

# Information Security Trends and Directions



# Types of Cyber Attacks

- SPAM
- Phishing scams
- Worms
- Spyware
- distributed denial-of-service attacks (DDoS)
- Botnets



# Hacking

- Hacking is the act of gaining access to a computer or computer network to obtain or modify information without legal authorization.
- Why hacking?
- Hacking vs Cracking
- Steps involved in Hacking
  - 1. Reconnaissance
  - 2. Scanning
  - 3. Gaining access
  - 4. Maintaining access
  - 5. Cover the tracks

# Denial-of-Service and Distributed Denial-of-Service

- What is denial of Service?
- Example a web site for on-line shopping
- Distributed Denial-of-Service (DDoS) attacks are where multiple participating devices engage in DoS attacks from a distributed locations.
- **DDoS metrics**
- **Compared with Q1 2015**
- 125.36 percent increase in total DDoS attacks
- 142.14 percent increase in infrastructure layer (layers 3 & 4) attacks
- 34.98 percent decrease in the average attack duration: 16.14 vs. 24.82 hours
- 137.5 percent increase in attacks > 100 Gbps: 19 vs. eight

# Malicious Code

- Computer Virus
- Worm
- Trojan horse

# Social Engineering

- Art of getting people to divulge information
- Being helpful or intimidation
- **Countermeasures**
- Train the employees
- Dispose of sensitive information securely
- Prevent Dumpster Diving

# Phishing



## NOTICE

Dear Email Client,

In line with the Gmail's policy and pursuant to the terms and conditions of the account accepted by you, in accordance with applicable rules and regulations, We are reviewing all our accounts and pursuant to the review, Google may take extra decision to close certain accounts.

Therefore, Google has decided to close your account. If you still want to maintain your account with us, find in the **attached our account review and update instruction**.

**This is valid for 72-Hours**

In case we don't hear from you within the above stated time period, Google will proceed to close your account after 30 days from the date of this notice. All the contents of your account will be permanently deleted.

# Countermeasures

- Do not offer any information
- Do not open any e-mail attachments
- Do not follow any hyperlinks or URL's
- Do not reply



# SPAM

- Unwanted e-mails



# Ransomware

A type of malware which restricts access to the computer system that it infects, and **demands a ransom** paid to the creator(s) of the malware in order for the restriction to be removed.



## How HolyCrypt encrypts a victim's Data

This version of HolyCrypt will only encrypt files located under the %UserProfile% folder and will only encrypt certain file extensions. These extensions are:

```
.txt, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd
```

# YOUR COMPUTER HAS BEEN LOCKED!



Your documents, photos, databases and other important files have been locked with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

The server will eliminate the key after 24h.

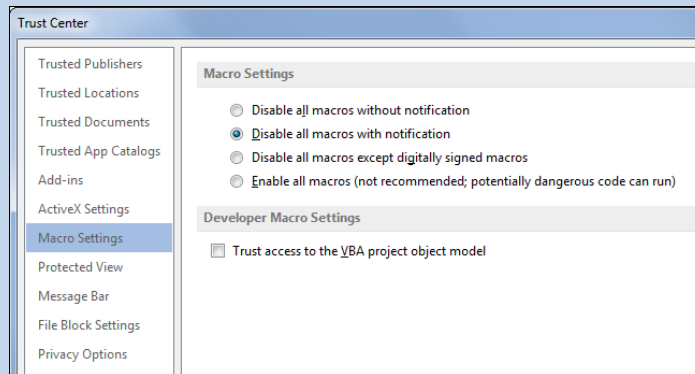
Open [http://test\\_ransomware.onion.link](http://test_ransomware.onion.link) and follow the instruction for the payment

# Security Solutions

- **At a minimum you should**
- Deploy Anti-virus protection
- Block SPAM
- Use a sandboxing solution
- Block risky file extensions(javascript,vbscript,chm etc)
- Use URL filtering (block access to C&C servers)
- Activate your client Firewalls
- Use HIPS (Host Intrusion prevention service)

# Best Practices

1. Backup regularly and keep a recent backup copy off-site
2. Don't enable macros in document attachments received via e-mail
3. Don't give yourself more login power than you require
4. Consider installing Microsoft Office Viewers
5. Patch early patch often
6. Configure your security products correctly



# Trends in Information Security Threats

- Do not offer any information
- Do not open any e-mail attachments
- Do not follow any hyperlinks or URL's
- Do not reply

## Recent News

Over 60% of confirmed data breaches involve using weak, default, or stolen passwords. Even with security education and training, many employees still can't recognize a phishing attempt.

(<http://www.cert.gov.lk/alerts.php>)

The screenshot shows a web browser window with the URL [www.cert.gov.lk/alerts.php](http://www.cert.gov.lk/alerts.php). The page features a navigation bar with a search box containing the text "Search | Protection by F-Secure". The main content area is divided into two columns. The left column contains a "News" section with a compass icon and a list of news items, followed by an "Alerts" section with a megaphone icon and a list of alert titles. The right column contains a large "Alerts" section with a globe icon and a table of security alerts.

### News

- Sri Lanka CERT|CC helps establish Tonga CERT
- Bridging the Air-Gap-Vulnerabilities in Isolated Networks
- Cyber Security Week 2015- Be united..Be Secure...
- FLAME - The New Cyber Threat
- Is your computer infected with DNSChanger?

[More...](#)

### Alerts

- Multiple Vulnerabilities in Cisco
- CERBER Ransomware
- Multiple Vulnerabilities in Cisco

### Alerts

Released Date	Risk Level	Alert
2016-06-23	High	Multiple Vulnerabilities in Cisco
2016-06-02	High	CERBER Ransomware
2016-05-27	High	Multiple Vulnerabilities in Cisco
2016-05-16	High	RDP Drive Redirection Information Disclosure Vulnerability in Microsoft Windows Volume Manager Drive
2016-04-29	High	Multiple Vulnerabilities in Oracle Databases
2016-04-06	High	Possible Cyber Attacks During the Holiday Season
2016-03-30	Medium	Cross site scripting vulnerability in IBM WebSphere Application Server
2016-03-08	High	Multiple vulnerabilities in Google Chrome
2016-03-08	High	Multiple vulnerabilities in Google Chrome
2016-03-02	High	DROWN - Cross-protocol attack on TLS using SSLv2
2016-02-18	Medium	Multiple Vulnerabilities in Libgraphite library in Mozilla Firefox




# Subscribe

Subscribe

www.cert.gov.lk/subscribe.php

Search | Protection by F-Secure

Home About Us Services Knowledge Base Alerts Events Contact Us

 National Centre for Cyber Security

Follow @SLC

**News**

- Sri Lanka CERT|CC helps establish Tonga CERT
- Bridging the Air- Gap- Vulnerabilities in Isolated Networks
- Cyber Security Week 2015- Be united..Be Secure...
- FLAME - The New Cyber Threat
- Is your computer infected with DNSChanger?

**Subscribe**


Your Name:\*

Address:\*

Your E-mail:\*

Company Name:

Designation:\*



# Challenges encountered via online

- **Sextortion**
- **Online gaming**
- **Sexting**
  
- **Advice for parents and teachers**
- Educate the children regarding dangers of sharing personal photos even with known people specially sexting. The things they perform now can have serious repercussions in the future to tarnish their image and reputation.

# Contact

## Address

Room 4-112, BMICH, Bauddhaloka  
Mawatha,  
Colombo 07, Sri Lanka.

Tel: +94 112 691692 /2 691064 /2 679888

Fax: +94 112 691064

E-mail: [report@cert.gov.lk](mailto:report@cert.gov.lk)

<http://www.cert.gov.lk>

