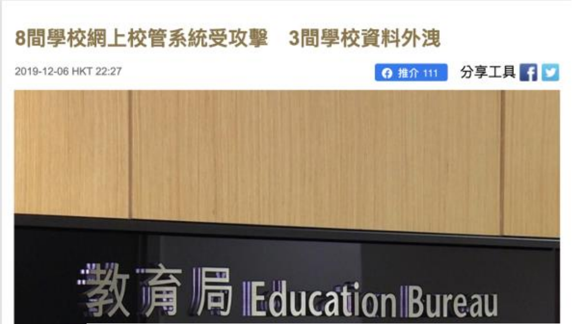
學校網絡安全的挑戰與防護

思科系統(香港)有限公司

亞太區網路安全顧問 莫偉基先生

Recent Cyber Security Incident

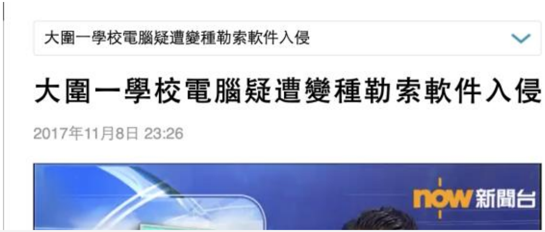


8間學校網上校管系統受攻擊　3間學校資料外洩

2019-12-06 HKT 22:27

推介 111 分享工具

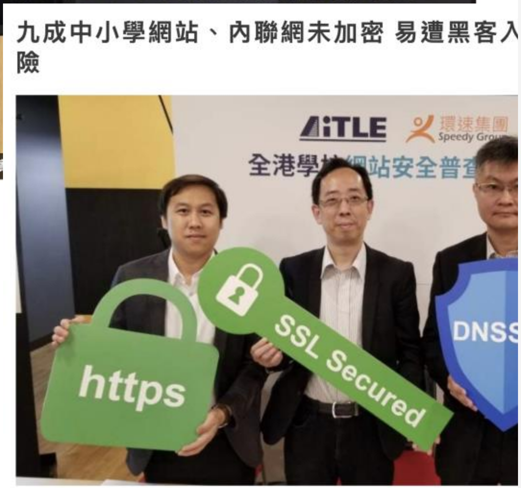
教育局證實



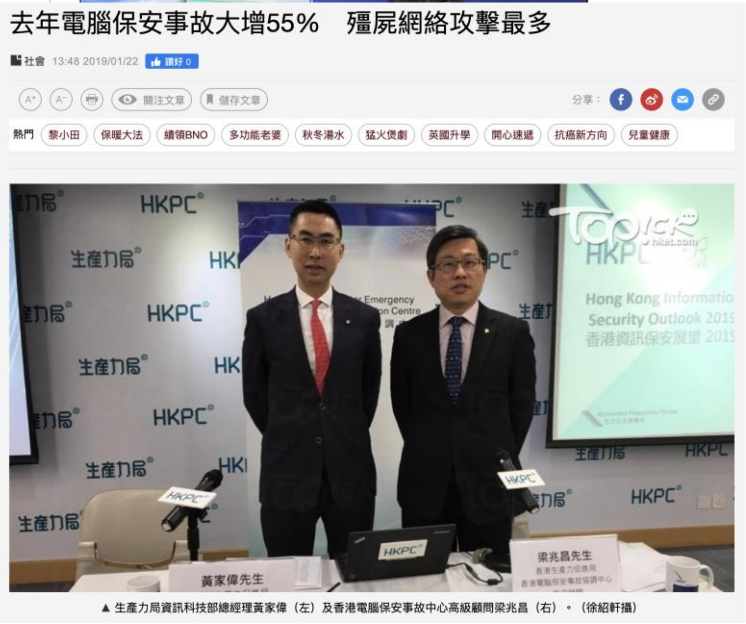
大圍一學校電腦疑遭變種勒索軟件入侵

大圍一學校電腦疑遭變種勒索軟件入侵

2017年11月8日 23:26



九成中小學網站、內聯網未加密 易遭黑客入
險



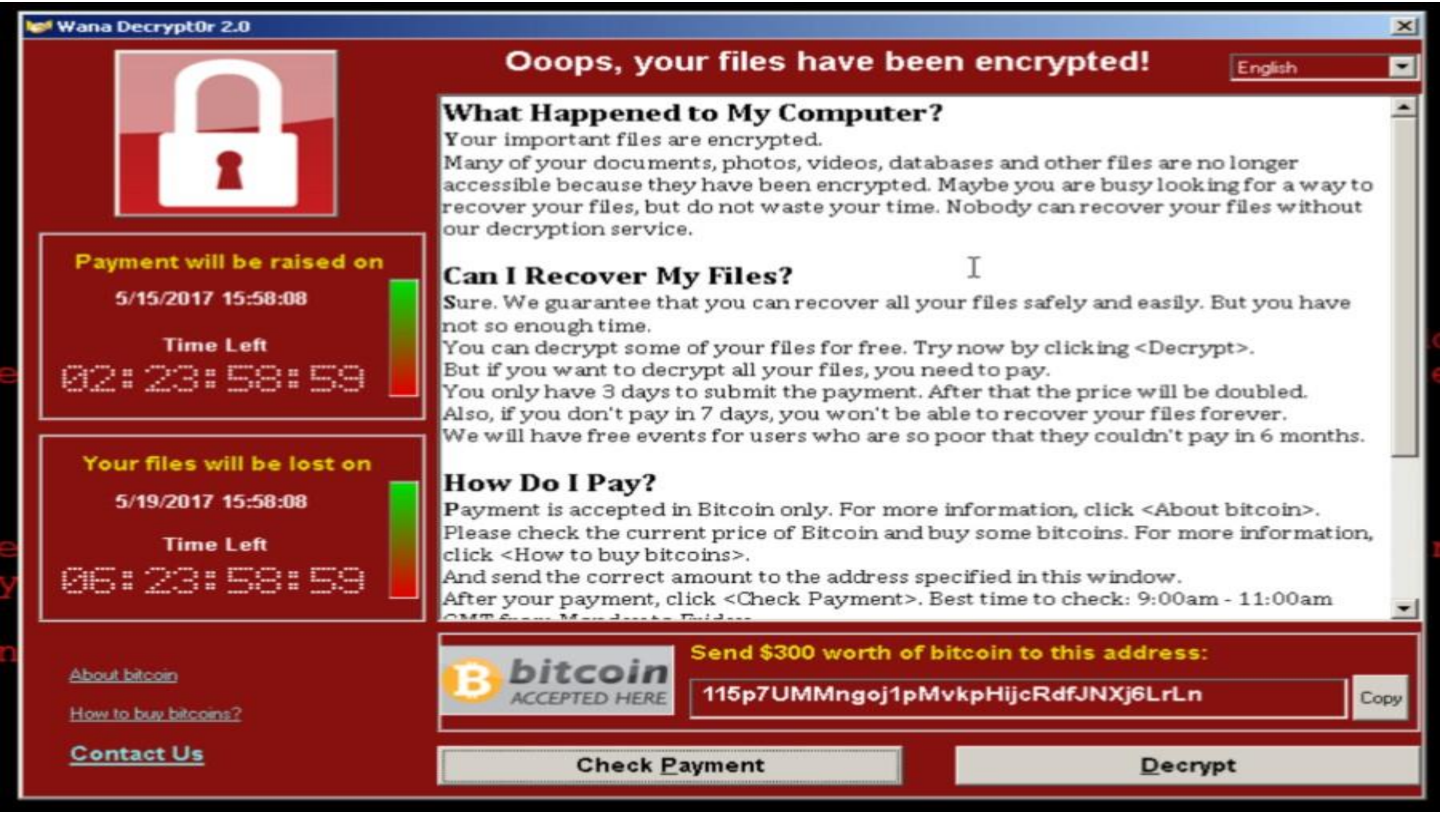
去年電腦保安事故大增55%　殭屍網絡攻擊最多

社會 13:48 2019/01/22 讚好 0

A+ A- 關注文章 儲存文章 分享：

熱門 黎小田 保暖大法 續領BNO 多功能老婆 秋冬湯水 猛火煲劇 英國升學 開心速遞 抗癌新方向 兒童健康

▲ 生產力局資訊科技部總經理黃家偉（左）及香港電腦保安事故中心高級顧問梁兆昌（右）。（徐紹軒攝）



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Three threats most likely to cause damage in 2019

Malicious cryptomining

Hackers want to make money and use your infrastructure to do it.

As the infection spreads, it reduces system performance and raises costs across your organization by draining your computing power.

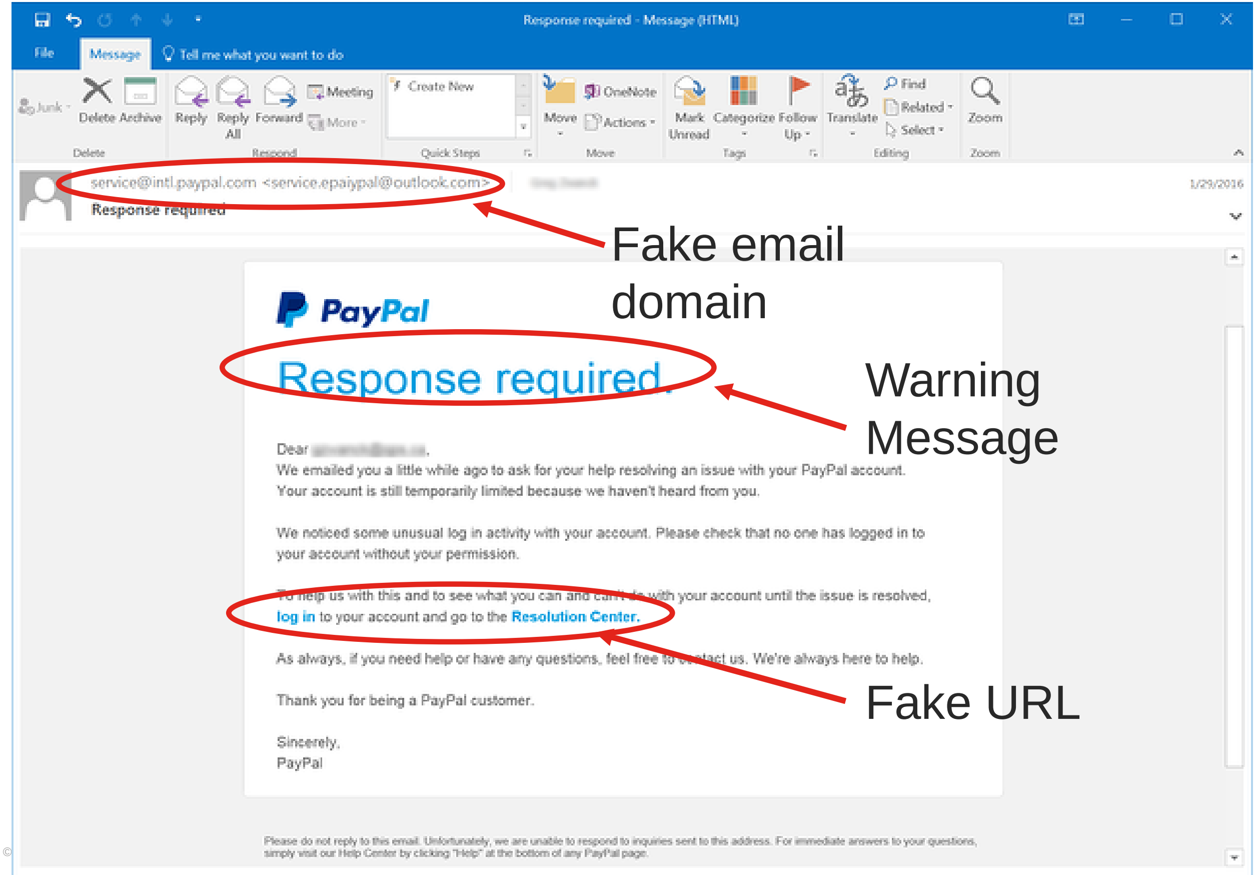
Ransomware

It doesn’t matter if the initial threat is to personal information or client data, if a machine is infected with ransomware, your entire organization could be at risk. Attacks can lie dormant for an undetermined length of time, making them even harder to spot and stop.

Phishing

Attackers can easily obtain sensitive information such as usernames, passwords, banking data, or credit card details. If an employee opens a phishing email at work, or follows a malicious link, they could put the whole organization in jeopardy without realizing it.

Threat from Email



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted] 1/29/2016

Response required

PayPal

Response required

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

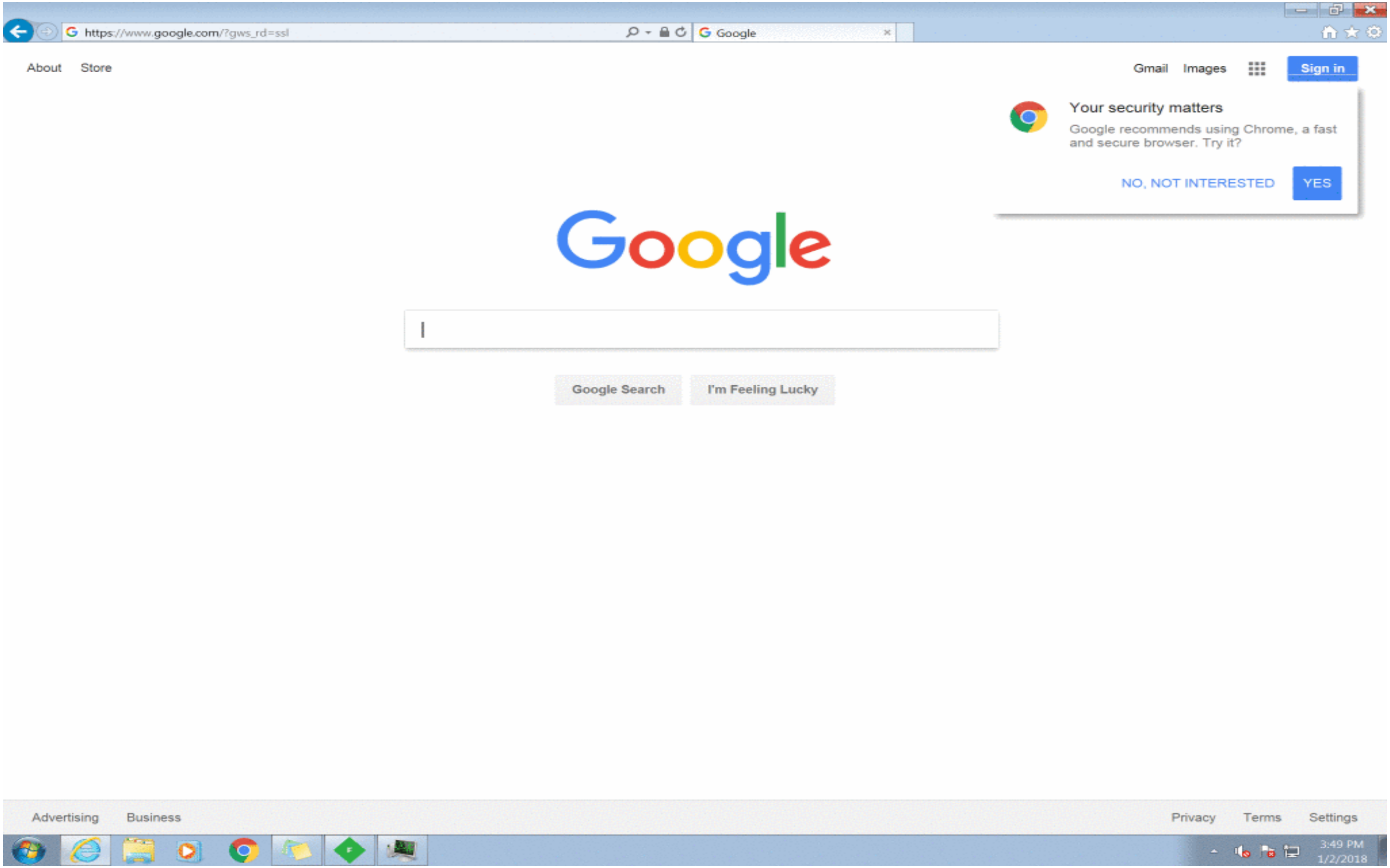
Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Fake email domain

Warning Message

Fake URL

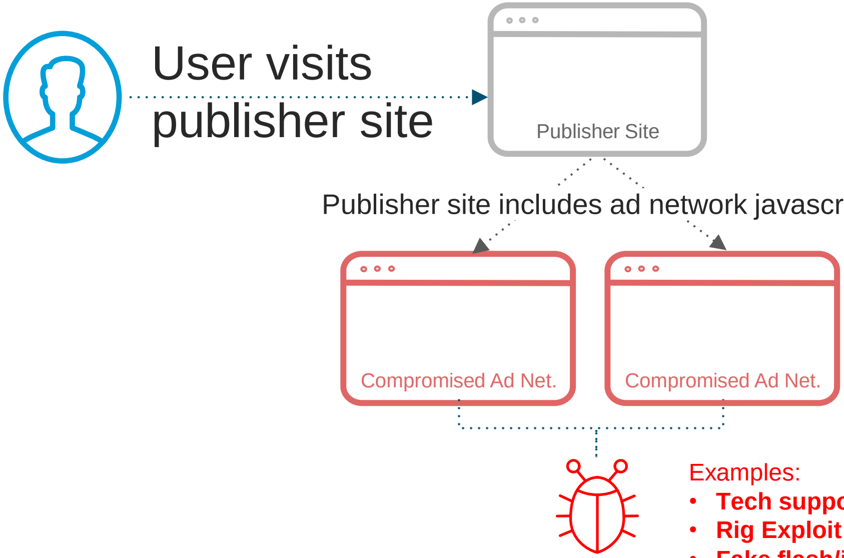


Your security matters

Google recommends using Chrome, a fast and secure browser. Try it?

NO, NOT INTERESTED YES

Ad Campaign Flow (廣告活動流程)



User visits publisher site

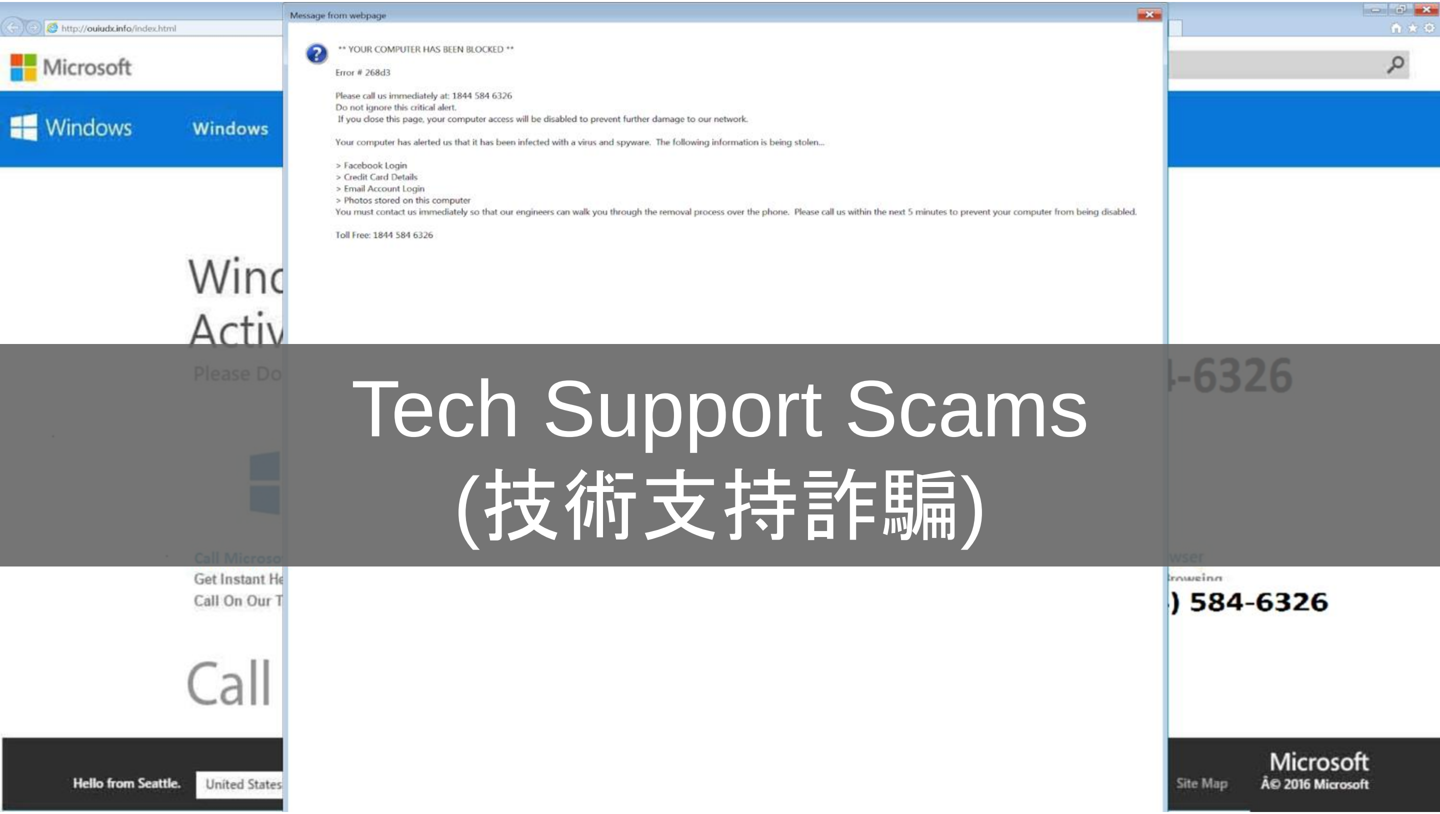
Publisher site includes ad network javascript

Examples:

- **Tech support scam (技術支持詐騙)**
- **Rig Exploit Kit (**惡意活動分析報告**)**
- **Fake flash/java update (偽造的Flash和Java更新**)

Ad network fingerprints and sends user to malvertisement

Tech Support Scams
(技術支持詐騙)



** YOUR COMPUTER HAS BEEN BLOCKED **

Error # 268d3

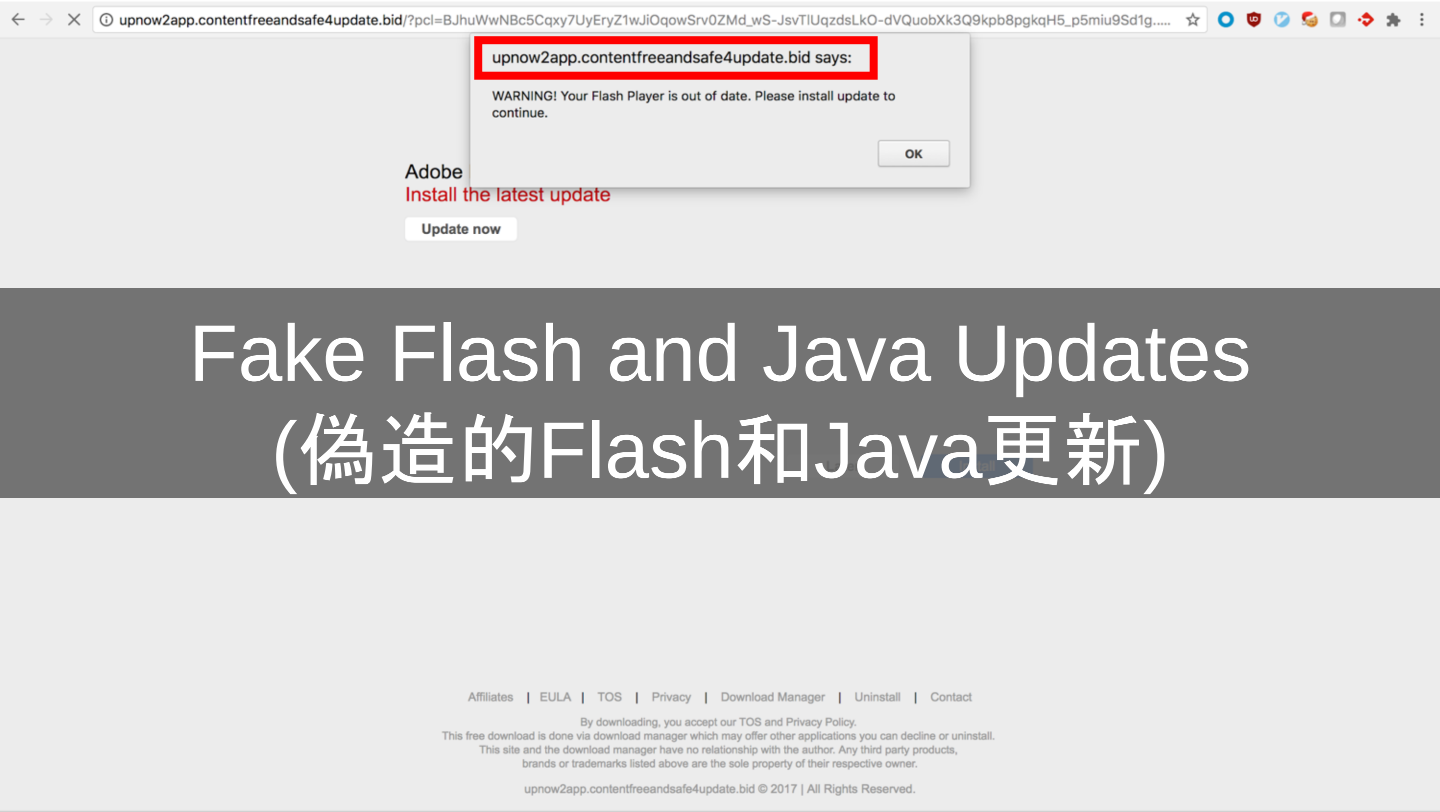
Please call us immediately at: 1844 584 6326
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. The following information is being stolen...

> Facebook Login
> Credit Card Details
> Email Account Login
> Photos stored on this computer
You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: 1844 584 6326

Fake Flash and Java Updates (偽造的Flash和Java更新)



upnow2app.contentfreeandsafe4update.bid/?pcl=BJhuWwNBc5Cqxy7UyEryZ1wJiOqowSrv0ZMd_wS-JsvTlUqzdsLkO-dVQuobXk3Q9kpb8pgkqH5_p5miu9Sd1g.....

upnow2app.contentfreeandsafe4update.bid says:

WARNING! Your Flash Player is out of date. Please install update to continue.

Adobe

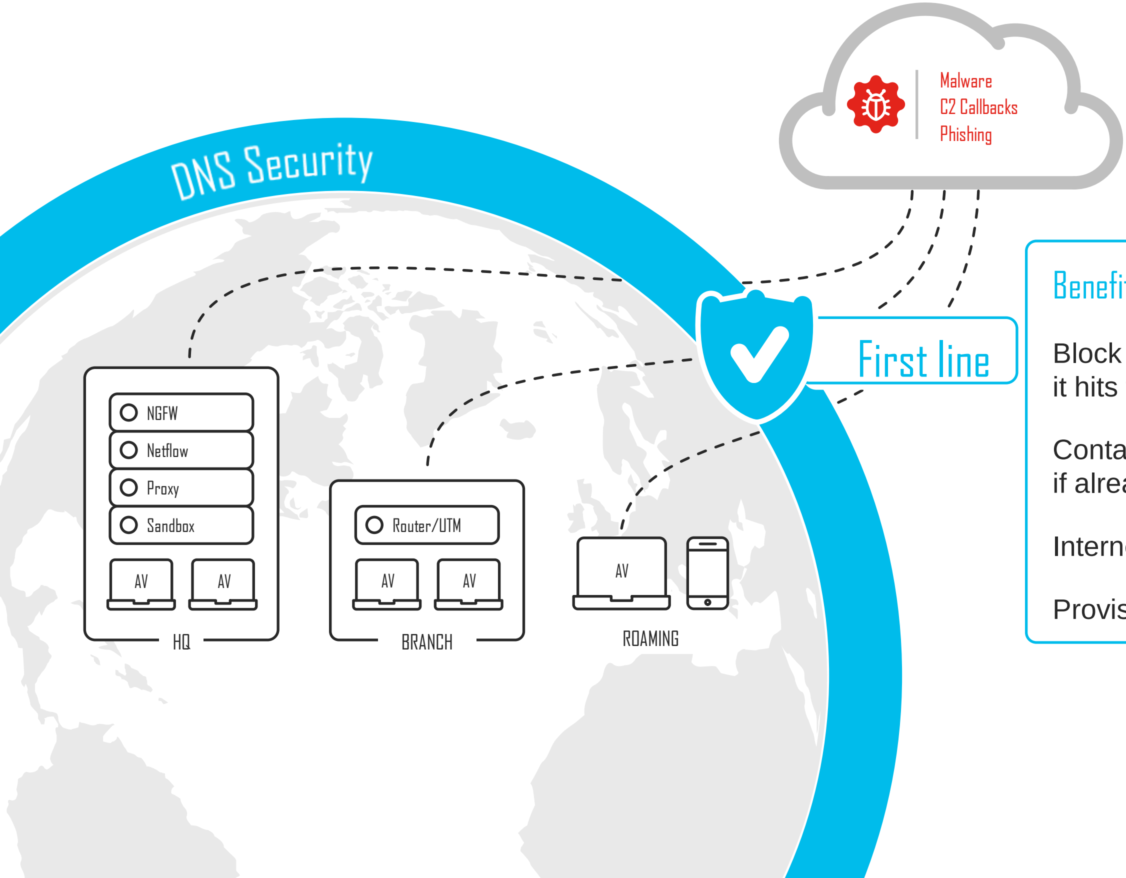
Install the latest update

Affiliates | EULA | TOS | Privacy | Download Manager | Uninstall | Contact

By downloading, you accept our TOS and Privacy Policy.
This free download is done via download manager which may offer other applications you can decline or uninstall.
This site and the download manager have no relationship with the author. Any third party products, brands or trademarks listed above are the sole property of their respective owner.

upnow2app.contentfreeandsafe4update.bid © 2017 | All Rights Reserved.

Where does DNS Security fit?



Benefits

Block malware before it hits the enterprise

Contains malware if already inside

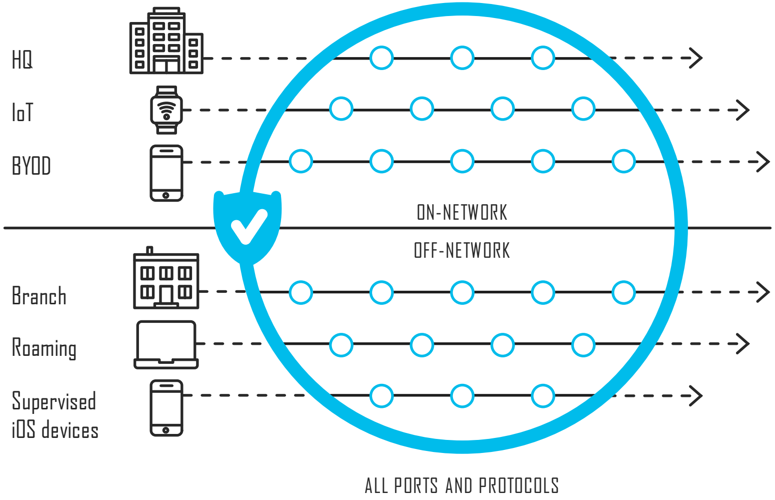
Internet access is faster

Provision globally in minutes

Visibility and protection for all activity, anywhere

ENFORCEMENT

DNS Security Services



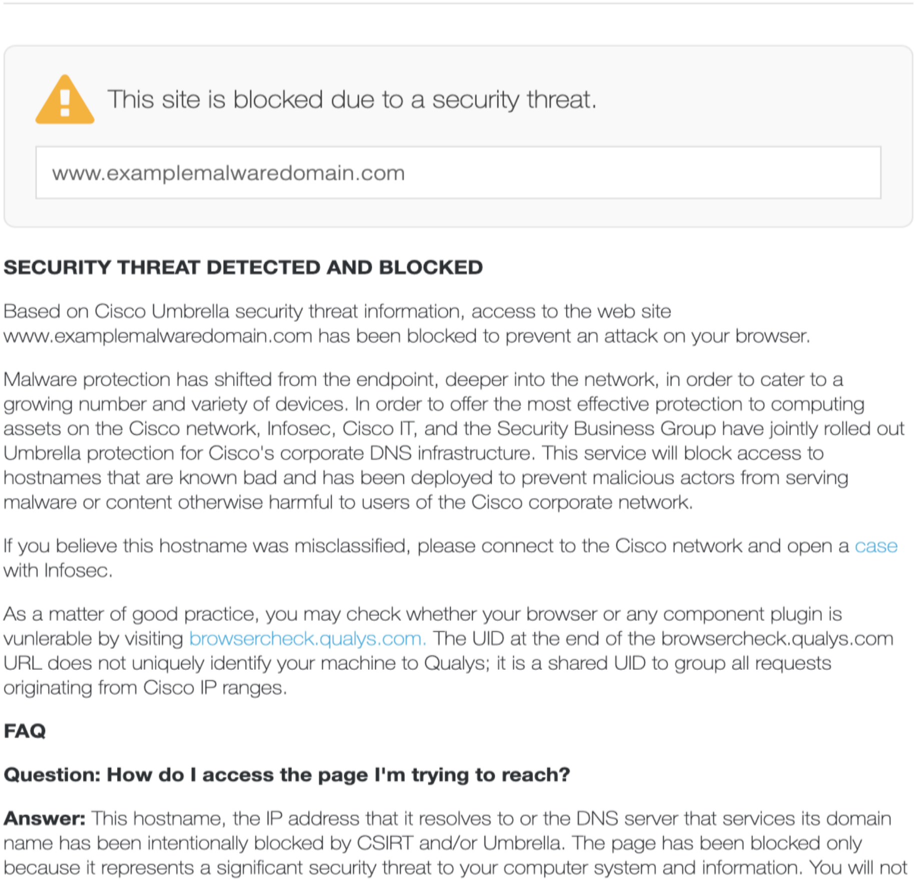
All office locations

Any device on your network

Roaming laptops and supervised iOS devices

Every port and protocol

Domain / URL Blocking



⚠ This site is blocked due to a security threat.

www.examplemalwaredomain.com

SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco Umbrella security threat information, access to the web site www.examplemalwaredomain.com has been blocked to prevent an attack on your browser.

Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this hostname was misclassified, please connect to the Cisco network and open a case with Infosec.

As a matter of good practice, you may check whether your browser or any component plugin is vunlerable by visiting browsercheck.qualys.com. The UID at the end of the browsercheck.qualys.com URL does not uniquely identify your machine to Qualys; it is a shared UID to group all requests originating from Cisco IP ranges.

FAQ

Question: How do I access the page I'm trying to reach?

Answer: This hostname, the IP address that it resolves to or the DNS server that services its domain name has been intentionally blocked by CSIRT and/or Umbrella. The page has been blocked only because it represents a significant security threat to your computer system and information. You will not

Questions?

Built into foundation of the internet

ENFORCEMENT

Destinations

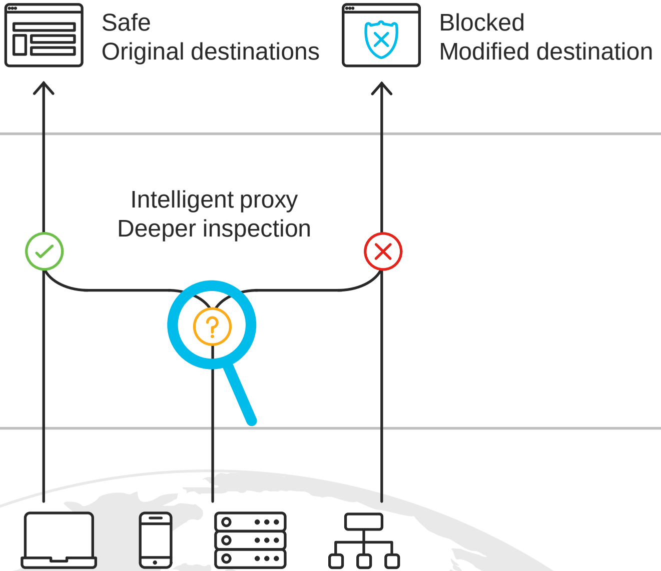
Original destination or block page

Security controls

- DNS and IP enforcement
- Risky domain inspection through proxy
- SSL decryption available

Internet traffic

On and off-network



Safe
Original destinations

Blocked
Modified destination

Intelligent proxy
Deeper inspection