TRINITY CYBER

STEGANOGRAPHY:

APPENDING DATA TO IMAGES

BACKGROUND

From photographs posted to Instagram to icons used in websites, image files have become part of our everyday Internet life. You might know that JPEG files are the preferred format for photographers. And that a png file can have a transparent background. We smile at the gif files that are animated. While there are a vast number of image file types, you might not know that there may be extra data hidden inside the file. The FBI refers to this as a form of steganography. Most of the time, this added content is a result of poorly written software that simply does not adhere to the file format standards.

Sometimes, the added content has legitimate benefit. Apple® takes advantage of this "feature" to make images come alive with "Live Photos". Adobe Photoshop uses this "extra space" to store abundant metadata about edited photographs. Legitimate or not, since appending extra data to images is common practice, the programs that use images (document editors, web pages, presentations, etc.) ignore the extra data, as do security professionals and the cybersecurity tools they use to protect you – and that's a problem.

THE PROBLEM

Cyber adversaries actively exploit the fact that extra data added to the end of an image file will be ignored when they append malware to an inbound image or these adversaries append the data they've stolen from you to an image being posted to an Internet site.

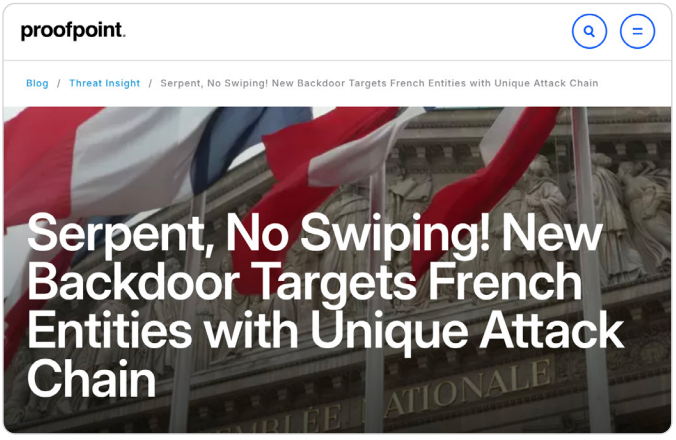

FIGURE 1: PROOFPOINT BLOG • MARCH 21, 2022

Think about countless images incorporated into the web sites you visit. Expand that number across your entire enterprise. Add to that the number of photos being shared through social media. The sheer volume of image files that move in and out of your enterprise is staggering. Do any of them have appended data? Is the appended data malicious? Is the appended data legitimate? Do you have the cycles to examine every one? Of course you don't.

Even if your tools could detect appended data on image files, which they cannot, you would be left with two bad options: block or alert. If you block images with appended data from entering your enterprise, nearly every web page you visit will be unusable. If you generate an alert from each image with appended data, your security team will be buried. So, you neither block or alert and roll the dice.

© Trinity Cyber, 2025. All rights reserved.

THE SOLUTION

With Trinity Cyber, the number of images that enter or exit your network with appended data is zero.

Trinity Cyber examines each and every image file for the presence of appended data and, except for some rare, legitimate uses like the examples cited above, removes the appended data and delivers a clean image. Every time. With Trinity Cyber's blazingly fast inline protection, adversaries no longer have this steganographic technique at their disposal. Period.

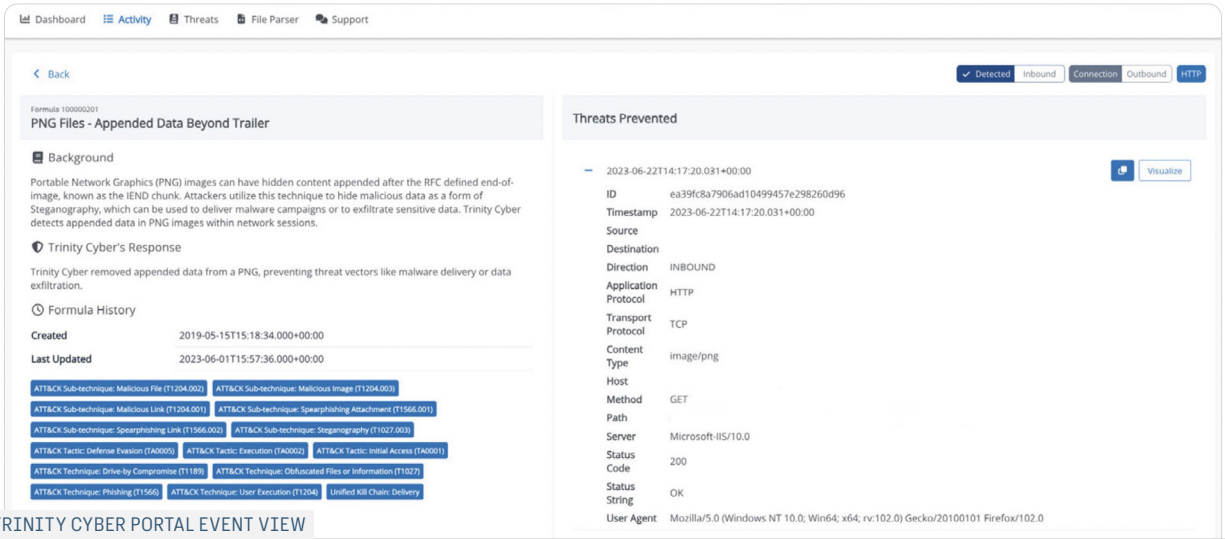

FIGURE 2: TRINITY CYBER PORTAL EVENT VIEW

Trinity Cyber Portal

Appending data to a graphic image file is a common adversary tactic for no better reason other than the fact that other security tools cannot check and cannot stop this technique. Since tools do not check for extra data, data standards for creating and curating images are loose at best. Many image files on web sites now have non-malicious "junk" appended to the content. This makes the technique even more attractive for the adversary because they can hide in the noise created by loosely moderated file creation standards.

Every time an image is cleaned of appended data, an event report is posted to the Trinity Cyber Portal. In the portal's user interface, these events get grouped together by a time range. The default range is set to 15 minutes to reduce the noise generated from the many images being cleaned per day. You can dig into each one and investigate if you want, but the events in these reports show that Trinity Cyber has protected you from this tactic, so there's rarely anything for you to do.

With all the poorly formatted graphic image files on the internet, these events can be voluminous. If you wish, you can exclude them from your Activity view – files will still be cleaned, the events just won't fill your dashboard. Simply add this filter in the Search box:

```
NOT formula.title: "Appended Data Beyond Trailer"
```

If you use our API instead of the UI, you can add a filter to an event query in GQL to exclude or include these events. You can also include or exclude them via your SIEM platform if ingesting from our API.

info@trinitycyber.com
(844) 853-5933

© Trinity Cyber, 2025. All rights reserved.