

New Phishing Scam Hides Malware in Image from James Webb Telescope

September 8, 2022 - There is a new email phishing scam making its way around the globe. Hackers are hiding malicious computer code in an image from the James Webb telescope, and no antivirus software can stop it.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
```

```
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

The picture in question is the first one that was released from the new space telescope. It was made famous when it was released by the White House on July 11th. The image is a deep-field view of a small portion of the sky, which shows thousands of galaxies.

The malware is actually hiding within the coding for the image. And the image is delivered as a Microsoft Office file that is attached to an email. Once opened, the code triggers the download of a malicious Microsoft Office template that infects the computer and begins to steal personally identifiable information as well as website sign-ons and financial data.

At this point, it isn't clear how to clean a computer that has been infected. Anyone who thinks that they may have received the above-mentioned attachment and opened it is advised to disconnect their computer from the internet, and not reconnect until a fix has been found. Victims should also closely monitor their credit cards and bank/brokerage accounts for unauthorized activities.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS