Yui Kee Computing Ltd.

# Newsletter

November 2002

## Contents

Contents ..... 1
Incident Update ..... 1
AVAR Conference Report ..... 1
Humour ..... 3
DDoS Attack Targets .info and .org ..... 3
Kaspersky Labs reports an attempt to hack its Web server ..... 3

## Incident Update

W32/Klez.H-mm again tops the virus lists. A new worm, W32/Winevar appears to have been released in response to the AVAR Conference in Korea. We first received copies of the worm on 23 November, the day after the conference ended, some developers reported first receiving samples from Korea, and the worm sometimes generates infected emails containing the test, " AVAR(Association of Anti-Virus Asia Reseachers) - Report. Invariably, Anti-Virus Program is very foolish." However, Winevar has not spread a great deal.

## AVAR Conference Report

Allan Dyer

The 5th Association of Anti-Virus Asia Researchers Conference was held in Seoul on 21 and 22 November. As usual, a mixture of anti-virus developers and researchers, representatives from government bodies and computing professionals attended. The papers were very informative, but I will focus on just a few points:

### Users Choice

Shigeru Ishii of the Japanese Information-technology Promotion Agency reported on the situation in Japan. He presented statistics from incident reports to the Agency and the results of a annual survey of over 1500 companies. Over the years, there was a switch from most viruses being detected after they had infected the victim, to most viruses being detected on arrival, before infection. This is a healthy trend, and shows that users can get it right. We all know that email is currently the most common source for viruses, but the survey showed just how overwhelming that is, with 96.1% of all viruses arriving by that route.

A surprise for the anti-virus researchers was the results of the question about the criteria for selecting anti-virus software. The top three criteria were: Function, Price, and Reliability of Manufacturer. Ability to detect viruses was suggested in the questionnaire, but was not in the top ten list.

### Smallpot

A honeypot is a computer attached to the net for the purpose of attracting attacks, just as an open pot of honey will attract wasps. Costin Raiu presented data from a network of honeypots designed to monitor the distribution and spread of net-borne malware, called the "Smallpot"

project. The result was an interesting survey of the varieties of malware actually spreading, and various curious incidents.

Analysis of the IP addresses allowed mapping of the sources of attack (and, therefore, existing victims of the malware). The USA came top of the list, with China second, and Hong Kong 7th, with many Asian countries near the top. For worms that preferentially attack "similar" IP addresses (which often translates to a similar location), the geographic distribution of the Smallpot machines skews the results towards the USA, Philippines, Romania and Russia. Correcting for this, Asia in general, and China in particular, have very high infection rates for many of these worms. Japan seems to be an exception to this, ranking quite lowly, especially since it has a very high Internet penetration. As there patches and other fixes available for the malware, there appears to be a great need for better systems administration in these countries.

## Fight Back

Jimmy Kuo echoed this in the day two Keynote Speech, saying that machines in Asia are among the worst protected in the world. He also suggested that legislation was required, either to allow the authorities to turn off an identified infected machine within their jurisdiction, or to allow the victims of an attack the legal right to fire back.

The thought here is that a lot of this malware opens a backdoor on the victim's machine to allow the attacker to control their network of "zombies". The control interface usually includes some sort of "shutdown" command, so it is possible for anyone to attempt to send that command, and thus stop the attack. It would be relatively safe - not damaging to data on the machine, just shutting down the malware, which the authorised user of the machine was probably unaware of and did not want. Under current laws in most jurisdictions, including Hong Kong, it would also be illegal: Unauthorised access by telecommunications.

I think that it might be possible to make useful legislation along these lines. However, allowing victims to "fire back" would be dangerous. Victims with insufficient knowledge might use inappropriate methods, there would probably soon be many cheap or free programs advertised as counterattack software that novices could use - each claiming to be "more powerful" than the last. If those programs went beyond what was allowed by law, the novice users might find themselves arrested.

Giving the power to a suitable authority seems a better course. The authority could determine which malware can be safely dealt with in this way, and build appropriate tools to identify whether the target machine is infected and, if it is, to send the appropriate command. These could then be automatically deployed in response to the report of an attack.

## Malware Names

Nick Fitzgerald presented the draft revisions to the Computer Anti-virus Research Organisation (CARO) Naming Convention. Ever since computer viruses appeared there has been chaos in naming them, with different anti-virus developers assigning different names to the same viruses. The only vendor-neutral naming standard was the CARO Virus Naming Convention, originally drafted in 1991.

The revisions update the convention to cope with the many changes in the last decade, and provide a basis for future developments. Although it is still under development, and there are many detailed recommendations (such as not using obscene or offensive names for the family name) that I will not list, the basic form of the new Fully Specified Malware Name (FSMN) is:

<malware_type>://<platform>/<family_name>.<group_name>.<infective_length>.<sub-varient><devolution><modifiers>

However, most malware will not require all components. It should be clear that just knowing the FSMN gives quite a lot of useful information about the malware.

Confusion caused by different and misleading names has wasted precious time in developing incidents and increased technical support workloads at corporate and developer helpdesks. I hope that all anti-virus developers adopt the new convention so that this is reduced in future.

## Humour

A new threat to the Internet: http://www.bbspot.com/News/2002/10/apologize.html

## DDoS Attack Targets .info and .org

About a month after attacks on the DNS root servers, UltraDNS, the company that manages the .info and .org top-level domains, has suffered a Distributed Denial of Service Attack. Ben Petro, CEO of UltraDNS, said, "This is the largest attack that we've seen", but stressed that it didn't affect the company's core domain name system (DNS) services.

The organisations that manage the top level domains are used to handling high loads and are well aware of the importance of their services. A successful attack would affect every organisation under those top level domains, and anyone trying to contact them.

Tracing the origin of the attacks, and punishing the perpetrator(s), is a problem because they use networks of "zombies" - machines that have been broken into, with remotely-controlled attach software installed. The initial trace leads to more victims.

Further Information:

http://zdnet.com.com/2100-1105-971178.html

## Kaspersky Labs reports an attempt to hack its Web server

On the night the November 7th there was a massive attack against Kaspersky Labs Web server resulting in a group of hackers sending subscribers of the Kaspersky Labs e-mail newsletter a message containing the recently discovered "Bridex" worm.

"During the last few years Kaspersky Labs has grown to become one of the leading virus experts and this status has attracted much attention from hackers resulting in daily attempts to penetrate of defences", said Eugene Kaspersky, Head of Anti-Virus Research. "Currently we are conducting an investigation to reveal the sources of this attack and are taking the necessary measures with our security system to ensure that this type of attack will never succeed in the future."

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2555 0209 Fax: 28736164
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/computer/


One Stop Anti-virus
&
Information
Security Partner
- Anti-Virus
- Firewall
- Communication Encryption
- File & Folder Encryption
- VPN
- Smartcard Token
- Content Security
- Security Check Services:
Vulnerability Scanning,
Penetration Test,
Risk Assessment ...etc.
YUI KEE