Yui Kee Computing Ltd.

Newsletter

July 2001

Contents

Latest Email Worm: W32/SirCam@MM

W32.SirCam.Worm@mm is a mass-mailing email worm. It arrives in an email with a random subject and an attachment with the same filename as the subject. The body of the message will always start and end with the same two sentences, either in English or Spanish. It is also capable of enumerating network resources and spreading over a LAN.

SirCam is destructive, it has several activation routines, in some circumstances it will attempt to use up all disk space, and there is a 1 in 20 chance that it will delete all files on drive C: on 16 October.

SirCam was first seen on 18 July 2001 and by 20 July it had moved into the top position on MessageLabs' "Viruses stopped today" list. According to Trend Micro's "Worldwide Virus Tracking Center" it was running a close second to W32/Magistr.A on the 20th, but had moved to the top place by the 23rd. For further information on SirCam, see:

http://www.itsd.gov.hk/itsd/virus/alert/alert/w32sircam.htm
http://www.sarc.com/avcenter/venc/data/w32.sircam.worm@mm.html
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SIRCAM.A
http://vil.nai.com/vil/virusChar.asp?virus_k=99141
http://www.f-secure.com/v-descs/sircam.shtml
http://www.sophos.com/virusinfo/analyses/w32sircama.html

All the anti-virus vendors issued virus definition updates before SirCam became very common, however, as late as 28 July we were receiving incident reports from users who had anti-virus software installed, but had not updated it. Contact us for assistance on automating updates, also consider using our YKScan service, where updates are checked for every 10 minutes - see attached report for a trial offer.

Microsoft IIS Servers Under Attack: CodeRed

Sites using Microsoft's web server should beware of the worm CodeRed, also called I-Worm.Bady. This worm exploits a flaw in the indexing service, sites that are not using this service should make sure it is disabled; sites that are using the service should use the Microsoft patch to fix the flaw:

http://www.microsoft.com/technet/security/bulletin/ms01-033.asp

When active, the worm continually attempts to connect to other web servers and infect them. It may also modify the web pages on the server with a message, "HELLO! Welcome to http://www.worm.com! Hacked By Chinese!"

Your intrusion detection system should be able to easily identify the worm's attacked. Further information on the worm is available at:

http://www.europe.f-secure.com/v-descs/bady.shtml
http://www.cert.org/advisories/CA-2001-13.html
http://www.ciac.org/ciac/bulletins/l-098.shtml
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp
http://www.sophos.com/support/news/ - codered

Special Offer

SOPHOS MAILsweeper

We are pleased to inform you that a promotion bundle program on Sophos Anti-Virus Interface (SAVI) and MAILsweeper is launched.

If you buy Sophos Anti-Virus Interface (SAVI) and MAILsweeper together, the cost is just 90% of the current list price.

Contact our Customer Services department at:

- Tel: 2870 8553
- Fax: 2873 6164
- e-mail: offer@yuikee.com.hk

F-Secure Hong Kong Office

F-Secure have announced changes in their organisational structure, F-Secure (Greater China) Ltd. Has closed their office in Hong Kong, Macau and People's Republic of China area to focus its activities through partners and distributors.

As a result our customers should contact us (28708556, techHelp@yuikee.com.hk) for support on F-Secure products.

Measuring and Reporting

The news constantly bombards us with stories of security disasters: destructive viruses, armies of hackers (an apology to people who know the difference between hackers and crackers, but the popular press has made its' definition), and worse. There was a recent Cyber-War between China and the USA (did you notice?). It would be easy to think that the Information Society is teetering on the brink of total failure from all these attacks.

However, in order to correctly plan our information security, we need something very different from sensationalised news reports. We have to quantify the various risks and threats in order to prioritise them for action. In many cases, the consequences of an incident are easy to evaluate - a new security vulnerability could expose *that* information, or a new virus could cause *that* damage.

The risks are a lot harder to quantify. How likely is it that your organisations' web page will be defaced? If another "Cyber-War" is reported, will that change? Should you immediately put your security staff on overtime in response? Which will cost more for your organisation, the latest big-name virus, or the one that has slowly but steadily been spreading and persistently causing small amounts of damage for months?

I suspect that the "Cyber-War" between USA and Chinese hackers was nothing more than a media event. Certainly, web pages were being defaced, but many had no political message. Even when the message was political, did the culprit do it because of the issue, or the theme was chosen simply because it was topical and likely to generate maximum publicity for the defacement? May was supposed to be the high point of the war, but a website specialising in statistics of website defacements (Attrition, http://www.attrition.org/mirror/attrition/annuals.html) shows the total in April was higher.

Similarly, W32.Leave.Worm gained recent publicity, but it is the older W32/Magistr@mm that I currently receive most often in email. W32/Magistr@mm also has destructive activation routines.

Obviously we cannot rely on the popular media for our risk assessments, we need hard data. There are many Internet sites that publish such information. I have already mentioned Attrition, for a more mainstream perspective, many CERT teams summarise their reports, including of course, the CERT Coordination Center (http://www.cert.org/nav/index_red.html). Information on virus spread is available from the WildList Organisation (http://www.wildlist.org/).

These sites depend on reports from organisations like yours. To quote from the CERT/CC site, "Because users are our primary source of information, we encourage you to report any incidents you experience on your systems or any vulnerabilities you find. These reports will help us inform you and others about potential threats and ways to avoid or recover from them."

However, many information security incidents go unreported. A striking example of this was the case of the virus W95/CIH (also known as Chernobyl), which activated on 26 April 1999, causing damage on hundreds of thousands of PCs, largely in Asia. After the activation, the author, Chen Ing-Hau, was quickly identified by a Taiwanese college and questioned by military authorities. However, he was then released because, incredibly, there had been no complaints to the Police in Taiwan. It is unbelievable that absolutely no computers in Taiwan were affected when nearby Korea had, according to the Korean Information Security Agency, 160,000 activations, and Mainland China suffered 250,000 activations according to some newspapers. Thankfully, the following year, a Taiwanese college student filed charges when his machine was struck on the next anniversary, 26 April 2000. Chen Ing-Hau was arrested and if found guilty he could face up to three years in jail under destruction charges.

Therefore, good reporting from organisations like yours has positive benefits to information security in general. It lets us understand the size and nature of the problem, making realistic risk assessments a possibility, and, in some cases, it allows action to be taken against the culprits. This also applies within an organisation - what are your reporting mechanisms for information security incidents, and are they adequate? If you cannot measure it, you cannot manage it.

If reporting is so important, why do so many incidents go unreported? Some possible reasons are:

- The incident is perceived as minor
- The victim does not know where to report to
- Making the report is too time consuming
- The victim is afraid of blame, ridicule or loss of reputation - this is particularly the case if the incident could be linked to non-work computer use during office hours.

The last is the reason that some organisations have a policy against making reports, however, organisations like the CERTs and WildList Organisation keep the victims' details confidential.

To be useful, the report must also be made to a relevant party - a police officer told me of a user reporting an email bomb to his local police station, and the desk sergeant called the bomb squad.

There are possible ways to collect these reports while avoiding the limitations. Two sites that give frequently updated statistics and do not depend on user reports are MessageLabs (http://www.messagelabs.com/) and Trend Micro's World Virus Tracking Center (http://wtc.trendmicro.com/wtc/), both vendor sites. Trend's site displays statistics of viruses found by their free on-line virus scanner, and by their central management virus solution. In some ways, MessageLabs' statistics have a wider base - they record viruses sent in email to or from their customers. This gives an indication of what is happening not just on their customers systems, but anyone who emails those customers. However, this does not give the full picture, there is an inherent bias towards viruses that have an email replication mechanism. Conversely, a worm that uses other methods to spread such as Sadmind (which propagates on Solaris systems) will not get counted.

Sadmind also defaces websites on vulnerable IIS servers, so your webserver on NT is more likely to be attacked because of a worm spreading on Solaris. Similarly, CodeRed (described in this issue) will not get counted. This illustrates the complexity of the factors that influence the risks in the real world, beyond the neat assumptions of the typical risk assessment.

Our current position is less than ideal: incidents go unreported; various data collection methods introduce their own biases, and the resulting information is not comparable between different summaries. The sites do agree on one thing: the trend is up. But the only way we will get better information is by making better reports more consistently.

Yui Kee Professional Services

Information Security is a dynamic discipline and your IT department needs timely, accurate information and support. Yui Kee Computing Ltd. (YKCP) provides reliable professional services and enables your company to concentrate on running your core business. The services are generally available with per-use or annual contract options, so you can closely match your requirements.

Anti-Virus Support

Computer viruses and worms are the commonest cause of security incidents, and speed of reaction is vital. Yui Kee has been the leading local anti-virus company for eight years and our qualified, experienced staff can support you on various terms:

YKBasic AV Support

One named caller in your company can enjoy:

- Local Telephone Helpdesk Support (Unlimited), Office Hours
- E-mail support (Unlimited)
- Optional subscription to newsletter, virus alert, weekly update and other available mailing lists
- 30% off On-Site Anti-Virus Support
- 30% off On-Site installation and deployment

Provided **Free** to all purchasers of Anti-Virus software of 10 users or more from YKCP.

YKPremium AV Support

- 4 hours On-Site AV planning with your security team / systems administrator
- Three named callers in your company can enjoy YKBasic AV Support
- 10 hours On-Site AV support

- Guaranteed 2 hour response and next day on-site
- Up to 50% of remaining unused hours can be rollover after expiry to the next contract provided the new contract is signed on a continuous basis.
- 30% off On-Site AV Training Courses

Additional units can be purchased to match your requirements:

- Named Callers
- AV Planning (by hour)
- AV Support (by hour)

YKOnSite AV Support

Call-out our Anti-Virus Experts as you require, call-out and hourly charges..

YKRemote AV Support

Professional Advice is just a phone-call or email away, charged per question.

YKTraining AV

Our Anti-Virus Experts deliver training direct to your staff. User and technical level courses are available.

YKHelpdesk AV

Our Helpdesk will field your virus-related user calls.

- 2 day pre-planning - tailors the helpdesk to your organisation's policies, AV software and network topology
- Second-level helpdesk - calls should be already qualified as virus-related
- Office-Hours or 24x7 service
- Weekly call summary
- Immediate alert to security team / system administrator with advice when a serious incident is identified
- Charged according to number of users, starting from 500 users.

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/