Yui Kee Computing Ltd.

Newsletter

April 2011

Contents

US Government Takes Command of Coreflood

<web-link for this article>

US Federal Prosecutors have obtained a court order to set up a substitute Command and Control system (C&C) and take over IP addresses and control of the Coreflood botnet, which has infected over 2 million Microsoft Windows computers over an 8 year period. The control will be used to stop the malware and record the IP addresses of infected systems so the victims can be warned.

However, the stop command is only temporary. Infected systems will still have the malware and will attempt to reload it when they are restarted. Therefore, the substitute C&C will need to operate for a long time, while the victims are traced via ISP records. The criminals behind Coreflood may also try to regain control of the botnet. The Internet System Consortium, helped by Microsoft, will operate the substitute C&C.

Analysis of Coreflood has hinted at a highly-organised software development team and a lot of investment behind it and some of the online banking credentials it was used to obtain netted the villains hundreds of thousands of US dollars. The botnet has clearly been a lucrative revenue stream, and the gang faces the decision of whether to fight to regain control, or walk away and set up a new botnet.

The takedown operation is claimed to be the first time the US government has got a court order to setup a substitute C&C. However, in October 2010, the Dutch police and Government, and security company Fox-IT cooperated to behead the Bredolab botnet and use the botnet itself to alert victims. In a hotly debated show in March 2009, the BBC program Click took over small botnet by hiring it, demonstrated it was functional, and warned the victims by changing their wallpaper.

Yui Kee's Chief Consultant Allan Dyer commented, "Operations that take control of botnets are often controversial because the 'good guys' are also using the victim's computer without authorisation. There are right and wrong ways of doing this, Click's approach was wrong, it funded the criminals and did not have the support of a court order. Skilled and accountable law enforcement, with public safety in mind and backed by the courts is the way to go. Notifying the victims via the botnet is a risk, there could be unintended consequences. PCs are not

designed for safety-critical tasks, and anyone running a critical system should be keeping malware out, but we know this is not always true - look at Stuxnet. Surely there is an ethical obligation to take the less invasive but more laborious approach first - tracing the IP address? Also, dismantling this botnet is a fleeting victory, I hope the investigators are tracing the developers, before they release their next botnet."

More Information

In a first, feds commandeer botnet, issue 'stop' command
Coreflood/AFcore Trojan Analysis
Feds Take 'Coreflood Botnet': 'Zombie' Army May Have Infected 2 Million Computers, Stolen Hundreds of Millions of Dollars
Backdoor.Coreflood
Troj/CoreFloo-C
Dutch police behead Bredolab botnet
BBC team exposes cyber crime risk
Click's botnet experiment
Click's botnet experiment
BBC Click paid cybercrooks to buy botnet

I am My Phone

<web-link for this article>

Allan Dyer

The British Computer Society website has recently published an ambitiously titled article by Andrew Kemshall, co-founder of SecurEnvoy. I would like to spend a few paragraphs criticising the article.

Mr. Kemshall's central argument is that security tokens are like cassette tape, an obsolete technology, and about to be replaced by authentication by mobile phone and SMS.

Unfortunately, he says, "Nothing lasts forever and two factor authentication isn't any different", and lists cassette tape, VHS, DVD and Blu-Ray as a technological progression. This is wrong, in principle and in detail. In detail, cassette tape actually outlasted VHS; because they filled different technological niches. Solid-state MP3 devices replaced audio tapes. More generally, each technology has particular characteristics that determine its suitability for various tasks, and an old technology may remain in use for particular tasks, even while it has been replaced for others.

However, the principle is that audio recording is still around, as it has been since Thomas Edison's experiments in 1878. Two factor authentication is a function that, like audio recording, can be achieved using different technologies and Mr. Kemshall is wrong to equate it to one particular technology for one factor: dedicated physical tokens.

Mr. Kemshall advocates SMS as a replacement for physical tokens. This can be described as a variant of authentication by tokens - the "something you have" is your mobile phone instead of the dedicated physical token. Perhaps his article should have been titled, "No more Dedicated Tokens"?

A former issue with SMS authentication was that the network might be temporarily suspended or the user may be in a signal dead spot, such as the basement of a building or computer room, preventing the reception of a code when needed. Mr. Kemshall tells us that pre-loaded codes solve this, "As soon as a user enters their authentication code, the system automatically forwards a new SMS message, overwriting the code in an existing message ready for the next session." This implies that a person who steals the phone will always have a valid access code for one session, no matter how fast the user reports the loss. Not much different to a dedicated

token, but the code could also be accessed by a "friend" who borrows the phone "for a minute". A phone may be a personal device, but they are shared and shown-off socially. "You've got Angry Birds on there? Can I see?"

Most of the other points raised in favour of SMS cite the cost and inconvenience of tokens - deploying 1000 tokens could take six months, for example. Why this timescale is required is not spelt out, but I suspect it has something to do with carefully ensuring that the correct person gets the token. Setting up an SMS solution can be done in a day, simply use the existing employee database with mobile numbers automatically identified. This assumes that the employee database is accurate and up-to-date, so it would be a good idea to add the time and cost of really verifying that before using it.

People loose tokens, and they loose phones, but, Mr. Kemshall reports, "a third of the population would notice they'd lost their mobile phone within 15 minutes and 60 per cent would within the hour", the fact a token is missing may not be noticed until the next time it is needed. Fast reporting of loss is good, but how many people, when they loose their phone, would remember to call up the helpdesk to get the SMS authentication disabled? Most would be more concerned with the address book, photo album and value of the device. Also, phones are easy to resell, so they are a more attractive target for theft.

An issue not addressed is the security of the phone network. The access code is being sent by store-and-forward, via a public, third party communications network. What analysis has been done on the vulnerabilities this introduces?

The assumption of "something you have" authentication is that possession proves identity. SMS authentication is a variant of "something you have" authentication, assuming that possession of a phone proves identity, with certain advantages: cheapness, ease of deployment; and disadvantages: weak binding of the phone to the user, unexplored risks in the public network. The rise of SMS authentication does not presage the end for two-factor authentication. It does not even hammer the final nail into the physical tokens' coffin. It does offer one more tool for your toolbox. Carefully evaluate the needs of the job when choosing your tools.

More Information

No more tokens

Chinese Domain Name Launch

<web-link for this article>

Since 22 February 2011, the Hong Kong Domain Name Registration Company Limited (HKDNR) has been accepting registrations of .香港 domain names. During the initial Pre-Launch Priority Registration period, up to 10 March, HKDNR accepted applications from existing .hk domain name holders. The successfully-registered domain names became active on 23 March 2011. Now that the pre-launch priority registration period is over, Chinese domain names can be registered on a first-come-first-served basis.

As an existing .hk domain name holder, Yui Kee took the opportunity to register Chinese equivalents of its domain names. We have since completed the provision of our websites under the new domains. Therefore, you can now visit our sites at:

- http://文章.銳基.公司.香港/
- http://網.銳基.公司.香港/

The content on these sites is exactly the same as the English equivalent domain names. The only difference is that, for the Chinese domain names, if the user's browser does not have a language preference configured, and there are English and Chinese versions of the page requested, the Chinese page will be served. The English domain names default to serving the

English page. Of course, we would recommend users to set their preferred language in their browser.

Technical Considerations

Internet engineers will know that the current domain name system only supports ASCII characters, but a clever trick has been used to implement additional characters without requiring every company and every user on the internet to upgrade their software on the same day. The Internationalized Domain Name system encodes these non-ASCII characters as ASCII characters using Punycode. When a section of a domain name contains a non-ASCII character, the Punycode form starts with the four characters xn--, so the website addresses above can also be written:

- http://xn--7dv288b.xn--3jst58k.xn--55qx5d.xn--j6w193g/
- http://xn--zf0a.xn--3jst58k.xn--55qx5d.xn--j6w193g/

Punycode covers non-Chinese characters too, such as ü and other accented European characters, Cyrillic, and the Japanese character sets. HKDNR provides a useful Punycode converter.

Punycode is useful because you do not need the correct fonts or up-to-date software to access internationalized domain names, the Punycode form can always be used. A recent browser, such as Firefox 3.6, will automatically convert the entered Punycode domain name to the native language characters. An older browser, such as Internet Explorer 6, will show the Punycode. The minor disadvantages of Punycode are that the code is not memorable, and if a native-language URL is printed, it is practically impossible for a foreigner to enter the URL.

Some useful hints when implementing internationalized domain names:

Your webserver can be configured to default to different languages for different virtual sites. For Apache, if your directory hierarchy follows the domain names, changing all your .香港 sites to default to Chinese could be as simple as adding this to your configuration file:

```
<Directory "/var/sites/xn--j6w193g">
LanguagePriority zh-tw zh-cn en fr de it ja
</Directory>
```

Your wordprocessor or editor's autocorrect may not be your friend, it can mangle your punycode names. For example, Word's dictionary will recommend "an" as the correct spelling of "xn". Word's "AutoFormat as you type" will replace "--" with "—", and the difference can be very hard to see in some fonts. There are at least two Word features to switch off: AutoCorrect: Replace text as you type; AutoFormat as you type: Symbol characters (--) with (—); and starting a spell check is obviously something to avoid.

Whether or not internationalised domain names will open up the internet to billions of users that are unfamiliar with the Latin character set or cause problems by Balkanising the internet is debatable, but we can definitely expect to see a lot more of them in future.

More Information

HKIRC Officially Launches Full Chinese .香港 Domain Name
Internationalized domain name
Why is Website Language Negotiation So Poorly Adopted?
Browser Language Preference Report
Chinese '.hk' Domain Name FAQ
Punycode
Punycode Conversion Tool

AVAR 2011 Call for Papers

<web-link for this article>

AVAR, Association of anti Virus Asia Researchers will hold its 14th AVAR Conference (AVAR 2011) on November 9-11 November 2011 at the Renaissance Harbour View Hotel in Hong Kong. Hosted by AVAR and organized by West Coast Labs, the conference promises to be an insightful and informative event.

The conference will comprise a dual track program of 40-minute presentations of both technical and corporate topics. Submissions are invited on all subjects relevant to anti-malware. In particular, AVAR welcomes the submission of papers that will provide delegates with ideas, advice and/or practical techniques.

Presentations are also encouraged that include practical demonstrations of techniques or new technologies such as threats on mobile devices, threats by social networks, threats from exploits and vulnerabilities, 0-day threats, etc.

Discussion of the current state of malware in Asia is also welcomed, as well as sharing of techniques or ideas to improve this situation for the future.

Submissions should be sent to avar2011@aavar.org. The closing date for submissions is 30th June 2011.

The conference website and detailed information about the event will be ready at the beginning of May.

More Cameras Might Lie

<web-link for this article>

Having shown that Canon's image verification scheme is flawed in 2010, ElcomSoft has now shown a similar vulnerability in Nikon's Image Authentication System. They were able to extract the original signing key from a Nikon camera, thus enabling the creation of amusing fakes to demonstrate the problem.

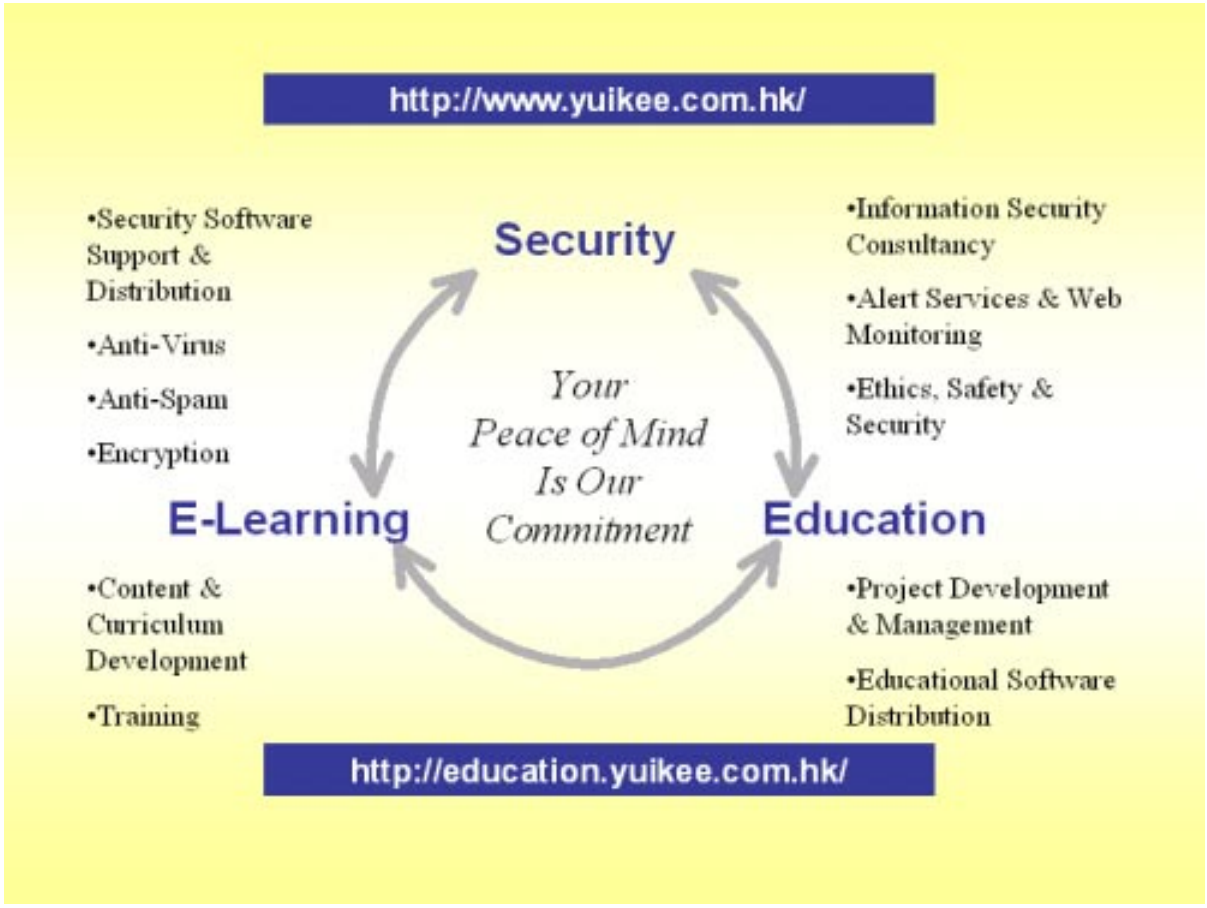
All past and current digital SLR cameras manufactured by Nikon and supporting Image Authentication are affected, including Nikon D3X, D3, D700, D300S, D300, D2Xs, D2X, D2Hs, and D200 digital SLRs.

More Information

Nikon Image Authentication System Vulnerability
Nikon Image Authentication System: Compromised
Nikon image authentication system cracked
The Camera Never Lies?

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: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/