New Trojan in Town: Meet the Zberp Trojan

securityintelligence.com/new-zberp-trojan-discovered-zeus-zbot-carberp/

May 22, 2014

Advanced Threats May 22, 2014

By Dana Tamir 4 min read

A New Trojan in Town: Meet Zberp

Trusteer researchers recently discovered a new Trojan that has been targeting more than 450 financial institutions around the world, mainly in the U.S., U.K. and Australia. The new Trojan, which seems to be a variant of the well-known Zeus Trojan (a.k.a. Zbot), also demonstrates behaviors associated with the Carberp Trojan family. Therefore, we named it the **Zberp** Trojan.

According to an analysis conducted by Trusteer researchers Martin G. Korman and Tal Darsan, the Trojan seems to have been assembled from the leaked source code of two well-known Trojans: Zeus and Carberp. The Zeus source code was exposed to the public in 2011, and it is already used by some criminal groups that customize its behavior and develop new features. The Carberp source code was offered for sale last year.

“Since the source code of the Carberp Trojan was leaked to the public, we had a theory that it won’t take cyber criminals too long to combine the Carberp source code with the Zeus code and create an evil monster,” explained Korman and Darsan. “It was only a theory, but a few weeks ago we found samples of the ‘Andromeda’ botnet that were downloading the hybrid beast.”

The new **Zberp Trojan**, a variant of the Zeus VM Trojan, enables cyber criminals to grab basic information about the infected computer, including the Computer name, IP and more. It can take screen shots and send them to the attacker. It steals data submitted in HTTP forms, user SSL certificates and even FTP and POP account credentials. The Zberp Trojan also includes optional features that enable Web injections, dynamic Web injections, MITB/MITM attacks and VNC/RDP connections.

In addition to its malicious capabilities, the Zberp Trojan uses a combination of evasion techniques that it inherited from both the Zeus and the Carberp Trojans.

Zberp uses an “invisible persistence” feature that is has been used by the Zeus VM variant: the malware deletes its persistence key from the registry during the Windows startup process to prevent security solutions from detecting it during normal system scans that take place after the system boots. To ensure persistency, however, the malware rewrites the persistence key back to the registry during system shutdown.

The Trojan also disguises the configuration code in an image file through steganography, a technique used by malware authors to embed code in a file format that looks legitimate and bypasses malware detection solutions.

```
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  □″□ℵ..JFIF......
00 01 00 00 FF FE 00 3C 43 52 45 41 54 4F 52 3A  ....□ .<CREATOR:
20 67 64 2D 6A 70 65 67 20 76 31 2E 30 20 28 75   gd-jpeg v1.0 (u
73 69 6E 67 20 49 4A 47 20 4A 50 45 47 20 76 36  sing IJG JPEG v6
32 29 2C 20 71 75 61 6C 69 74 79 20 3D 20 31 30  2), quality = 10
30 0A FF DB 00 43 00 01 01 01 01 01 01 01 01 01  0.□□.C..........
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  ................
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  ................
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  ................
01 01 01 01 01 01 01 FF DB 00 43 01 01 01 01 01  .......□□.C.....
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  ................
```

Figure 1: The header of the configuration image

Figure 2: The configuration is disguised in an “Apple” image

```
07 00 41 58 2B 74 53 71 37 32 2B 36 6A 54 63 52  ..AX+tSq72+6jTcR
72 58 52 41 69 53 6E 77 6A 42 5A 4B 38 6D 76 35  rXRAiSnwjBZK8mv5
58 7A 64 78 71 63 6C 54 47 32 71 67 6E 45 2F 38  XzdxqclTG2qgnE/8
32 64 34 72 6E 43 47 57 39 50 35 4F 41 6E 6F 62  2d4rnCGW9P5OAnob
52 55 78 50 2F 4E 6E 65 4B 35 77 68 6C 76 54 2B  RUxP/NneK5whlvT+
54 67 4A 36 47 30 56 4D 54 2F 7A 5A 33 69 75 63  TgJ6G0VMT/zZ3iuc
49 5A 62 30 2F 6B 34 43 65 68 74 46 54 45 2F 38  IZb0/k4CehtFTE/8
32 64 34 72 6E 43 47 57 39 50 35 4F 41 6E 6F 62  2d4rnCGW9P5OAnob
52 55 78 50 2F 4E 6E 65 4B 35 77 68 6C 76 54 2B  RUxP/NneK5whlvT+
54 67 4A 36 47 30 56 4D 54 2F 7A 5A 33 69 75 63  TgJ6G0VMT/zZ3iuc
49 5A 62 30 2F 6B 34 43 65 68 74 46 54 45 2F 38  IZb0/k4CehtFTE/8
32 64 34 72 6E 43 47 57 39 50 35 4F 41 6E 6F 62  2d4rnCGW9P5OAnob
52 55 78 50 2F 4E 6E 65 4B 35 77 68 6C 76 54 2B  RUxP/NneK5whlvT+
54 67 4A 36 47 30 56 4D 54 2F 7A 5A 33 69 75 63  TgJ6G0VMT/zZ3iuc
49 5A 62 30 2F 6B 34 43 65 68 74 46 54 45 2F 38  IZb0/k4CehtFTE/8
32 64 34 72 6E 43 47 57 39 50 35 4F 41 6E 6F 62  2d4rnCGW9P5OAnob
52 55 78 50 2F 4E 6E 65 4B 35 77 68 6C 76 54 2B  RUxP/NneK5whlvT+
54 67 4A 36 47 30 56 4D 54 2F 7A 5A 33 69 75 63  TgJ6G0VMT/zZ3iuc
```

Figure 3: The base64 encoded configuration hidden within the image

The Carberp source code contribution to the Zberp Trojan can be seen in its “hooking” technique, commonly used by malware developers to control the browser, grab key strokes and steal information. It also keeps the malware “invisible,” evading detection by anti-virus and anti-malware tools.

The figure below shows that the hook is implemented in the same place, but its implementation is slightly different: The push instruction highlighted in the Carberp code (on the left) was changed by one byte in the Zberp code (on the right), and a 'mov' instruction was added to it. These changes ensure that even security solutions capable of detecting Carberp variants will not identify the new code.

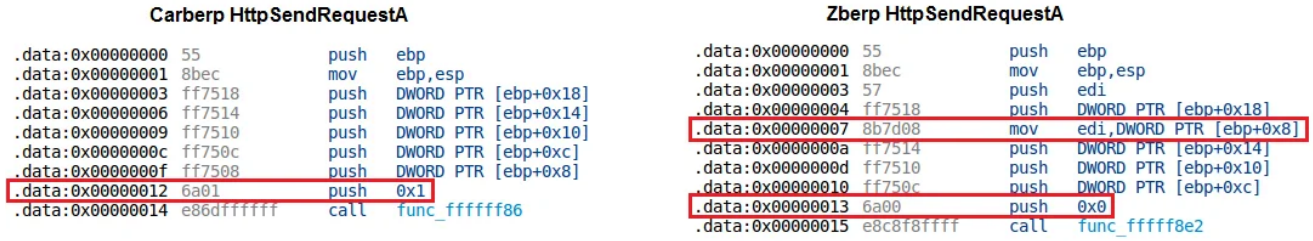

Figure 4: Comparison between Carberp and Zberp hooks

Another evasion technique that has been embedded in the Zberp Trojan is the use of SSL, which secures the communications with the Command and Control server and evades detection by network security products.

According to a Virus-Total scan, the Zberp Trojan was able to evade most anti-virus solutions when it was first detected. Trusteer's endpoint protection solutions, which do not require prior knowledge about emerging threats in order to stop them, detected and removed the Zberp Trojan immediately — on 'day zero.'

How Trusteer Customers Are Protected

Trusteer Customers Are Protected!

Trusteer, an IBM company, is the leading provider of endpoint cyber crime prevention. Trusteer solutions combine multi-layer defenses with real-time threat intelligence to achieve sustainable protection against malware and targeted attacks.

Preventing Enterprise Breach

Trusteer Apex protects enterprise endpoints by preventing infections via the exploitation of vulnerabilities in endpoint applications. In addition, it detects, mitigates and removes Zberp (and other Zeus variants) from infected user devices. No product update is needed.

Preventing Online Financial Fraud

Trusteer Rapport protects customer endpoints by detecting, mitigating and removing Zberp (and other Zeus variants) from infected devices. No product update is needed.

Trusteer Pinpoint Malware Detection can identify and warn organizations of malware-infected devices that attempt to log in and transact with their website. No product update is needed.

Dana Tamir
Director of Enterprise Security at Trusteer, an IBM Company

Dana Tamir is Director of Enterprise Security at Trusteer, an IBM Company. In her role she leads activities related to enterprise advanced threat protection ...