May 17, 2017

Re: Wanna Crypt Ransomware Windows Security Patch.

To all of our customers and partners;

This bulletin addresses the known Microsoft Windows Security vulnerability that exposes Windows-based devices to potential WannaCrypt ransomware attacks. As many Windows users around the world are being affected by Wanna Crypt ransomware (malware) attack that locks their files/data pending ransom payment, we would like to remind our customers how to keep their video security systems safe.

Ransomware is a computer virus that prevents the users from accessing the operating system, or encrypts all the data stored on the computer.
The user is asked to pay a ransom (often in bitcoin currency) in order to decrypt their files or gain access to their operating system.

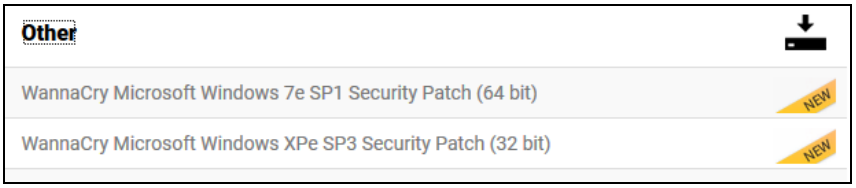
Note: Virus **WannaCrypt** is also detected as: WORM_WCRY.A (Trend Micro); Trojan.Ransom.WannaCryptor.H (BitDefender); Trojan/Win32.WannaCryptor (AhnLab); WannaCry (other)

Installing Microsoft Windows Security Patch.

All standard i3 NVR systems purchased after April 10th, 2017 have the necessary Microsoft Windows security patch installed. **All other users are urged to update their Windows OS immediately.**
This applies to all users with NVR serial numbers **174047 and below** as well as all customers using "Special Build" customized NVR units.

For your convenience, we have made Microsoft Windows security patches available for download from our website. To download the security patch, please follow instructions below:

1. Go to www.i3international.com/software-downloads
2. Click on **Other**



3. Download WannaCry Microsoft Windows security patch suitable for your operating system: Windows 7e SP1 or Windows XPe SP3.
4. Safely close the SRX-Pro Server software to access your Desktop (Login as an administrator user and press **Ctrl + Alt + Shift + F4**)
5. Un-zip and run the security patches on your HVR/NVR to install them.
6. Re-start SRX-Pro Server software and log in.
7. Go **File** > **Shutdown** and allow your Server to shut down.
8. Press the Power button on the front panel of your unit to restart your Server.

www.i3international.com
1 866 840 0004

CANADA 780 Birchmount Road,
Unit 16, Scarborough
ON, M1K 5H4

USA: 4450 Witmer Industrial Estates
Unit 4, Niagara Falls,
NY, 14305

Regular Windows OS Updates

Important notice to Dealers

Because most Windows Upgrades require system reboot and some updates require user intervention, Automatic Windows Upgrades are **disabled** on all i3 NVR Servers. It is the responsibility of the customer to ensure that their Windows OS is up-to-date and all Security and other OS updates are downloaded and installed in a timely manner.

Windows Updates must be manually downloaded and installed **regularly** to maintain the security of i3 HVR/NVR Servers, especially i3 Servers that are connected to the Internet.

All i3 Dealers are strongly encouraged to educate their customers on the importance of regular Windows Updates. The dealers are encouraged to train End Users to perform the updates themselves, add this service to all maintenance contracts or reach out to existing customer base and suggest a service maintenance call with explicit purpose of protecting i3 Servers from WannaCry virus and all other Windows vulnerabilities.

Additional Safety Tips for your i3 Server.

- Always download and install Windows Updates.
- Use Antivirus software (not included with i3 Server) and always install most recent updates.
  Important: Scan C:\ and D:\ drives only. Do not scan video storage drives.
  Read 170505-HW-03_NVR_Antivirus_Scanning_Instructions.pdf bulletin for more information.
- Do not open email attachments unless you are expecting them. When receiving attachments/links from known contacts, confirm the safety of the file/link with them before opening – infected computers are able to send out emails/messages to the contacts in the address book.
- Do not click on suspicious links in unsolicited emails, text messages or social media messages/websites.
- Do not visit unsafe or unreliable websites. Phishing emails often masquerade as a known/popular/trusted website or service. The perpetrators, however, will not be able to use the legitimate web address. Check the link address without clicking on it by hovering the mouse cursor over the link.

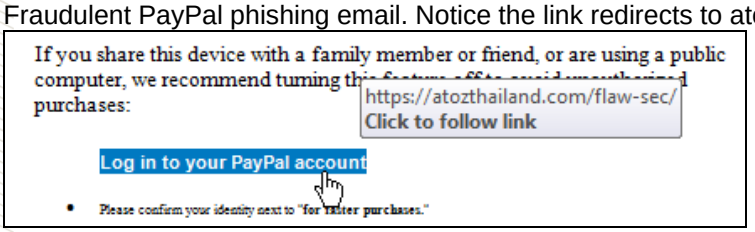
www.i3international.com
1 866 840 0004

CANADA 780 Birchmount Road,
Unit 16, Scarborough
ON, M1K 5H4

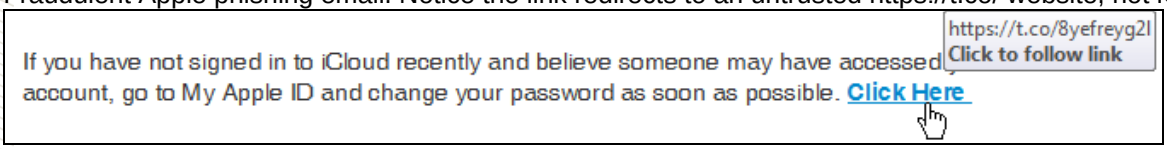
USA: 4450 Witmer Industrial Estates
Unit 4, Niagara Falls,
NY, 14305

Examples of fraudulent "phishing" emails:
To confirm the identity of the link in the suspicious email, hover your mouse cursor above the link. **Do not click on it.** You will be able to see the link address.

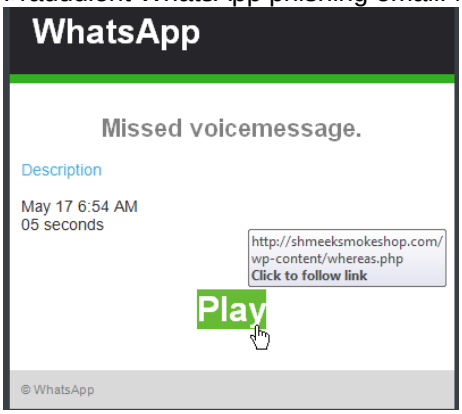
Fraudulent PayPal phishing email. Notice the link redirects to atozthailand.com, not PayPal.



Fraudulent Apple phishing email. Notice the link redirects to an untrusted https://t.co/ website, not iCloud/Apple.



Fraudulent WhatsApp phishing email. Notice the link redirects to shmeeksmokeshop.com, not WhatsApp.



Please contact technical support if you have any questions or issues.
Email: support@i3international.com
Tel.: 1.877.877.7241
Live Chat: http://i3chat.i3international.com/chat

www.i3international.com
1 866 840 0004

CANADA 780 Birchmount Road,
Unit 16, Scarborough
ON, M1K 5H4

USA: 4450 Witmer Industrial Estates
Unit 4, Niagara Falls,
NY, 14305