WHITE PAPER: SYMANTEC SECURITY RESPONSE

# IM_a nuisance – W32.Imav.A

John Canavan
Symantec Security Response

# IM_a nuisance – W32.Imav.A

## Contents

## Abstract
The unique features and design methods associated with variants of the Beagle family of worms of the have ensured that these threats continue to be the most pervasive of Internet worms.

A new Beagle variant discovered in early 2006, W32.Imav.A, attempted to exploit a propagation vector not previously employed by these worms – instant messaging. However, the effectiveness of this technique was limited by the fact that a specific version of the ICQ program was targeted. Other novel features of this variant included its ability to communicate directly with login.icq.com and its use of a packet filtering API to block access to security-related Web sites. These developments underline the need to monitor the emergence of new Beagle variants very closely.

## Introduction – Happy Birthday Beagle
Two years on from its emergence and the Beagle family still remains one of the most pervasive Internet worms.

Leading the way in the new modular malware model, the Beagle family of threats has thrived by breaking its functionality down into separate basic components. Its associated downloaders, email address harvesters, and many other Trojan parts have thrived growing their network ever further and making their venture a profitable one.

The first variants of the Beagle family were seen in January 2004 [1], and from the outset these worms used some interesting techniques not typically seen in mass-mailers.

The initial mass-mailing samples opened a back door on the infected machines listening on TCP port 6777. This allowed a file to be downloaded and executed on the system when a trigger string is sent to the back door. It also ran a notification thread which contacts a remote Web site, announcing the presence of a newly compromised computer. This notification would prove to be a key technique the authors used to keep track of their infected network and seed new variants and components.

Later variants of the worm would terminate security-related processes, deleting their associated registry subkeys and files, and stop and remove system services. They overwrote host files to prevent access to security-related Web sites and even uninstalled previous variants of itself. And they did most of this while injected in explorer.exe.

For a period, the Beagle authors engaged in viral warfare against the authors of the Netsky family. Beagle variants would automatically terminate Netsky related processes and delete their registry subkeys, then create their mutexes to prevent re-infection.

Most of these features – and the design methods employed – focused on keeping control of the infected

machine, allowing easy installation of updates, hiding the presence of the infection of the system, and making disinfection more difficult.

Given this background, it is hard to imagine the motivation behind what appeared to be a major change in focus in on of the latest variants of the family to surface – the switch to ICQ as its major infection vector.

## W32.Imav.A

First sighted on January 26 2006 at known Beagle Trojan download URLs, W32.Imav.A [2] appeared to be just another Beagle Trojan.

Downloaded with the filename my_foto.zip, this threat displayed a candid photograph of a flame-haired, freckled skinned woman in a green bikini hanging out by a light-house as its first course of action.

It then set about copying itself to %System% and dropping its associated .dll file alongside it.

| *File Name* | *Size (bytes)* | *MD5* |
|---|---|---|
| im_1.exe | 33,745 | 960dddec022cc846a0a0075b98906c7b |
| im_2.exe | 17,886 | e2562b406a7cdf53ed50adfcf2f9fcd9 |

**Table 1: Properties of two of the files dropped by W32.Imav.A**

When executing from %System%, W32.Imav.A adds the entry `"im_autorn" = "%System%\im_1.exe"` to the registry `Run` subkey. It then starts up the usual Beagle Trojan routines, proceeding to kill a list of security-related processes, polling another list of URLs for a file to download, disabling a list of security-related services, renaming or deleting a long list of file names from security-related products and some associated registry entries. All pretty standard fare.

On a little further inspection, however, it became evident that W32.Imav.A had more to offer.

## ICQ

Ever since Eric Chien and Neal Hindocha presented their paper, "Malicious Threats and Vulnerabilities in Instant Messaging" [3], on the dangers of malware for instant messaging at VB 2003, anti-virus analysts have awaited the emergence of a rapidly spreading IM worm. Up until now we've seen attempts from Kelvir, Bropia, Funner, Bisex, various IRC bots, and many other threats to propagate via instant messaging, but none have succeeded to a level comparable with the classic mass-mailing email worm. So, perhaps when one of the most successful of the classic email worms turns to IM, we should be worried.

Throughout its history Beagle has adopted new techniques designed to increase its effectiveness, and

ability to spread. It makes sense that the authors would attempt to make use of whatever infection vectors are available to it, and therefore it's inclusion of an IM module is not a surprise. What is strange is the particular means of IM propagation they chose. By restricting themselves to ICQ they immediately lose a huge section of potential users, but they cut their potential infection user-pool yet further by making use of a password stealing technique which is unique to ICQ Lite/2003 versions of the software. Not only that, but if the Public Mode of these versions of ICQ is chosen on install the password will not be stored in the registry and thus the worm rendered impotent.

These choices appear even more curious when we look at PWSteal.LdPinch [4]. Variants of this Beagle related Trojan were downloaded by versions of the Mitgleider Trojan in early 2004. It logged keystrokes and sent system information on to a remote address, but interestingly also had the ability to steal ICQ passwords. PWSteal.LdPinch had the ability to steal passwords from client versions ICQ99b-2003a/Lite/ICQ2003Pro, reading and decrypting each ICQ profile's MainLocation value from the registry, but could also retrieve passwords stored in .dat files used by older versions of ICQ. It even stole passwords from alternative ICQ clients – Trillian, Miranda and &RQ.

W32.Imav.A iterates through ICQ profiles stored in the registry at `HKEY_CURRENT_USER\Software\Mirabilis\ICQ\NewOwners\<UIN>\` and `HKEY_LOCAL_MACHINE\Software\Mirabilis\ICQ\NewOwners\<UIN>\`. A number of versions of ICQ store the user's password here in the value `MainLocation`. This value is encoded based on the volume serial number of the system; however decryption techniques are well-known and have been used by several other malware authors (Bizex, Ldpinch) to date.

## Hungry? Have a SNAC

What is particularly noteworthy is that W32.Imav.A communicates directly with login.icq.com, logging itself in as a client. It builds its own FLAP packets of SNAC data.

To log in to the server W32.Imav.A needs to re-encrypt the password it has just decrypted from the registry. This time it's done with a simple byte-for-byte XOR with the following array:

*Example 1: Array used by W32.Imav.A to re-encrypt passwords*

```
0xF3, 0x26, 0x81, 0xC4, 0x39, 0x86, 0xDB, 0x92, 0x71, 0xA3, 0xB9, 0xE6,
0x53, 0x7A, 0x95, 0x7C
```

The FLAC login packet is constructed as below, with the Type-Length-Values specified.

| *Data Type* | *Description (Value)* |
|---|---|
| 4 BYTE | (0x00 0x00 0x00 0x01) |
| TLV(1) STRING | UIN/ICQ Number |
| TLV(2) STRING | Encrypted password |
| TLV(3) STRING | Client Version (ICQBasic) |
| TLV(16) WORD | unk (0x010A) |
| TLV(17) WORD | major version (0x0014) |
| TLV(18) WORD | minor version (0x0020) |
| TLV(19) WORD | lesser version (0x0000) |
| TLV(1A) WORD | build version (0x090B) |
| TLV(14) DWORD | version, (0x0000043D) |
| TLV(0F) STRING | language, 2 chars (en) |
| TLV(0E) STRING | country, 2 chars, (us) |

**Table 2: Type-Length-Values of the FLAC login packet**

Once authenticated, W32.Imav.A connects to the BOS server, using host/port information and auth-cookie from the login.icq.com's initial reply, and completes the protocol negotiation stage.

When the login process is complete W32.Imav.A attempts to send messages to random users containing the string "my foto" and a link to my_foto.zip located on a remote server.

## IP Filtering

Another interesting routine used by W32.Imav.A is it's blocking of security-related Web sites. Older variants of Beagle made use of a technique commonly seen in the malware world to block access to security-related sites. They added a long list of hosts they wanted excluded to the windows hosts file, %System%\drivers\etc\hosts. Although effective against the average home user, this was easily spotted and rectified by simply checking the contents of that file.

In Windows 2000, Microsoft introduced an API to implement packet filtering functionality. The API allows for similar functionality to that included in the TCP/IP properties of a network adapter.

To further impede the user in removing it from their machine Beagle now makes use of this Packet Filtering API to drop packets destined for a pre-defined list of Web sites.

`GetAdaptersInfo()` returns a linked list of completed `IP_ADAPTER_INFO` structs, from which the worm can get the current IP address assigned to all active interfaces `(PIP_ADDR_STRING CurrentIpAddress;)`.

`PfCreateInterface()` creates a new filter interface. This new interface will be used to control the adding and deleting of filters from the adapters found from `GetAdaptersInfo()`. The filter is created with the default `PF_ACTION_FORWARD` attributes for its `inAction` and `outAction`.

The new filter interface is then associated with each of the active network adapters using `PfBindInterfaceToIpaddress()`. At this point the packet filter is active and in place, but not set to actually filter anything.

W32.Imav.A performs a DNS lookup on each site to be blocked and creates an associated `PF_FILTER_DESCRIPTOR` struct for each result. This struct defines the packet filter containing details of the source and destination to filter on.

`PfAddFiltersToInterface()` then adds the filter to the previously created filter interface. The filter reverses the default processing rule for the interface, that is, the rule that was specified during the call to `PfCreateInterface()`. So, in this case traffic to hosts matched by a filter rule will be dropped. W32.Imav.A sets both input and output filters for the `PF_FILTER_DESCRIPTORS` generated.

## Conclusion

Although the actual impact of the Beagle variant W32.Imav.A in the wild was minimal, its use of new techniques reminds us that the Beagle authors will continue to be a threat as they pursue new means of propagation. As they embrace this experimentation, we must keep close watch on developments.

## References

[1] For example, see W32.Beagle.A,
http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.a@mm.html.
[2] For detailed information on W32.Imav.A, see
http://securityresponse.symantec.com/avcenter/venc/data/w32.imav.a.html
[3] For a copy of this paper from Symantec Security Response, see
http://securityresponse.symantec.com/avcenter/reference/malicious.threats.instant.messaging.pdf
[4] For detailed information on PWSteal.Ldpinch, see
http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.ldpinch.html

## About the Author

John Canavan is a software engineer with the Symantec Security Response team, based in Dublin, Ireland. John graduated from Dublin City University (DCU) in 2002, recieving a B.Sc. in Computer Applications (with honors). Shortly afterwards, John was apponited to his current position with Symantec where he had previously worked as a Network Security and SQA Engineer. John has published several articles in industry magazines and recently presented a paper at the VB2005 conference.

## About Symantec

Symantec is the global leader in information security, providing a broad range of software, appliances, and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, California, Symantec has operations in 35 countries. More information is available at www.symantec.com.

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
408 517 8000
800 721 3934
www.symantec.com


04/05 10406630