UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

*Join the Global Conversation*

**The Citizen Lab**

**Research Brief**
Number 4 – May 2012

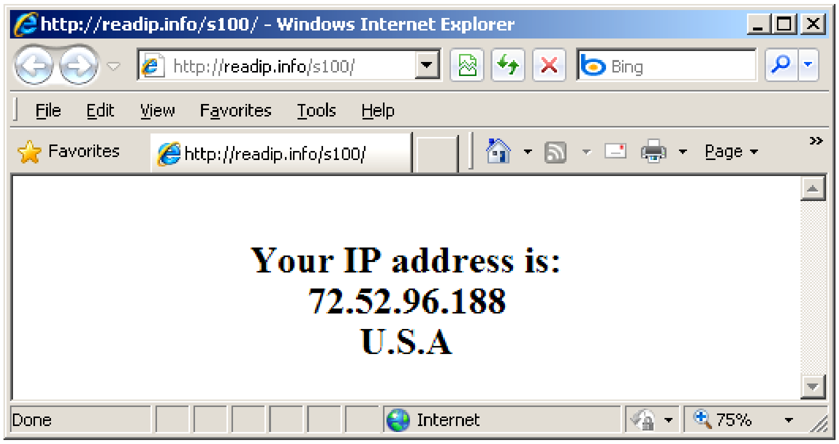
# *Iranian Anti-Censorship Software 'Simurgh' Circulated with Malicious Backdoor*

By Morgan Marquis-Boire

## FINDINGS

Simurgh is an Iranian stand-alone proxy software for Microsoft Windows. It has been used mainly by Iranian users to bypass censorship since 2009. The downloadable file is less than 1 MB and can be downloaded within a reasonable amount of time even with a slow internet connection, which makes it convenient for many users in Iran. Simurgh runs without prior installation or administrator privileges on the computer and therefore, can be copied and used from a USB flash drive on any shared computer (i.e Internet cafes).

Simurgh is available for free download from its official website https://simurghesabz.net. After running the executable file, a user interface (see below) opens. When the user clicks "Start", Simurgh will attempt to establish a secure connection. The web browser will then open a new window to provide users with a test page, confirming their secure connection originating from a different country.


http://readip.info/s100/ - Windows Internet Explorer
http://readip.info/s100/
Bing
File Edit View Favorites Tools Help
Favorites
http://readip.info/s100/
Page
Done
Internet
75%

Your IP address is:
72.52.96.188
U.S.A

It has recently come to our attention that this software is being recommended and circulated among Syrian Internet users for bypassing censorship in their country. This information led to the discovery and analysis of a back-doored version of this software.

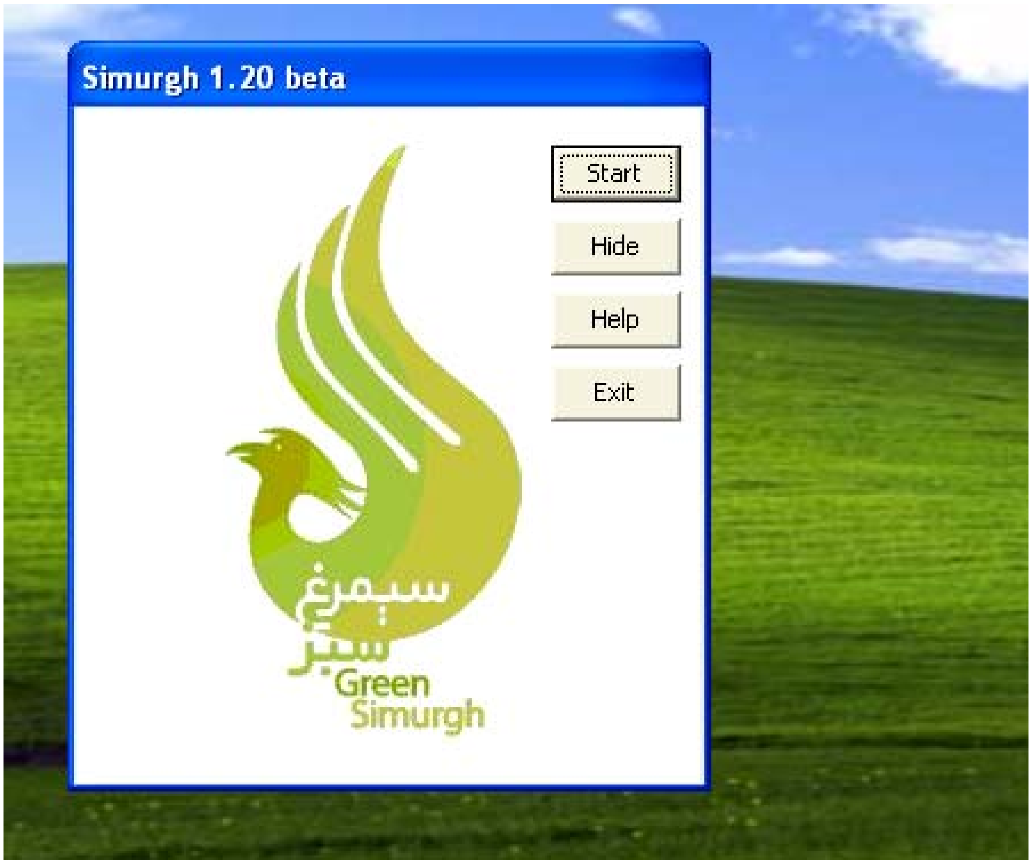
The malicious copy will install the Simurgh software, but will also install an undesirable backdoor on the victim’s computer. This software is distributed as “Simurgh-setup.zip” and is identifiable via the following md5 and sha256 hashes:

5e2a714fdfc2309af843056e8c5ae7d3 Simurgh-setup.zip
9c1a238d87e3bad41708c2e98f753442a224ed9df994e1a34083b2bf336047e5 Simurgh-setup.zip

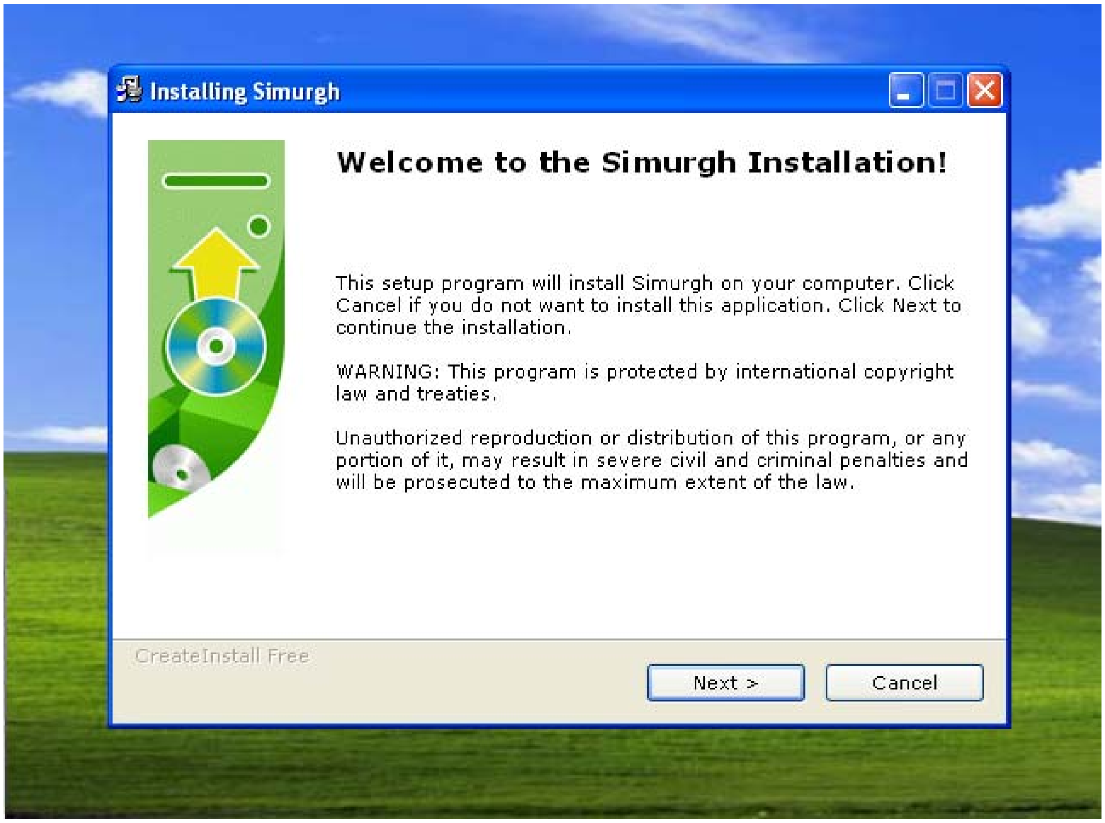
When you unzip this file you are presented with Simurgh-setup.exe

379480c807812f3521466f7ff5ffa273 Simurgh-setup.exe
e20438a4cf90b67dab613451cc5b3bc35256413461dafdfc35425429d8d478df Simurgh-setup.exe

The installer from the most recent legitimate version of Simurgh looks like this:



Executing the malicious version starts an installation dialogue which looks like this:



Welcome to the Simurgh Installation!

This setup program will install Simurgh on your computer. Click Cancel if you do not want to install this application. Click Next to continue the installation.

WARNING: This program is protected by international copyright law and treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties and will be prosecuted to the maximum extent of the law.

In addition to creating a copy of Simurgh in:

**C:\Program Files\Simurgh\Simurgh.exe**

The malicious GUI installer drops 4 binaries in C:\windows\system32\drivers:

MSINET.OCX – 73da54b69911bdd08ea8bbbd508f815ef7cfa59c4684d75c1c602252ec88ee31
richtx32.ocx – 318cc48cbcfaba9592956e4298886823cc5f37626c770d6dadbcd224849680c5
shdocvw.dll – fdae6764d190bf265dbc2df352174ccdcc97b1680545e348f1ee1111b0808693
lsass.exe – 9320d247dd94f610f31037df8eda75fe79991f126d2e55d35a9532d09ff79896

The first three files are legitimate Microsoft system files which appear to be dependencies of the fourth, ‘lsass.exe’. This file is VB6 native code and is installed as an implant to allow persistent access to the victim’s computer and to provide data exfiltration capabilities.

As part of the installation the following registry entry is written which ensures the running of the Trojan on logon:

HKLM\software\microsoft\windows nt\currentversion\winlogon\shell explorer.exe
C:\WINDOWS\system32\drivers\lsass.exe REG_SZ 0

On startup, ‘lsass.exe’ deletes ‘C:\WINDOWS\Media\Windows XP Start.wav’. This file is the ‘navigation’ sound in Explorer, IE, and other applications based on a common set of controls. Since ‘lsass.exe’ uses several of these controls, this is presumably done to prevent ‘clicking’ sounds during the operation of the implant. However, this will also lead to a lack of navigation sounds in other applications, where they would be expected.

In addition to ensuring persistence, ‘lsass.exe’ enumerates basic details of the system (IP address, hostname, victim username) and provides keylogging functionality. This binary contains three javascript files which are written out as the text files:

C:\WINDOWS\system32\win.txt
C:\WINDOWS\system32\1.txt
C:\WINDOWS\system32\2.txt

These act as basic HTML templates for data mined from the victim’s system (such as keystrokes). Processing of ‘win.txt’ renames it to ‘upl.htm’ which is then sent via HTTP post request to a remote site registered with a Saudi Arabian ISP.

If this Trojan is found to be installed on a computer one must consider all online accounts (E-mail, banking, etc.) to have been compromised and it is advised that all online passwords be changed as soon as possible. While this Trojan is detected by most anti-virus software as malicious, AV software cannot always be guaranteed to clean up an infected system and a full re-install is suggested.

This Trojan has been specifically crafted to target people attempting to evade government censorship. Given the intended purpose of this software, users must be very careful if they have been infected by this Trojan. Additionally, they should be cautious about installing software, especially circumvention software, from untrusted sources. Where possible, software should be downloaded from trusted official websites over HTTPS. If checksums or cryptographic signatures are provided by the software vendor, these should be checked prior to installation.

## UPDATED: MAY 30, 2012

Since our report was published, the Simurgh team has taken several important steps to warn their users about this threat.

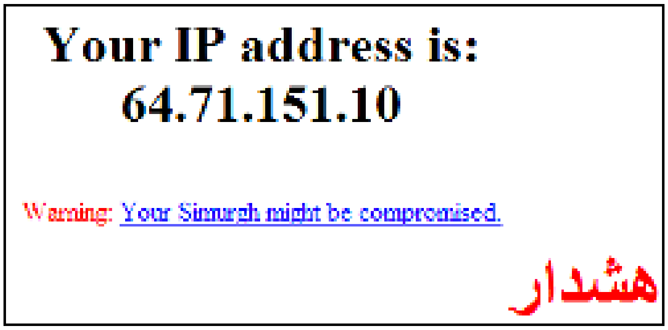
1) The Simurgh team warns their users directly on the website https://simurghesabz.net/with a prominent message in Arabic, Farsi and English about the malicious versions of the software. They post MD5 checksums of the official binaries and malicious packages, as well as instructions for how to check MD5 checksums against downloaded software. If you use Simurgh you should immediately compare your installer against the checksums posted on the official site.

You can also find these checksums below:

Official binaries
- simurgh120.20100910.exe – 07855ead46bb15718ee73d513bdb9678
- simurgh120beta.20100326.exe – ddecf8ac6c96c148cc7c42183d25baa9

Malicious installer packages
- Simurgh-setup.zip – 5e2a714fdfc2309af843056e8c5ae7d3
- Simurgh-setup.exe – 379480c807812f3521466f7ff5ffa273
- Simurgh-setup.exe – 300b0d061dfb9c9c6d7bdeecc74169f1
- simurgh[homs-sin.ibda3.org].exe – c8c8817af66312cfcfcb1ddf952f9d98

2) As Sophos has pointed out in a recent blog post on Naked Security http://nakedsecurity.sophos.com/2012/05/29/spying-trojan-targets-iranian-web-surfers-dissidents/, the splash page that loads when Simurgh is initialized to show the users' IP has been configured to warn users who may be compromised. If you see a warning you should immediately run an antivirus program to remove the software or for greater assurance, reinstall your operating system.



**Your IP address is:**
**64.71.151.10**

Warning: Your Simurgh might be compromised.

هشدار

In addition to the steps Simurgh has taken, we have made outreach to and notified the provider that was hosting the malicious version of Simurgh and they have now taken down the malicious package.

## ABOUT MORGAN MARQUIS-BOIRE

Morgan Marquis-Boire is a Technical Advisor at the Citizen Lab, Munk School of Global Affairs, University of Toronto. He works as a Security Engineer at Google specializing in Incident Response, Forensics and Malware Analysis.