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
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 GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

115p7UMMnogoj1pMvkJcRdfJNXj6LrLn

Check Payment
Decrypt
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

Fake email domain

Response required

Warning Message

Fake URL
Ad Campaign Flow (廣告活動流程)

User visits publisher site

Publisher site includes ad network javascript

Compromised Ad Net.

Compromised Ad Net.

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

DNS Security
- NGFW
- Netflow
- Proxy
- Sandbox

First line
- AV
- AV
- AV
- AV

HQ
- Router/UTM
- AV
- ROAMING

BRANCH
- AV

ROAMING
Visibility and protection for all activity, anywhere

DNS Security Services

- HQ
- IoT
- BYOD
- Branch
- Roaming
- Supervised iOS devices

All office locations
Any device on your network
Roaming laptops and supervised iOS devices
Every port and protocol

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
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 vulnerable 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

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