Malicious Memes that Communicate with Malware

By By: Aliakbar Zahravi Dec 14, 2018 Read time: 3 min (753 words)

Published: 2018-12-14 · Archived: 2026-04-05 18:08:20 UTC

Steganography, or the method used to conceal a malicious payload inside an image to evade security solutions, has long been used by cybercriminals to spread malware and perform other malicious operations. We recently discovered malicious actors using this technique on memes. The malware authors have posted two tweets featuring malicious memes on October 25 and 26 via a Twitter account created in 2017. The memes contain an embedded command that is parsed by the malware after it's downloaded from the malicious Twitter account onto the victim's machine, acting as a C&C service for the already- placed malware. It should be noted that the malware was not downloaded from Twitter and that we did not observe what specific mechanism was used to deliver the malware to its victims. The malware connected to this malicious meme has been proactively blocked by Trend Micro machine learning and behavioral detection technology at the time of discovery.

This new threat (detected as TROJAN.MSIL.BERBOMTHUM.AA) is notable because the malware's commands are received via a legitimate service (which is also a popular social networking platform), employs the use of benign-looking yet malicious memes, and it cannot be taken down unless the malicious Twitter account is disabled. Twitter has already taken the account offline as of December 13, 2018.

Hidden inside the memes mentioned above is the "/print" command, which enables the malware to take screenshots of the infected machine. The screenshots are sent to a C&C server whose address is obtained through a hard-coded URL on pastebin.com.

Analyzing the Malware

We found that once the malware has been executed on an infected machine, it will be able to download the malicious memes from the Twitter account to the victim's machine. It will then extract the given command. In the case of the "print" command hidden in the memes, the malware takes a screenshot of the infected machine. It then obtains the control server information from Pastebin. Afterwards, the malware sends out the collected information or the command output to the attacker by uploading it to a specific URL address.

 A screen capture of the malware's code showing the Pastebin URL

Figure 1. A screen capture of the malware's code showing the Pastebin URL

During analysis, we saw that the Pastebin URL points to an internal or private IP address, which is possibly a temporary placeholder used by the attackers.

 Private IP address that a Pastebin URL points to

Figure 2. Private IP address that a Pastebin URL points to

The malware then parses the content of the malicious Twitter account and begins looking for an image file using the pattern: “” on the account.


A screen capture of the malicious Twitter account

Figure 3. A screen capture of the malicious Twitter account


A screen capture of one of the malicious memes posted on the Twitter account

Figure 4. A screen capture of one of the malicious memes posted on the Twitter account

At the time of analysis, the two memes (DqVe1PxWoAIQ44B.jpg and DqfU9sZWoAAlnFh.jpg) contained the command “print”. The embedded commands instruct the malware to perform various operations on the infected machine, such as capture screenshots, collect system information, among others, as described below.

Once the malware downloads the image, it attempts to extract the command that starts with the ‘/’ character.


A screen capture of code snippet to locate a command string

Figure 5. A screen capture of code snippet to locate a command string

The following is the list of commands supported by this malware:

Commands	Description
/print	Screen capture
/processos	Retrieve list of running processes
/clip	Capture clipboard content
/username	Retrieve username from infected machine
/docs	Retrieve filenames from a predefined path such as (desktop, %AppData% etc.)


A screen capture of code featuring the commands supported by the malware

Figure 6. A screen capture of code featuring the commands supported by the malware

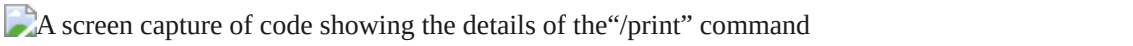
A screen capture of code showing the details of the“/print” command

Figure 7. A screen capture of code showing the details of the“/print” command

Trend Micro Solutions

Users and businesses can consider adopting security solutions that can protect systems from various threats, such as malware that communicate with benign-looking images, through a cross-generational blend of threat defense techniques. Trend Micro endpoint solutions such as the **Smart Protection Suites**products and **Worry-Free Business Security** solutions can protect users and businesses from threats by detecting malicious files and

messages as well as blocking all related malicious URLs. **Trend Micro™ Deep Discovery™**products has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

These solutions are powered by Trend Micro™ XGen™ security, which provides high-fidelity machine learning that secures the gateway and endpoint, and protects physical, virtual, and cloud workloads. With technologies that employ web/URL filtering, behavioral analysis, and custom sandboxing, XGen security offers protection against ever-changing threats that bypass traditional controls and exploit known and unknown vulnerabilities.

Indicators of Compromise

Related Hashes (SHA-256)

- 003673cf045faf0141b0bd00eff13542a3a62125937ac27b80c9ffd27bb5c722
- 3579d609cf4d0c8b469682eb7ff6c65ec634942fa56d47b666db7aa99a2ee3ef
- 88b06e005ecfab28cfdbcab98381821d7cc82bb140894b7fdc5445a125ce1a8c
- 8cdb574ba6fcaea32717c36b47fec0309fcd5c6d7b0f9a58fc546b74fc42cacd

Tags
