DTPacker

Threat: **Malware Packer**

Author: **Jeffrey Farnan** Date Originally Published: **February 28th, 2022**

1. SUMMARY

- A new .NET malware packer has been discovered which has been dubbed DTPacker. This packer has been observed distributing multiple RATs and information stealers, such as Agent Tesla, Ave Maria, AsyncRAT and Formbook. One of the campaigns it uses is to lure users onto fake soccer sites, one of them been a fake Liverpool Football Club site where users were fooled into downloading the DTPacker delivering the malicious payload.

2. MALWARE FAMILY

- **Type** = Malware Packer.
- **Sub-type** = Remote Access Trojans (RATs), Infostealers, Ransomware, etc.

- Malware Packers are tools to mask malicious files by encrypting, compressing or changing the format of the payload to make it look like something else entirely. The payloads can be Rats, Trojans or Ransomware but by been packed these files can go undetected by anti-virus software and security researchers.
- There are many types of packers some can be bought but others can also be custom built. The most common packers are: UPX, MPRESS, ExeStealth, Andromeda, VMProtect and PESpin.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Unknown.
- **First seen date/period** = January 2020.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = February 11th, 2022.

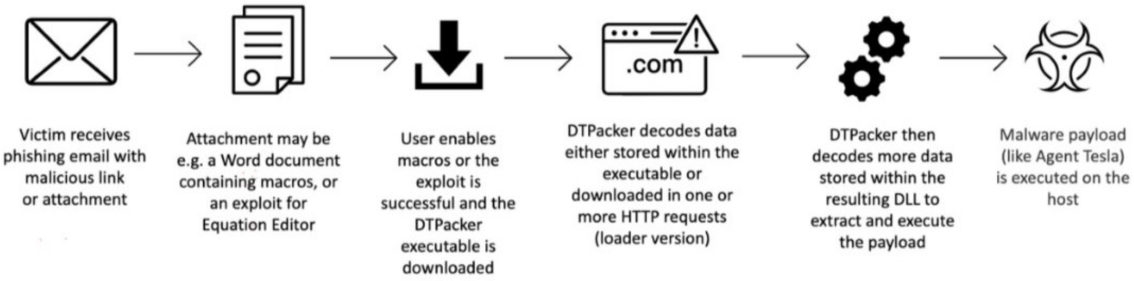
4. MALWARE HISTORY

- A packer is defined as a packed file when executed unpacks itself in memory. Malware uses packing and other forms of obfuscation in order to foil analysis by anti-virus systems. Packers use a variety of methods combined with file encryption in order to prevent reverse engineering and to hinder analysis of the program.

- Researchers have observed DTPacker being used by threat actors in 2020 that is known for delivering banking Trojans to victims in Europe and Asia. It has been used by several threat actors in multiple campaigns such as phishing campaigns and embedded in fake websites.

5. MALWARE DESCRIPTION

- Proofpoint identified a new malware packer dubbed DTPacker. It's called DTPacker because the payload was decoded using the passwords related to Donald Trump, which were trump2020 and Trump2024. This malware is used to distribute Remote Access Trojans used to steal information and can lead to follow on attacks such as ransomware. This packer can be distributed in many different way such as phishing campaigns but recently it has been spotted embedded into a fake website designed to look like the genuine Liverpool Football Club site.
- **Packer / Downloader:** Malware typically has two forms, a packer and a downloader, the main difference between these is at location of the payload data. A packer typically embeds payload data in something like an image file, while the later involves downloading the payload. The first stage decodes an embedded or downloaded resource, while the second stage extracts and executes the payload. Poofpoint said that DTPacker uses both forms, giving the threat actors more flexibility. Downloading a payload from a hosted location allows the file to be modified on the server side. Using an embedded payload doesn't require reaching out to the internet which provides one less signal for detection attempts."
- **Payload:** When the payload is decrypted in memory it's executed on the system. Some of the payloads this packers has been distributing includes multiple RAT's and information stealers including Agent Tesla, Ave Maria, AsyncRAT, and FormBook.
- **Phishing Campaigns:** Phishing emails has been observed with a malicious document which is used as the initial infection vector.


.com
Victim receives phishing email with malicious link or attachment
Attachment may be e.g. a Word document containing macros, or an exploit for Equation Editor
User enables macros or the exploit is successful and the DTPacker executable is downloaded
DTPacker decodes data either stored within the executable or downloaded in one or more HTTP requests (loader version)
DTPacker then decodes more data stored within the resulting DLL to extract and execute the payload
Malware payload (like Agent Tesla) is executed on the host

- The email contains an attachment, usually a malicious document (such as a Word document containing macros) or compressed executable, which downloads the DTPacker executable. Once downloaded, DTPacker then decodes data that is stored within the executable or downloaded in one or more HTTP requests. Once the packer is on the system it can decode its data and execute the payload.
- **Obfuscation:** This malware has been very effective in evading security measures. It uses multiple obfuscation techniques to bypass antivirus and sandbox analysis. This malware is likely being distribute in underground forums.

6. POTENTIAL CUSTOMER DEFENSES

Packers are not inherently bad, they help to protect files, data and applications. They are a great resource for Malware developers helping to obfuscate file code making it difficult to detect and be analyzed. Although unpacking a suspicious file is normally beyond most users, here is some helpful measures you can take:

- Have anti-malware software on all your devices, having it updated can help protect you against suspicious packers.
- If the file is packed with UPX a simple solution is to download UPX and using the following command line the file can be unpacked: **upx -d -o unpacked.exe packed.exe**
- If a file is packed by an unknown vender or one of those venders mentioned above, the best course of action is to delete it. If the packed file comes from an unknown vendor or untrusted website and you are suspicious of it, again the best course of action is to delete it.

Research Sources:

- https://sensorstechforum.com/dtpacker-loader-packer-malware/
- https://threatpost.com/donald-trump-packer-malware-infostealers/177887/
- https://thehackernews.com/2022/01/hackers-using-new-malware-packer.html
- https://www.proofpoint.com/us/blog/threat-insight/dtpacker-net-packer-curious-password-1
- https://resources.infosecinstitute.com/topic/top-13-popular-packers-used-in-malware/
- https://duo.com/decipher/dtpacker-malware-steals-data-loads-second-stage-payloads

Disclaimer: All opinions expressed in this article are the opinions solely of the author.