radware

Smart Network. Smart Business.

ERT Threat Alert

New Trojan Found: Admin.HLP

Leaks Organizations Data

Eyal Benishti

Security Researcher, ERT

28.08.2012

Contents

Executive Summary

Radware's ERT Research Lab released a threat alert regarding a new Trojan Key Logger malware, named **Admin.HLP**, that was found 28 August, 2012 for the first time at one of its customers.

Admin.HLP, the newly found Trojan, is malicious software that monitors keystrokes on the victim's computer, collects user passwords, credit card numbers and other sensitive information. It then sends all the stolen data out of the organization to the attackers' remote servers over secured HTTPS connection.

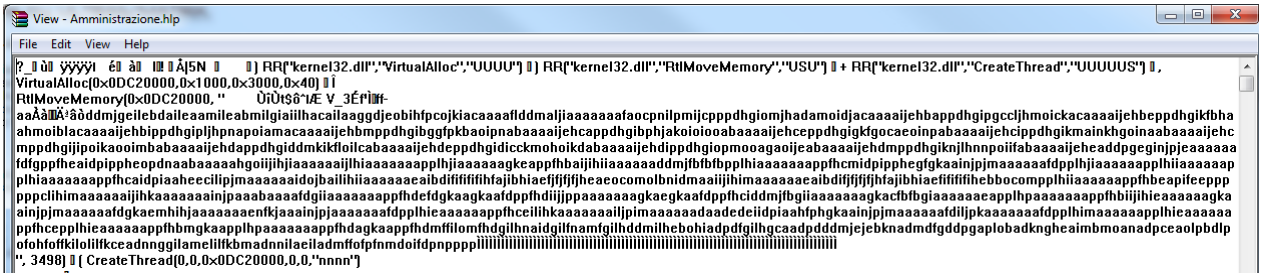
The Admin.HLP Trojan is hidden within a standard windows help file named **Amministrazione.hlp** and it is attached to emails. This standard help file does not activate any installed anti-virus programs, and therefore it goes under the radar of standard anti-virus solutions. Once the victim opens the Windows help file, the Admin.HLP Trojan installs itself on the victim's computer where it starts to collect keystrokes. The Trojan periodically sends the stored keystrokes to the attackers' remote server.

To remain a persistent Trojan threat, Admin.HLP creates a startup file in Windows, guaranteeing that the Trojan is invoked after every restart of the computer.

Technical Details

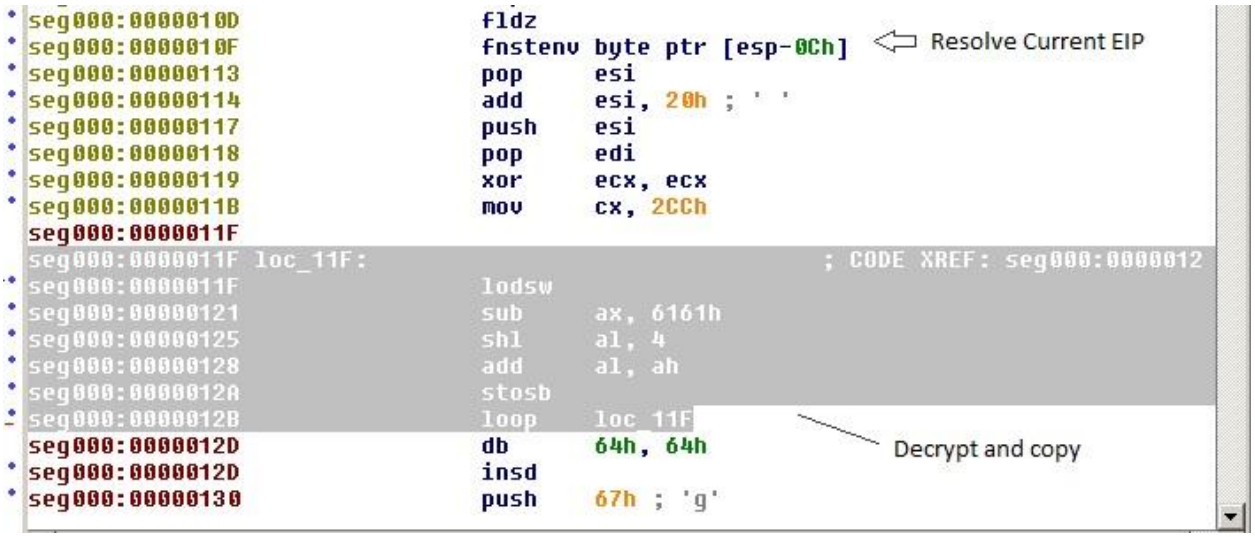
File Name: Amministrazione.hlp
SHA256 :
c574182165297d759324e3f155e876aa020957c73cf73b6dbb23530a7faf32ec
OS : XP SP3

By using HLP-script language, the attacker is able to inject the encrypted malicious payload and execute the stub to decrypt the Trojan code.



The Trojan is copying the code to a predefined location and starting a new thread to execute the malicious code.

The decryption stub is responsible for the code decryption.

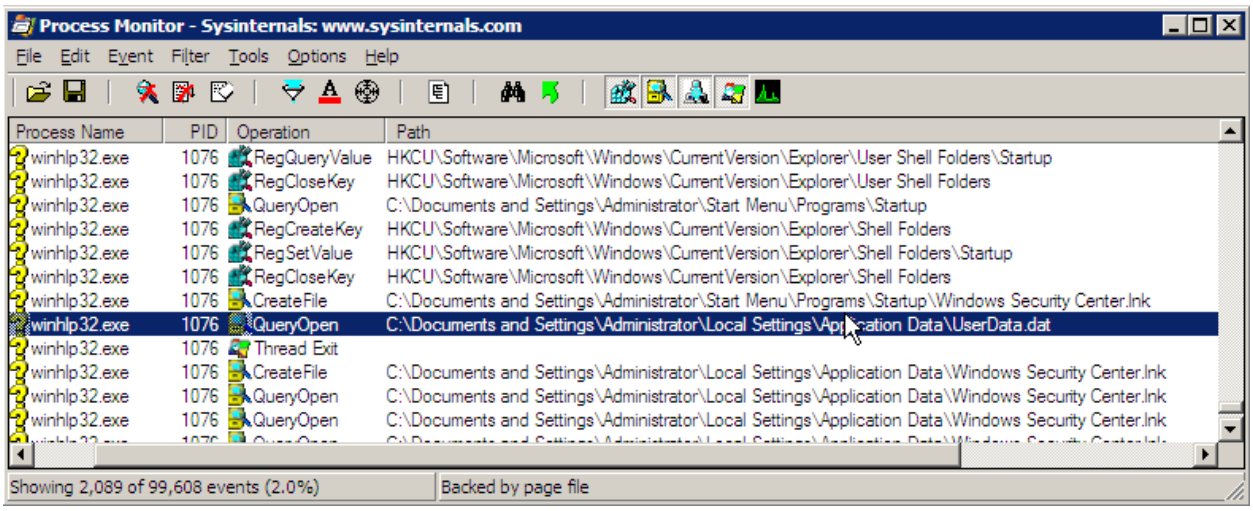


Once the Trojan is executing, it is injecting itself into **EXPLORER.EXE**.

The Trojan is implementing a Key Logger and the output is saved into **UserData.dat** file under the '**Application Data'** directory.

```
9   [08/27/2012 11:13:41] (C:\Documents and Settings\Administrator\Local Settings\Application Data)
10  testing the keylogger in action
11  [08/27/2012 13:19:19] (Run)
12  cmd
```

In addition, for persistency reasons, the Trojan is creating a startup file named '**Windows Security Center.lnk'** pointing to '**Windows Security Center.exe'** under 'Application Data' directory, this link is being watched by the process and being recreated upon removal.



The Trojan is sending the collected information (Passwords, Credit Card numbers, etc.,) to **images.zyns.com** over HTTPS.

Radware ERT Advice:

Radware's ERT team has created a signature to block all communication between infected organizations and the attackers' remote servers. This prevents data leakage from the organization at all costs, no matter how many computers are infected in the organization or how difficult is it to remove the Trojan from the end users computers.

Radware's customers are encouraged to contact our ERT and to receive immediate assistance. Other prospects and non-Radware customers can contact our ERT through a Radware representative.