Quick Heal
Security Simplified

‘Golroted’ malware uses web browser weakness to steal sensitive information

Introduction

At the Quick Heal Threat Research & Response Labs, we have been closely monitoring the ‘Golroted’ malware family since the last few months. This malware enables attackers to run multiple spam campaigns that make use of spear phishing emails. These malicious emails contain attachments of exploited Microsoft Office files or zip files of possib le keyloggers. In the case of Microsoft Office files, these infected files further download or contain encrypted versions of keyloggers themselves.

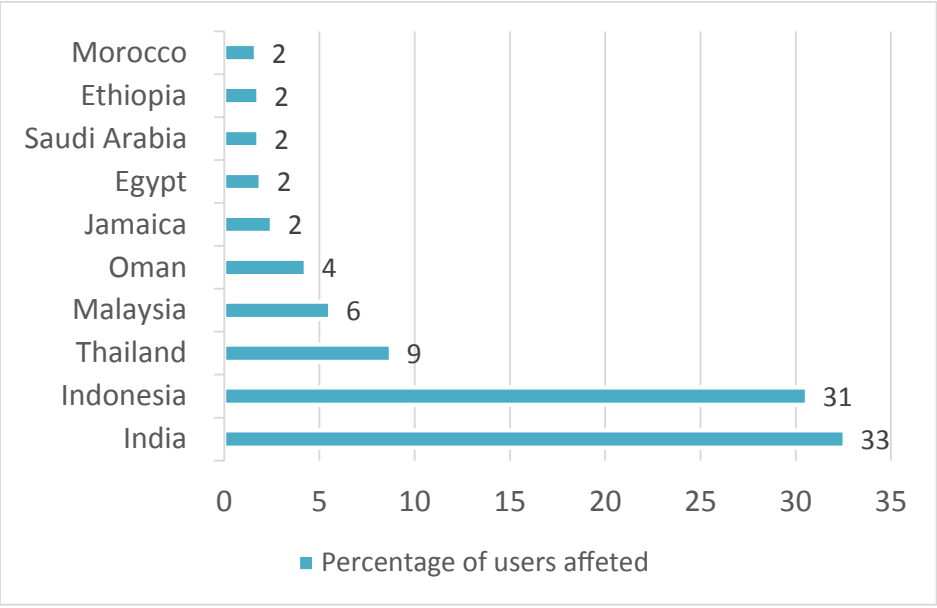
The Attack Mechanism of Golroted

The attack mechanism of the Golroted malware works as follows:

Once a user opens the malicious attachment, Golroted collects sensitive information from the compromised machine and sends this data to a preconfigured server. This is done by either uploading this data directly to a FTP server or by resending the data as email attachments. The Command and Control server (C&C) is located in the United States.

Countries Affected by Golroted

It has been found that India ranks first in the list of most affected countries with 33% of victims. Next in the list is Indonesia with 31% and Thailand with 9% of cases reported there.



What Golroted Can Actually Do

The primary purpose of this malware is to steal as much information as possible from an infected machine. The following information is known to be gathered by Golroted:

- Computer Name
- Local Date and Time
- Installed Language
- Operating System
- Internal IP Address
- External IP Address
- Installed Firewall
- Installed Antivirus Software

In addition to gathering and stealing this information, Golroted also has the ability to carry out the following activities:

- Capture screenshots
- Record keyboard strokes
- Log titles of all open windows
- Gather all clipboard data
- Send data to email addresses, FTP servers or web panels

Copy itself to removable and external drives
Block access to specific websites

Technical Analysis of Golroted in Action

The files that are dropped by Golroted have the following names and descriptions:

Dropped File	Description
%\AppData%\<random name>.exe	Copy of malicious file which is executed upon Startup
%Temp%\holdermail.txt	File used to store "Browser Password Recovery Report"
%\AppData%\pid.txt	Contains the process ID of executed samples
%\AppData%\pidloc.txt	Contains the information of compromised computers

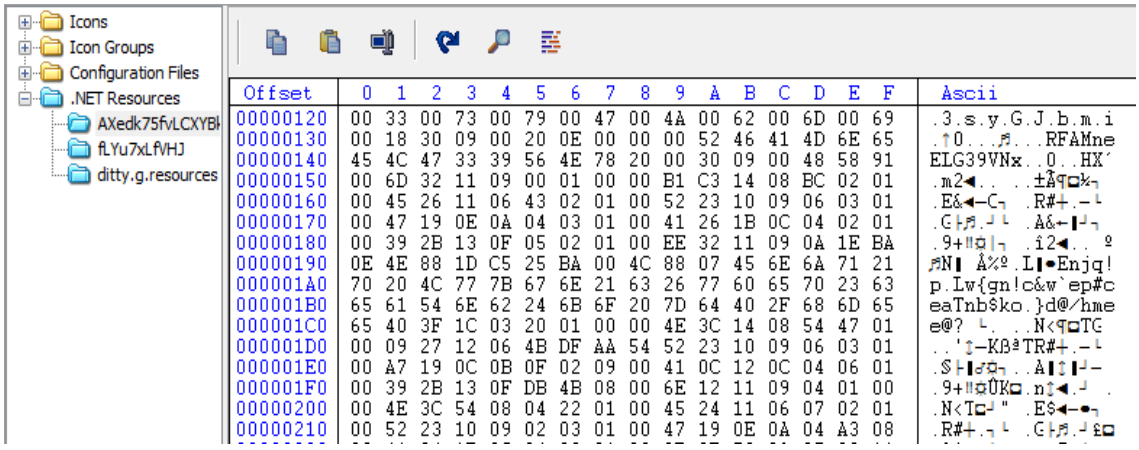
Once these files are within the system, Golroted sets the following registry entry in order to maintain its persistence:

Registry Entry	Value
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell	/%Application Data%\<random folder name>\<random name>.exe

The malware also has the capabilities of a USB worm through which it can replicate itself into removable or external drives that are connected with the system. The dropped files and their descriptions are as follows:

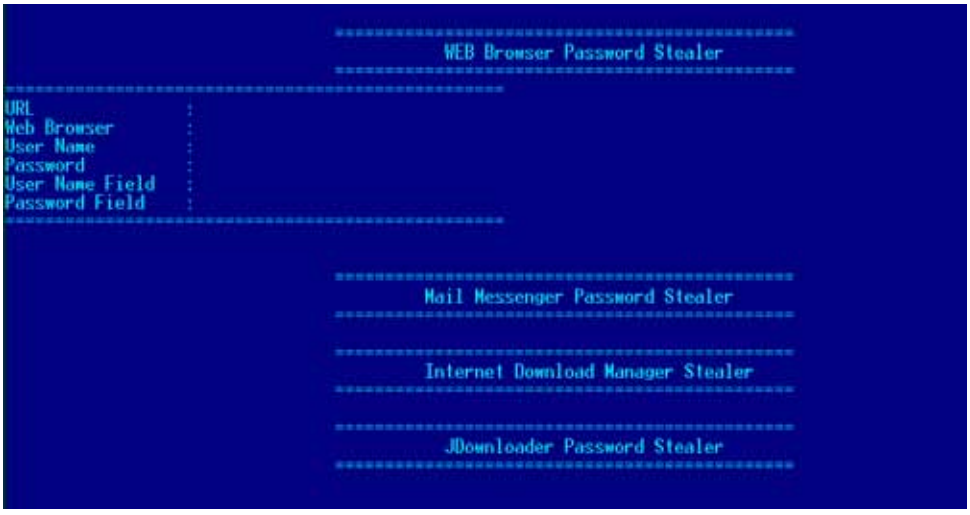
%DriveLetter%\Sys.exe	Drops copy of itself in removable drive with this filename
%DriveLetter%\autorun.inf	Drops this file into removable drive to autorun the malware when it is connected to victims machine

The Golroted malware makes use of Microsoft Visual C# / Basic .NET wrappers with obfuscation to avoid detection by security vendors and antivirus products. This makes the process of reverse engineering difficult for security programs and vendors. The actual keylogger is stored in an encrypted format as a part of resources in a .NET file as shown in the below image.



The decrypted file contains strings which clearly indicate that the keylogger and clipboard logger functionality are compromised along with the information stealing.

The Golroted malware sends the stolen user information and passwords along with details about the installed language, operating system, internal and external IP addresses, installed antivirus and firewall in the formats shown below. It also keeps track of sites visited and documents opened. In some cases, screenshots of these documents are also taken and uploaded to the C&C server.



Spam Campaigns

After studying the campaigns, it has been found that the attackers make use of email and browser password dump tools from 'Security Exploded' and they occasionally use a cracked version of 'Hawkeye keylogger' as well. The observed spam campaigns run under multiple banners as shown below:

- i
- c1
- m1
- vc1
- collins
- kcee
- kel
- nice
- tunde
- victor

The names ‘kcee’ and ‘tunde’ refer to some of the common names in Nigeria.

The Quick Heal Labs have cracked the communication mechanism of the Golroted C&C server. After listening in on the communication with this server and analyzing the data collected, we have found that 1,566 victims have been affected by this information stealing malware since October 2014.

The C&C server also collected the login IDs and passwords of various banks, social networking sites and email accounts. The statistics of collected passwords are as below:

Password Category	Total Users	Indian Users
Email accounts	656	310
Government related sites	95	30
Banking & financial sites	37	13
Social networking sites	312	95
Online booking sites	53	23
Miscellaneous	1217	

The malware has also collected passwords and screenshots of user accounts from the computers of victims. These included screenshots of the following sites:

Banking sites	Online payment sites	Email accounts	Social networks	Social networks
Vietcombank	Paytm	Gmail	Facebook	LinkedIn
Standard Chartered	PayPal	Yahoo	Amazon	Instagram
State Bank of India		Rediff	Shaadi.com	Tumblr
IDBI Bank		Windows Live Mail	Twitter	Shopclues
Techcombank			Matrimony.com	Jabong
HDFC Bank			Skype	Zing
Union Bank			Dropbox	Zoom

Since most users make use of the ‘auto password save feature’ provided by web browsers, the chances of being affected by the Golroted malware are quite high. Credentials from several web services and social accounts can be stolen in a matter of seconds. So users should avoid

using this feature and should instead choose to manually enter their password every single time.

Conclusion

Cyber crooks are using off-the-shelf keylogger tools wrapped inside cryptors for this information stealing mechanism. We strongly recommend that all users avoid using the 'Remember Password' feature of web browsers to ensure that their private data remains confidential.