

# Ensiko: A Webshell With Ransomware Capabilities

[blog.trendmicro.com/trendlabs-security-intelligence/ensiko-a-webshell-with-ransomware-capabilities/](https://blog.trendmicro.com/trendlabs-security-intelligence/ensiko-a-webshell-with-ransomware-capabilities/)

July 27, 2020



Ensiko is a PHP web shell with ransomware capabilities that targets various platforms such as Linux, Windows, macOS, or any other platform that has PHP installed. The malware has the capability to remotely control the system and accept commands to perform malicious activities on the infected machine.


It can also execute shell commands on an infected system and send the results back to the attacker via a PHP reverse shell. It is capable of scanning servers for the presence of other webshells, defacing websites, sending mass emails, downloading remote files, disclosing information about the affected server, brute-force attacks against file transfer protocol (FTP), cPanel, and Telnet, overwriting files with specified extensions, and more.

## Technical Details

### Webshell Authentication

The malware has the ability to be password-protected. For authentication, the malware displays a Not Found page with a hidden login form as seen in the next two figures:

 Not Found page and hidden login form Figure 1. Not Found page and hidden login form

 PHP code for password authentication Figure 2. PHP code for password authentication

The password for this sample is “**RaBiitch**”, while the following figure shows captured network traffic for an authentication request to the web shell panel:

 Captured network traffic Figure 3. Captured network traffic

 Appearance of Ensiko webshell Figure 4. Appearance of Ensiko webshell

### Webshell features

The following is a list of Ensiko’s capabilities:


Features	Description
Priv Index	Download ensikology.php from pastebin


Ransomware	Encrypt files using RIJNDAEL 128 with CBC mode
CGI Telnet	Download CGI-telnet version 1.3 from pastebin; CGI-Telnet is a CGI script that allows you to execute commands on your web server.
Reverse Shell	PHP Reverse shell
Mini Shell 2	Drop Mini Shell 2 webshell payload in <code>./tools_ensikology</code>
IndoXploit	Drop IndoXploit webshell payload in <code>./tools_ensikology/</code>
Sound Cloud	Display sound cloud
Realtime DDOS Map	Fortinet DDoS map
Encode/Decode	Encode/decode string buffer
Safe Mode Fucker	Disable PHP Safe Mode
Dir Listing Forbidden	Turn off directory indexes
Mass Mailer	Mail Bombing
cPanel Crack	Brute-force cPanel, ftp, and telnet
Backdoor Scan	Check remote server for existing web shell
Exploit Details	Display system information and versioning
Remote Server Scan	Check remote server for existing web shell
Remote File Downloader	Download file from remote server via CURL or wget
Hex Encode/Decode	Hex Encode/Decode
FTP Anonymous Access Scanner	Search for Anonymous FTP
Mass Deface	Defacement
Config Grabber	Grab system configuration such as <code>"/etc/passwd"</code>
SymLink	link
Cookie Hijack	Session hijacking
Secure Shell	SSH Shell
Mass Overwrite	Rewrite or append data to the specified file type.
FTP Manager	FTP Manager
Check Steganologer	Detects images with EXIF header
Adminer	Download Adminer PHP database management into the <code>./tools_ensikology/</code>
PHP Info	Information about PHP's configuration
Byksw Translate	Character replacement

 Code listing Ensiko features Figure 5. Code listing Ensiko features

### Ransomware Analysis


The malware uses PHP **RIJNDAEL\_128** with **CBC mode** to encrypt files in a web shell directory and subdirectories and appends filenames with the “.bak” extension. The following code snippet demonstrates this behavior of the malware:

 Code showing encryption behavior Figure 6. Code showing encryption behavior

 Encryption and decryption code Figure 7. Encryption and decryption code

 Webshell portion with ransomware key Figure 8. Webshell portion with ransomware key


 Log of files being encrypted Figure 9. Log of files being encrypted


 Encrypted files in directory Figure 10. Encrypted files in directory

 POST request to affected server Figure 11. POST request to affected server

The malware also drops an index.php file and sets it as the default page using a .htaccess file; the attacker is also notified of this action via email. The following code snippet shows this behavior:

 Code snippet for dropped .htaccess page Figure 12. Code snippet for dropped .htaccess page

 The notification that appears when index.php is accessed Figure 13. The notification that appears when index.php is accessed

 Appearance of index.php page Figure 14. Appearance of index.php page

 Encoded form of index.php Figure 15. Encoded form of index.php

 Decoded appearance of index.php Figure 16. Decoded appearance of index.php


### Tool Set


To carry out more tasks on an infected system, the malware can load various additional tools onto an infected system. Most of these tools are loaded from Pastebin. The malware creates a directory called tools\_ensikology to store these tools.

 Tools loaded from Pastebin Figure 17. Tools loaded from Pastebin

### Steganologer

There is a technique in which a malicious actor hides code within the exchangeable image file format (EXIF) headers of an image file and uses a PHP function called `exif_read_data` to extract and run this code on an affected server. The steganologer function identifies images with EXIF headers and labels them as a logger. In the following screenshot, test1.jpg and test2.jpg both have EXIF headers with hidden code and are identified s.


 Files with hidden code Figure 18. Files with hidden code

 Code for identifying files with hidden executable code Figure 19. Code for identifying files with hidden executable code

### Backdoor Scan

A backdoor scan checks a given remote host for the existence of a webshell from a hardcoded list.

 first screenshot of code for finding other webshells on affected server

 Second screenshot of code for finding other webshells on affected server Figures 20 and 21. Code for finding other webshells on affected server

### Remote server scan


Like a backdoor scan, the remote server scan function-checks the remote server for the presence of other web shells. However, instead of using a hardcoded list, it accepts manual input for files to be searched for:


 Interface for checking for other webshells

 Code for checking for other webshells Figures 22 and 23. Interface and code for checking for other webshells

### **Mass Overwrite**

The Mass Overwrite function can rewrite/append the content of all files with specified extensions and directories, including all subdirectories of a web shell.

 User interface for overwriting files

 Code for overwriting files Figures 24 and 25. User interface and code for overwriting files

## **Conclusion**

---

Ensiko is a web shell used by an attacker that enables remote administration, file encryption, and many more features on a compromised web server. A common method to deploy web shell is exploiting web application vulnerabilities or \*gaining access to an already compromised server. Additionally, Ensiko has ransomware capability to encrypt files on an infected web server using the RIJNDAEL encryption algorithm. It is also capable of scanning servers for the presence of other web shells, defacing websites, sending mass emails, downloading remote files, disclosing information about the affected server, gaining access to databases, running brute-force attacks against file transfer protocol (FTP), cPanel, and Telnet, overwriting files with specified extensions, and more.

### **Indicators of Compromise**

<b>SHA-256 Hash</b>	<b>Trend Micro Detection Name</b>
5fdbf87b7f74327e9132b5edb5c217bdcf49fe275945d502ad675c1dd46e3db5	Trojan.PHP.WEBSHELL.SBJKSJ

### Ransomware

This article discusses Ensiko, a PHP web shell with ransomware capabilities that targets various platforms such as Linux, Windows, or macOS that has PHP installed. It can remotely control a system and accept commands to run on the infected machine.

By: Aliakbar Zahravi July 27, 2020 Read time: ( words)

Content added to Folio