $120,000." It is all a ruse to deliver malware, though.

My name is Marquel.

Your website or a website that your organization hosts is infringing on a copyright protected images owned by myself.

Check out this document with the URLs to my images you utilized at www.bleepingcomputer.com and my earlier publication to get the proof of my copyrights.

Download it right now and check this out for yourself:

https://firebasestorage.googleapis.com/v0/b/files-d6e6c.appspot.com/o/download-dlm39vbk30.html?alt=media&token=d0b122e7-49bb-4c04-9b26-d2364ca615f2&ID=381406677867196640

I do think you've deliberately violated my legal rights under 17 USC Sec. 101 et seq. and could possibly be liable for statutory damage as high as $120,000 as set forth in Section 504 (c) (2) of the Digital millennium copyright act ("DMCA") therein.

This message is official notice. I demand the removal of the infringing materials mentioned above. Take note as a service provider, the Digital Millennium Copyright Act requires you, to remove and disable access to the infringing materials upon receipt of this particular letter. In case you don't stop the utilization of the previously mentioned copyrighted materials a legal action will likely be commenced against you.

I have a strong belief that utilization of the copyrighted materials mentioned above as allegedly infringing is not permitted by the copyright proprietor, its agent, or the laws.

I swear, under penalty of perjury, that the information in this message is correct and that I am the legal copyright proprietor or am certified to act on behalf of the proprietor of an exclusive right that is allegedly infringed.

Best regards,

Marquel Lowe
08/17/2021

Malware analyst Brad Duncan examined the file and found it was a ZIP archive with JavaScript that fetches the BazaLoader DLL, a backdoor attributed to the TrickBot gang that typically leads to a ransomware infection.

The malware then reaches to its command and control (C2) server and gets Cobalt Strike, a penetration-testing tool widely abused by cybercriminals to maintain persistence and deliver other payloads.

As seen from the samples above, the notifications are quite convincing and take advantage of the legitimacy of the contact form emails, which increases the chances of receiving a "safe" mark from email security solutions.

Looking for signs of malicious intent (incomplete contact information, incorrect grammar, suspicious links) is a good way to avoid falling for this social engineering trap.
