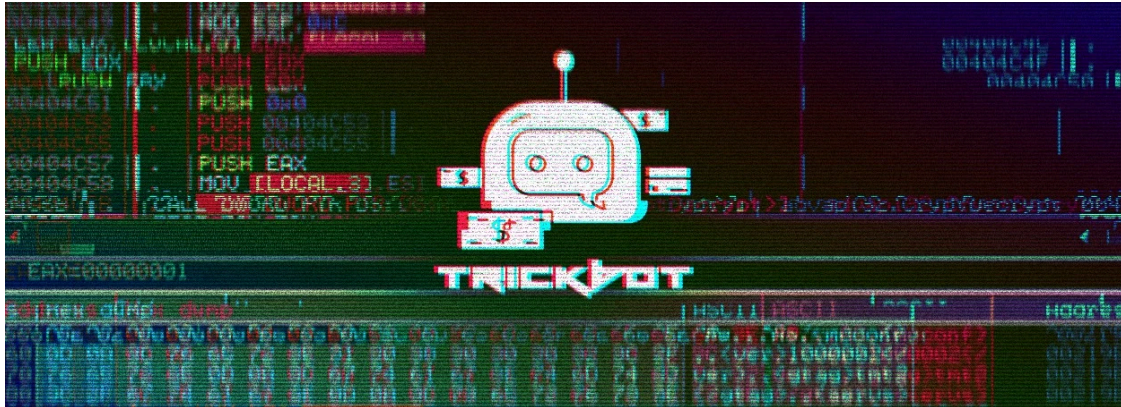


Malware Tries to Trump Security Software With POTUS Impeachment

By Lawrence Abrams

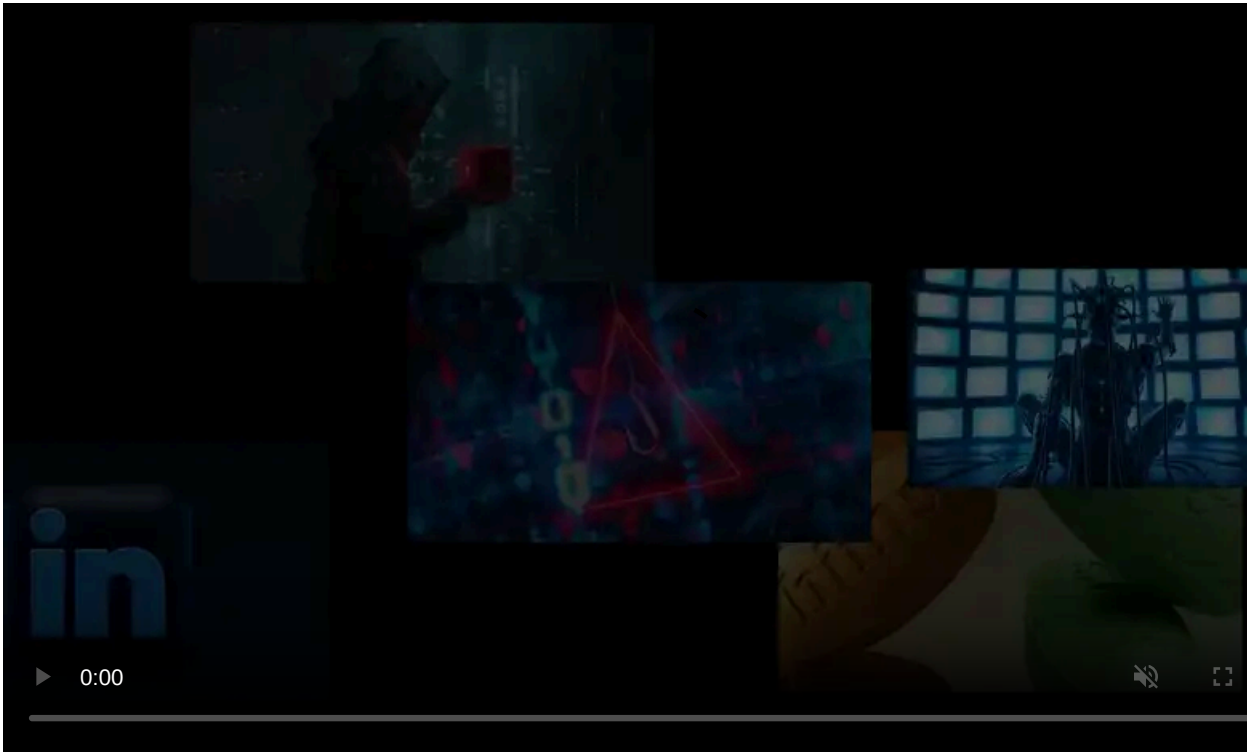
Published: 2020-01-30 · Archived: 2026-04-05 15:32:47 UTC



The TrickBot malware has been spotted using text from articles about President Trump's impeachment to bypass the scanning engines of security software.

Before distributing malware, developers commonly use a crypter to encrypt or obfuscate the malware's code to make it FUD (Fully UnDetectable) by antivirus software.

One common technique used by crypters is to take harmless text from books or news articles and inject it into the malware in the hopes that these strings will be whitelisted by security software.



Visit Advertiser website [GO TO PAGE](#)

This exact technique was [discovered by researchers](#) in the past that allowed them to bypass Cylance's AI-driven scanning engine by adding strings from the Rocket League executable to malware.

The TrickBot trojan appears to be using a similar bypass by using article text from popular news sites.

Trying to Trump security software

In two new samples of TrickBot discovered by Head of SentinelLabs [Vitali Kremez](#) and security researcher [MalwareHunterTeam](#), the malware developers are injecting text from an article about President Trump's impeachment into the malware.

"The anti-virus engines bypasses focus on adding and appending known "goodware" strings to binaries in order to bypass static machine learning engines as similarly it was discovered and used by Cylance engine model," Kremez told BleepingComputer in a conversation. "Known goodware strings might include news headlines like widely populated Trump impeachment news stories mixed with the actual and pseudo-real applications that become appended to the malicious binaries by the malware crypter builder engine."

The [first sample](#) uses text from an impeachment story at [Independent.co.uk](#) and adds it as part of the file information for executable.

File Version Information	
Copyright	© gtime New York adversary Nadler had just spent.
Product	he spiritual guru and former presidential candidate sai
Description	hamber made a point of looking visibly bored
Original Name	and economic dangers, Treasury Secretary Steven Mnuchin
Internal Name	you've been paying attention online, senators have been catching
File Version	1, 0, 0, 1
Date signed	11:05 AM 1/24/2020

TrickBot Sample #1

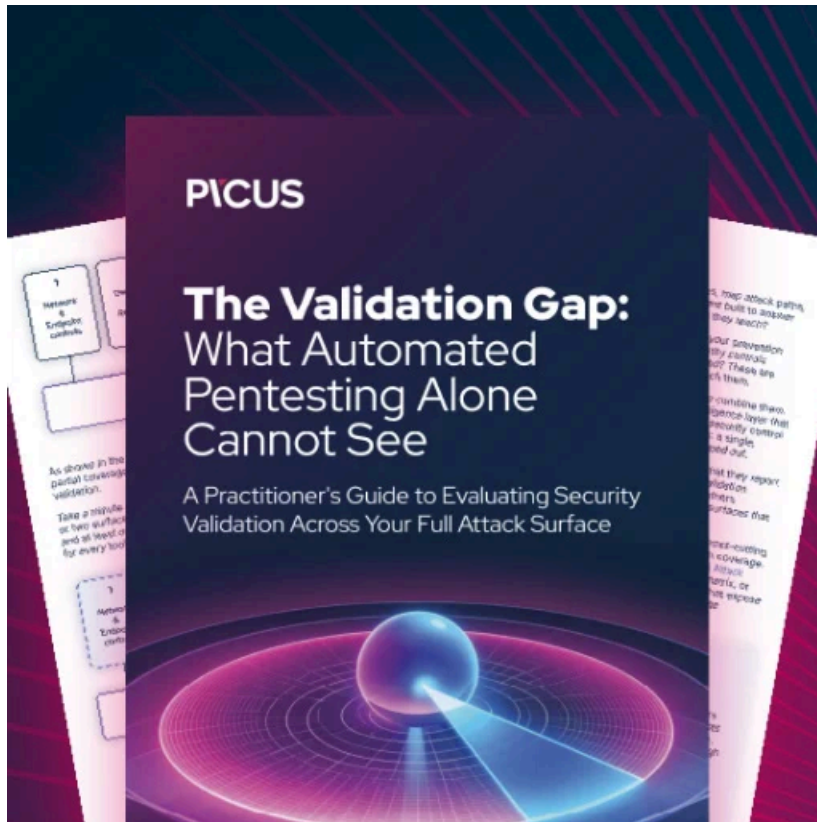
The [second sample](#) uses text ripped from a [CNN article](#) about Trump's impeachment and adds it as custom exif data tags.

```
"Ukrainian natural gas company is at  
rump has lambasted Schiff for previous inaccurately paraphrasing  
Russian propaganda that Ukraine opposed him in 2016,  
Thursday Schiff went line-by-line through the real thing  
investigations was Donald Trump  
foreign leader to get in touch with  
iuliani originated at the White House  
Burisma board. Impeachment managers  
Biden conspiracy theory played against the  
Rudy Giuliani, about two different investigations  
Biden conspiracy theory played against the"
```

It is not 100% clear if this text allowed it to bypass antivirus engines or if other changes were responsible, but when first submitted to VirusTotal, sample 1 was only detected by 11/70 security products and sample 2 was only detected by 6/70.

"This TrickBot crypter and related top cybercrime group invest significant resources in making sure they study and understand anti-virus detection model to be ahead of the game," Kremez explained. "By and large, malware crypters and detections remain to be a "cat-and-mouse" game with the TrickBot and other top crimes groups trying to evade anti-virus models and defense and detection trying to catch up."

It also illustrates how attackers use current events in the proliferation of their malware. Another example shown today is a recent Emotet spam campaign pretending to be [information about the Coronavirus](#).



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/malware-tries-to-trump-security-software-with-potus-impeachment/>