COSEINC
Solid Security.Verified.

TROJAN.DROPPER.BISONAL

Udi Shamir

Coseinc (AML) Advanced Malware Labs

Overview

Bisonal is a malware whose primary purpose is to attack Japanese sites. It functions as a RAT (remote administrative tool) and communicates with its command-and-control (C&C) server without the user noticing it. When required, it can upload information to the server and download new payload from the server for execution. Data within the binary is fully obfuscated to prevent analysts from easily obtaining them.

Bisonal was first discovered in early 2013. Since then, we have analyzed a few of its variants, including binary droppers and office document files (xls and docx).

This report aims to unravel the details of Bisonal trojan's operation and technical components. The information presented were extracted and analysed using COSEINC Automated Malware Analysis Lab (CAMAL) sandbox platform.

Background

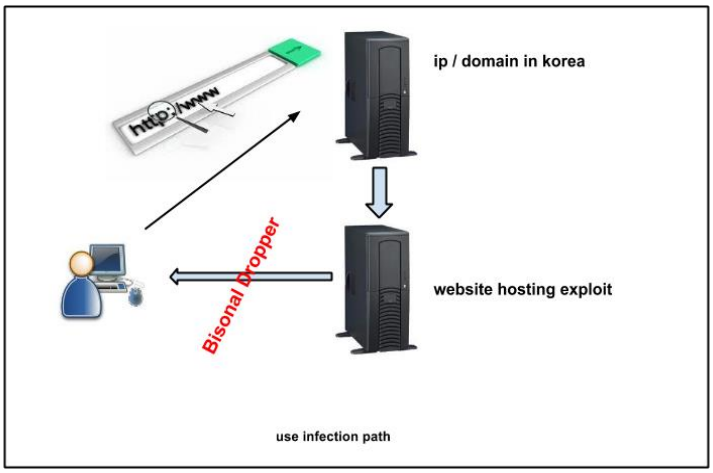
Downloader trojans are usually the first stage of the malware infection. Their sole purpose is to download files from the attacker's server and execute them on the victim's machine. Modern downloaders usually run without user awareness and are hard to detect as their mode of operation is similar to legitimate software.

Downloader trojans are frequently distributed via an application exploit. Once triggered, the downloader will obtain and execute additional malware from the internet.

Infection Vector

Bisonal main vector of infection is through social engineered emails. These emails redirect users to infected websites that deliver the exploit. Thereafter, it will initiate the "download & execute" sequence from the command-and-control server.

The Dropper will be the first to be downloaded and executed. This stage will bypass most security software as the domain and downloading process look legitimate. This legitimacy contributed to its low rate detection by most of the Antivirus engines. Bisonal was first spotted in late January 2013 and by May 2013 it was detect by only 7 antivirus engines out of 49 in VirusTotal.



Infection Details

We have seen several versions of Bisonal droppers in the past few months and the most prolific version has the file md5 of 68369ba443dc1f8d84b991da7fab4ec397b93ea7 . This section will discuss Bisonal's dropper functionality based on this version.

Technical Summary

Bisonal Dropper functionality can be split into two components: the main module and downloader module.

The *main module* is responsible for providing the framework to execute the various components within the malware.

The *communication module* is responsible for the sending of information to the server, receiving of new commands from the server and downloading of new executable. If a new executable is downloaded successfully, it will notifying the *main module* to execute it.

Main Module

One key function of Bisonal is to obtain the Operating System's information and it performs this by leveraging on cmd.exe. The malware first creates a single console version of cmd.exe. To hide cmd.exe presence, Bisonal modifies the STARTUPINFO structure which specifies the main window properties. Below are the values used in the STARTUPINFO,

Bisonal Hide cmd.exe

```
/* source code */
memset(&StartupInfo, 0, sizeof(StartupInfo));
StartupInfo.cb = sizeof(STARTUPINFO);
StartupInfo.dwFlags = STARTF_USESHOWWINDOW;
StartupInfo.wShowWindow = SW_HIDE;

CreateProcess( NULL, Args, NULL, NULL, FALSE,
          CREATE_NEW_CONSOLE,
          NULL,
          NULL,
          &StartupInfo,
          &ProcessInfo)
```

Upon successful creation of cmd.exe, it will also create namepipes to input commands to cmd.exe and to extract output from it. This is crucial, as the information gathered from the victim computer will determined the type of malware binary to download at a later stage. Examples of information gathered are,

- identifiers of the operating system (OS)
- running environment of the malware, such as running on virtual or physical machine
- the ip address of the machine
- hostname of machine
- proxy settings configured inside the client browser

Communication Module

Bisonal communication module is in charge of sending information, receiving commands or downloading new payloads from the command and control server.

To prepare for communication, Bisonal first decrypts the command and control server's encoded address. The encrypted key is embedded inside the dropper executable as follows,

EMBEDDED ENCRYPTION KEY

```
.text:00401E3C cipher?? : "wkko%00yjq{1|r|1pm1tm0Josp~{Yvsz0y~rz0g"
```

Subsequently, it will XOR each of its key characters with itself. This is a very common obfuscation technique found in other droppers.

After decryption, the embedded domain was found to be **fund.cmc.or.kr.** From our ASN record, fund.cmc.or.kr is a blacklisted domain.

DOMAIN ANALYZER

```
fund.cmc.or.kr not detected in white list.
ASN=AS3786 (LG DACOM Corporation)
*** ASN AS3786 in black list! ***
```

During the first communication, the malware will also send a long identifier string to the command and control server in the form of

flag:%s host:%s IP:%s OS:%sSP%d vm:%s proxy:%s' mid%s,0

Definitions of these fields are as follows,

Field	Description
flag	Value indicating if all modules in the malware is properly loaded
host	Hostname of the machine
IP	IP address of the machine
OS	Major OS version of the machine
SP	Minor OS version of the machine
vm	Value indicating if malware is running inside virtual or physical machine
proxy	Proxt setting of the browser
mid	4 bytes of randomly generated number

For subsequent communications with the command and control server, it uses another set of values. Below is a summary of these values.

BISONAL COMMUNICATION

// **Sending Malware Status** //
.data:00404244 aUpOk db 'Up OK!',0
.data:0040423C aUpFail db 'Up Fail',0
.data:0040422C aRunOk db 'Run OK!',0

// **Received Commands C&C** //
.data:00404220 aRun4d db 'Run -%4d',0
.data:00404234 Operation db 'open',0

The command and control server will provide the malware with the following information after each request:

C&C Server Header

```
reverse flow: 172.16.1.100.1036-115.91.31.146.80
HTTP/1.1 200
date : Fri, 14 Jun 2013 08:48:37 GMT
content-length : 1241
x-powered-by : ASP.NET
content-type : text/html
server : Microsoft-IIS/7.0
Connection:  Keep-Alive
```

From this information, we deduced that the command and control server is being hosted in a Windows IIS web server.

Conclusion

Trojan Droppers are mainly used to install additional malicious code on the victim machines and Bisonal is one of the newest droppers in the wild. It was primarily installed using exploits delivered as infected PDF and Office files.

Bisonal was written in C++ and the author used some codes that were freely available in one of the Chinese underground sites. Because of these, we were able to associate various new droppers as new variants of Bisonal. Aided by its interesting way of calling Operating System's command, Bisonal was not detected for 3 months by most antivirus engines.