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

Yui Kee Computing Ltd.

Newsletter

May 2017

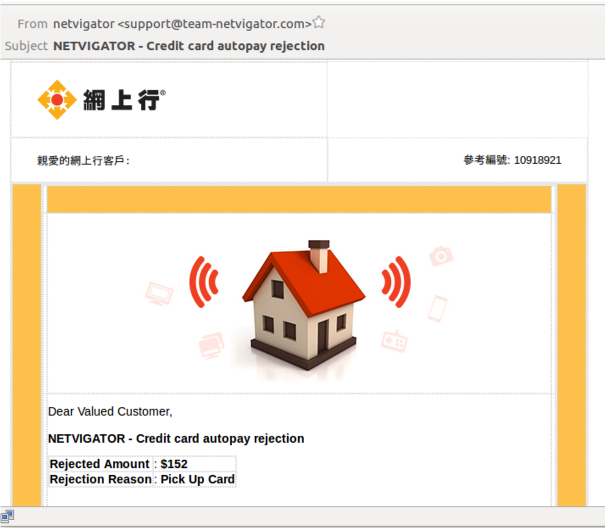
Contents

Phishing Emails Target Netvigator Customers

<web-link for this article>

Customers of Hong Kong's largest ISP, PCCW Netvigator are being targetted by emails that claim their credit card autopay has been rejected and that directs them to a webpage, hosted in Hong Kong, that collects credit card information.

The email uses Netvigator's corporate branding and appears to be sent from the plausible-sounding address "support@team-netvigator.com", although the domain team-netvigator.com does not exist. The message was sent via a German webmail service, online-service.de.



From netvigator <support@team-netvigator.com>
Subject **NETVIGATOR - Credit card autopay rejection**

網上行®

親愛的網上行客戶：

參考編號: 10918921

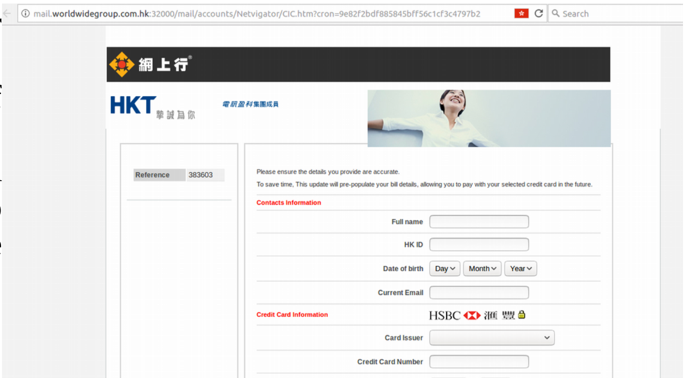
Dear Valued Customer,

NETVIGATOR - Credit card autopay rejection

Rejected Amount : $152
Rejection Reason : Pick Up Card

The link in the message, mail.isee.com.hk:32000/mail/admin/goto.html is hosted on a webmail service in Hong Kong that appears to be running the Merak Mail Server, Web Administration Version: 7.6.4 by IceWarp Software. That page redirects to mail.worldwidegroup.com.hk:32000/mail/accounts/Netvigator/CIC.htm?cron=9e82f2bdf885845bff56c1cf3c4797b2, which is also hosted on a server in Hong Kong running the same Merak Mail Server software. It may be that the German webmail service is running software based on the Merak Mail Server, and the attackers used a single vulnerability to break into all three servers.

The form, which also uses Netvigator branding, asks for the victim's name, Hong Kong ID card number, date of birth, email address, credit card issuer, credit card number, expiry date and CVV. The date is posted to Tekvew/nudnayd.php on the same server.



mail.worldwidegroup.com.hk:32000/mail/accounts/Netvigator/CIC.htm?cron=9e82f2bdf885845bff56c1cf3c4797b2

網上行®

HKT 摯誠為你

電訊盈科集團成員

Reference 383603

Please ensure the details you provide are accurate.

To save time, This update will pre-populate your bill details, allowing you to pay with your selected credit card in the future.

Contacts Information

Full name

HK ID

Date of birth Day Month Year

Current Email

Credit Card Information HSBC 滙豐

Card Issuer

Credit Card Number

Netvigator has issued advice on phishing emails.

Yui Kee's Chief Consultant,Allan Dyer, commented, "The attackers have taken some care to make their message as believable as possible, with a plausible fake email address and the expected corporate branding. However, the authorities should be able to shut down the Hong Kong servers promptly, minimising the damage."

Victims should contact the Police at 2860 5012.

Updated: 10th May 2017

Netvigator Phishing Campaign Continues

More emails targetting Netvigator customers have been received. They appear identical to the earlier messages, but link to a different Hong Kong webpage, mail.kwanming.com.hk/freebusy/Netvigator/index.php, that also asks for the victim's personal and credit card data. The sending mail server appears to be in Switzerland.

More Information

- NETVIGATOR – beware of phishing email

WannaCrypt: Are Linux Servers at Risk?

<web-link for this article>

The WannaCrypt ransomware has hit global headlines since Friday, and there is good advice available from many CERT teams and security researchers for Windows users, but what about Linux?

Although WannaCrypt cannot spread on Linux systems, affected Windows systems will check for disk drives, including network shares and removable storage devices, and encrypt files with extensions matching a long list. Therefore, if you are using a Linux computer as a file server for Windows clients, your files on the Linux server are at risk of being encrypted.

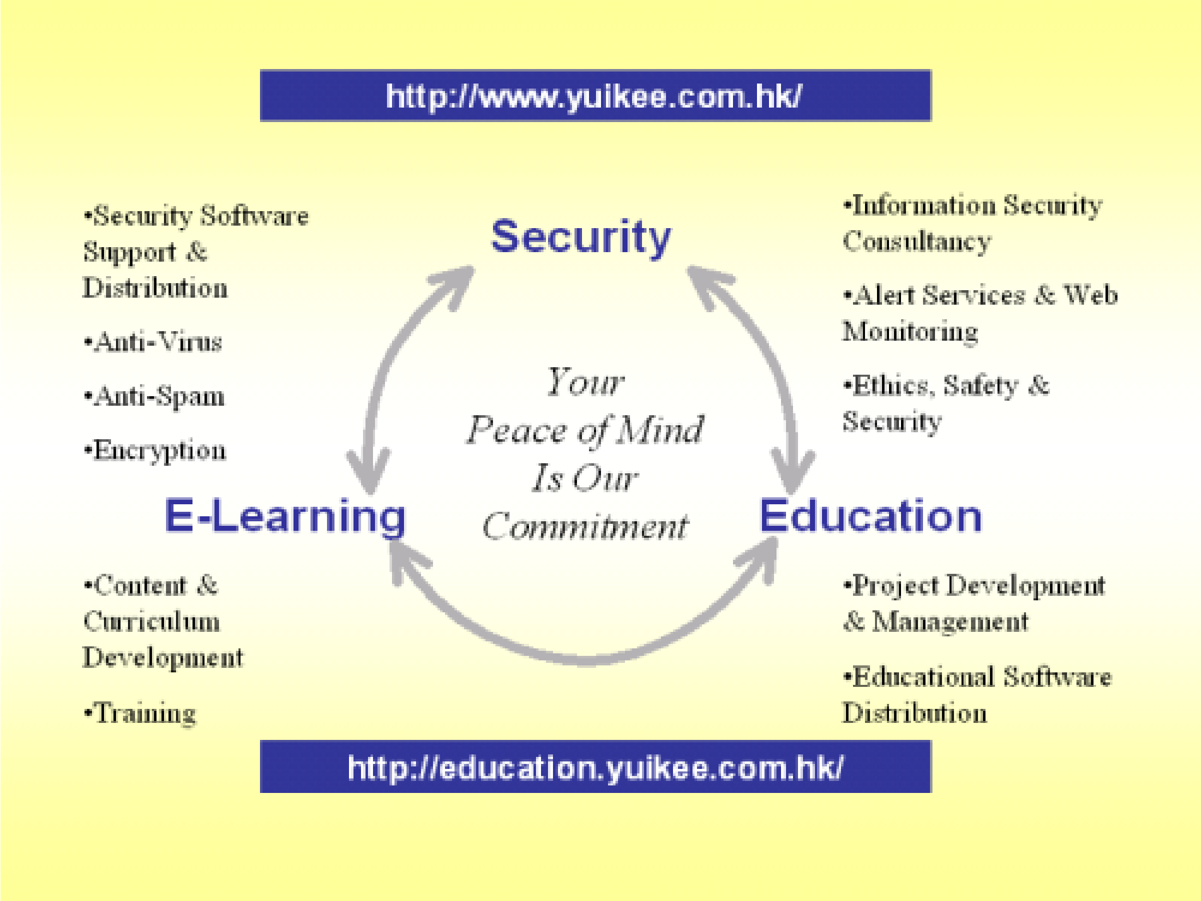
If you have a Linux fileserver with Windows clients, then consider disabling access until you can confirm that all the vulnerable clients have been updated. You might find setting access to Read Only useful in allowing some work to continue while checks continue.

Yui Kee's Chief Consultant, Allan Dyer, admitted, "Eight months ago, I predicted that 2016 was the year of Peak Ransomware, I was wrong. The WannaCrypt incident shows that there are still plenty of vulnerable systems with insufficient backups out there, and criminals are still targetting them. I was over-optimistic about how quickly the factors I mentioned would cause the decline of ransomware. How do you become part of the victory over ransomware? Take regular backups! With recent, offline backups to rely on, you can laugh at the ransom demand."

More Information

- Ransomed to Death
- WannaCry (WannaCrypt) Ransomware Encrypts Victim Data
- Beware of WannaCry Ransomware Spreading
- 74 countries hit by NSA-powered WannaCrypt ransomware backdoor: Emergency fixes emitted by Microsoft for WinXP+
- Everything you need to know about the WannaCry / Wcry / WannaCrypt ransomware
- WannaCry ransomware used in widespread attacks all over the world
- What you need to know about the WannaCry Ransomware

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

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/