Yui Kee Computing Ltd.

Newsletter

August 2014

Contents

Contents....1
SynoLocker Hits Chinese University's Faculty of Medicine....1
HKMA warns about fraudulent Bank of East Asia email....2

SynoLocker Hits Chinese University's Faculty of Medicine

<web-link for this article>

Ransomware targeting Synology NAS servers has encrypted personal data of 10,000 patients but patient care has not been affected.

The case is just one incident in the growing number of Synology Diskstations and Rackstations that have been attacked in recent days. The malware, called SynoLocker, gains access to the systems through vulnerabilities, then encrypts the data and displays a ransom message on the administrative interface (DiskStation Manager - DSM):

"All important files on this NAS have been encrypted using strong cryptography"

The message continues with instruction to pay 0.6 bitcoins (about US$350) via an anonymising network for the data to be unlocked.

At the Chinese University Faculty of Medicine, two servers in the Centre for Liver Health and Institute of Digestive Disease at the Prince of Wales Hospital in Sha Tin were affected. The servers contain day-to-day data, research and teaching materials. The servers were immediately disconnected, and the Police are investigating. A Police spokesman revealed that they had received multiple reports from victims of similar attacks since Monday, and IT news sites are reporting cases around the world.

It seems unlikely that the Chinese University was deliberately chosen, the criminals are indiscriminately attacking any Synology device they can find and the relatively low ransom was probably chosen as a level that many victims would see as a small price for their data.

If you are using a Synology NAS it is important to protect the administration interface **immediately**. Check and close ports 5000 and 5001 on your firewall.

If your Synology NAS displays the ransom message, power off the device immediately to avoid more files being encrypted and contact the Police and Synology support. Synology has additional advice on their Facebook page.

If you are using an NAS from another vendor, do not think that you are safe. There has been a trend towards making NAS boxes more capable and it is likely there are vulnerabilities to be exploited. Review your security policies and plan for defence in depth. A device holding sensitive information should not be exposed on the public internet. If remote access is

required, then a VPN should be used. Multiple backups in different locations allows recovery of vital data, if the backups have not also been maliciously encrypted.

More Information

Cyberattack hits 10,000 patients' health data
Synology on Facebook
Ransomware attack hits Synology's NAS boxen
Synology and the NAS-ty malware-flingers: What can be learned

HKMA warns about fraudulent Bank of East Asia email

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has warned about a fake email supposedly from The Bank of East Asia, Limited (BEA). The e-mail requests customers to follow a link and provide personal information. The target of one such link, "http://malaucene.fr/wp-includes/pomo/Servize-iTunes/app/registre/", had been removed at the time of writing. BEA did not send the emails, and the Police are investigating.

Victims who have provided personal information or conducted financial transactions through the website should contact BEA at 2211 1333 and any local police station or the Commercial Crime Bureau of the Hong Kong Police Force at 2860 5012.

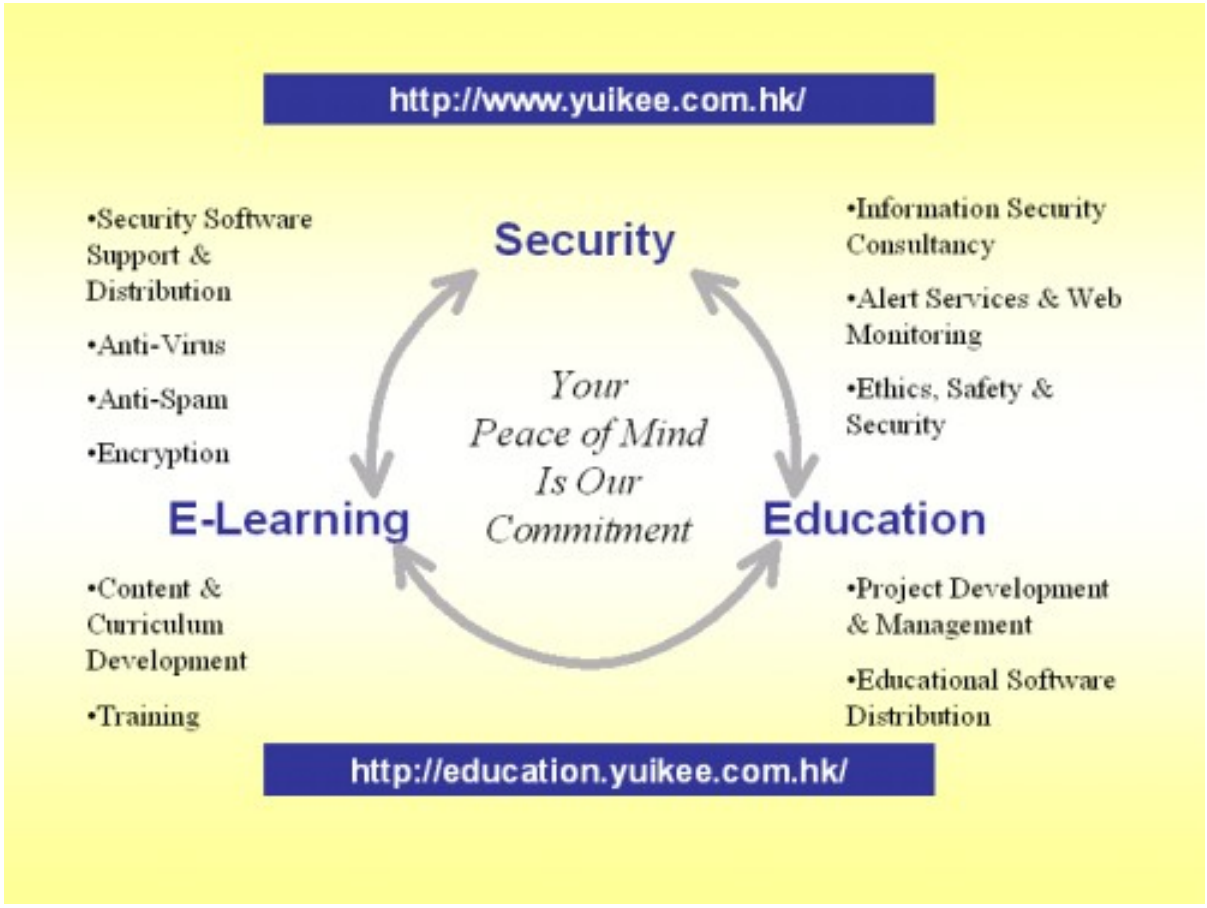
A HKMA spokesperson advised, "Members of the public are reminded not to access their Internet banking accounts through hyperlinks embedded in e-mails, Internet search engines or suspicious pop-up windows. Instead, they should access their Internet banking accounts by typing the website addresses at the address bar of the browser, or by bookmarking the genuine website and using that for access. In addition, banks are not expected to send e-mails asking their customers to provide their account information (e.g. Internet banking logon passwords) or verify their account information online. If in doubt, they should contact their banks."

More Information

Fraudulent email purporting to be related to The Bank of East Asia, Limited

YUI KEE
鋭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/