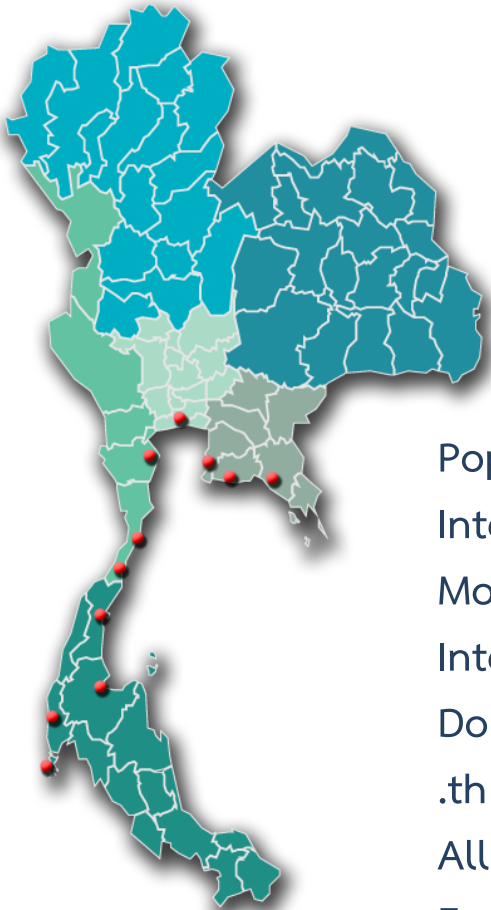


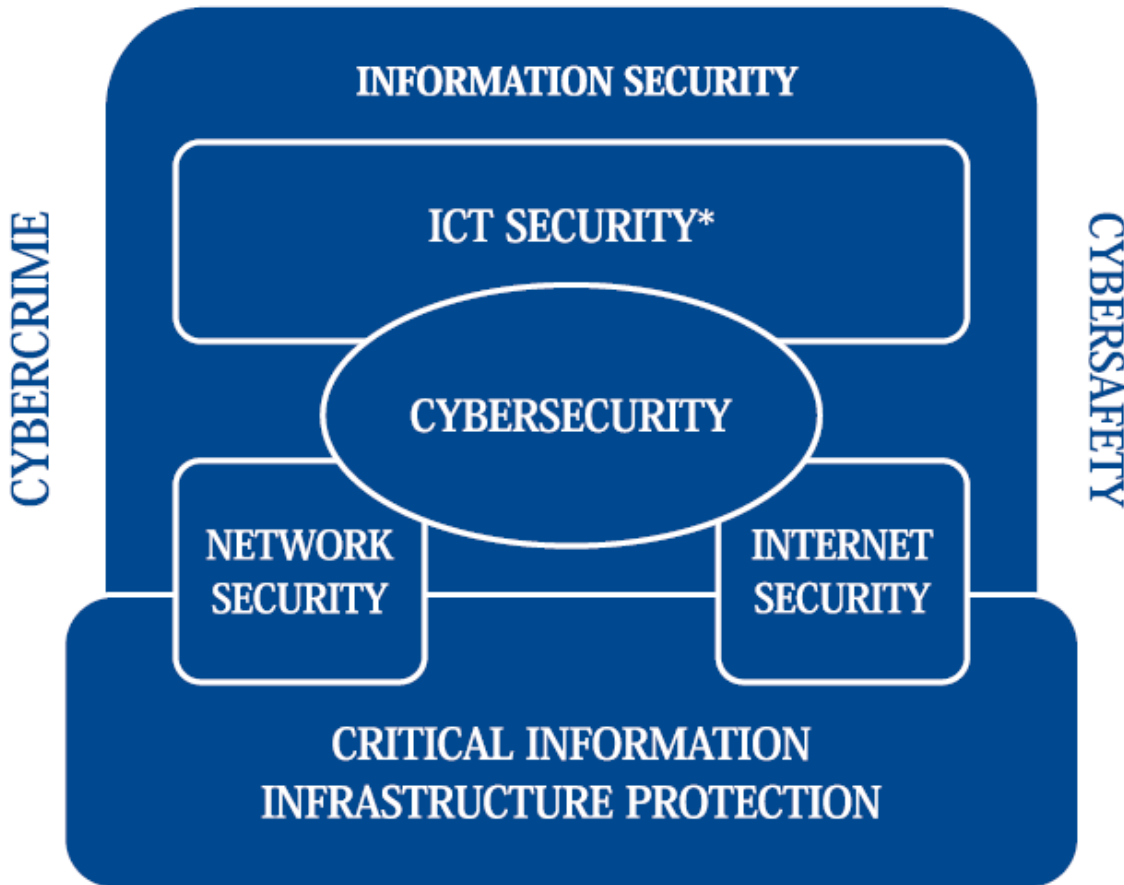
Statistics and status of incidents of government websites

Statistics Of Internet In Thailand



Population:	64.457 M
Internet users:	24 M
Mobile phone subscribers:	87.446 M
International Bandwidth:	507.084 Gbps
Domestic Bandwidth:	1.223 Tbps
.th domain names:	64,316
All domain names:	246,274
Facebook users:	18.766 M
Twitter users:	2 M

Core Of Cyber Security



C.I.A.

- **Confidentiality**
- **Integrity**
- **Availability**

10 RISKIEST COUNTRIES

1  INDONESIA

2  CHINA

3  THAILAND

4  PHILIPPINES

5  MALAYSIA

6  INDIA

7  MEXICO

8  UAE

9  TAIWAN

10  HONG KONG

*** Threat exposure rate (TER) : Measured as the percentage of PCs that experienced a malware attack, whether successful or failed, over a three month period – Source : Security Threat Report 2013 - SophosLabs

ThaiCERT – A Quick Introduction

- Thailand Computer Emergency Response Team (ThaiCERT)
 - A government funded unit, established in 2000
 - The first and only non-profit CERT (Computer Emergency Response Team) in Thailand
 - Provides its incident response service to Thai local constituency, or to other international entities where the sources of attacks originate from Thailand

ThaiCERT Incident Coordination Service

- Receive incident reports nationally and internationally
- Assign each incident report with a unique ticket number to keep track of the resolution development
- Maintain a up-to-date Point-of-Contact (PoC) of both public and private sectors in Thailand
- Operate with quality assurance (2-day)
- Provide 24x7 incident response service

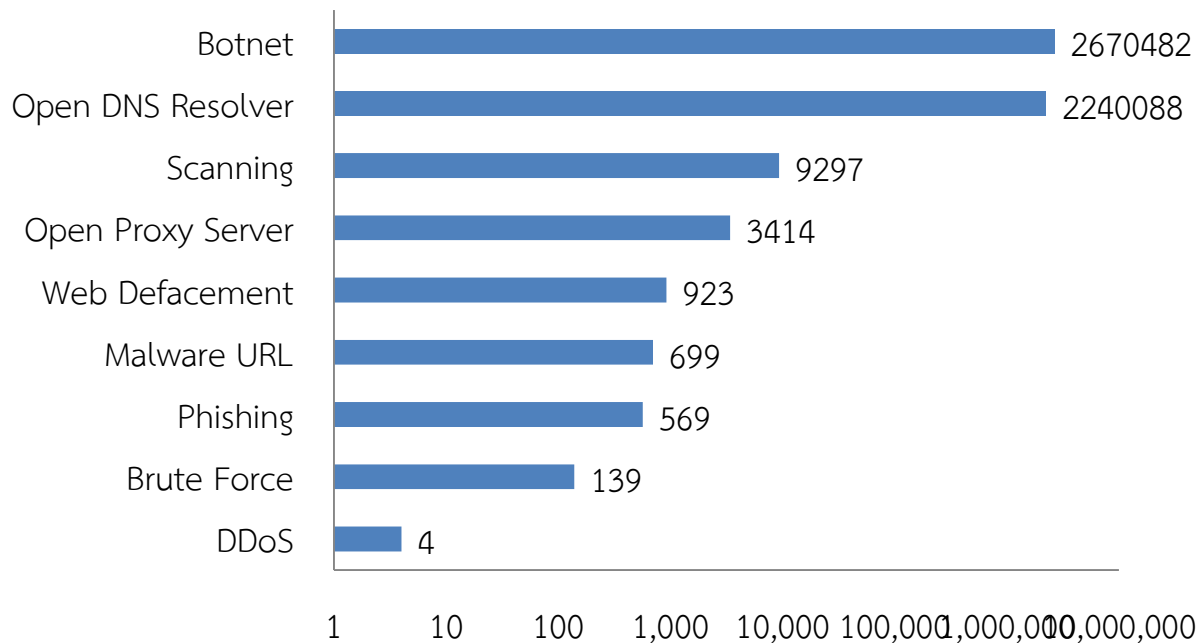
ThaiCERT Incident Coordination Service

- For statistical purposes, standard incident types were defined based on ECSIRT classification*
 - **Abusive Content** – Spam, Child/Sexual/Violence
 - **Malicious Code** – Virus, Worm
 - **Information Gathering** – Scanning, sniffing
 - **Intrusion Attempts** – Exploiting of known vulnerability, Login attempts
 - **Intrusions** – Account Compromise, Application Compromise
 - **Availability** – DOS, DDOS
 - **Fraud** – Phishing, Copyright
 - **Other**

* ECSIRT Incident Classification

available at <http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6>

Unique IPs Through Automatic Feed In 2014

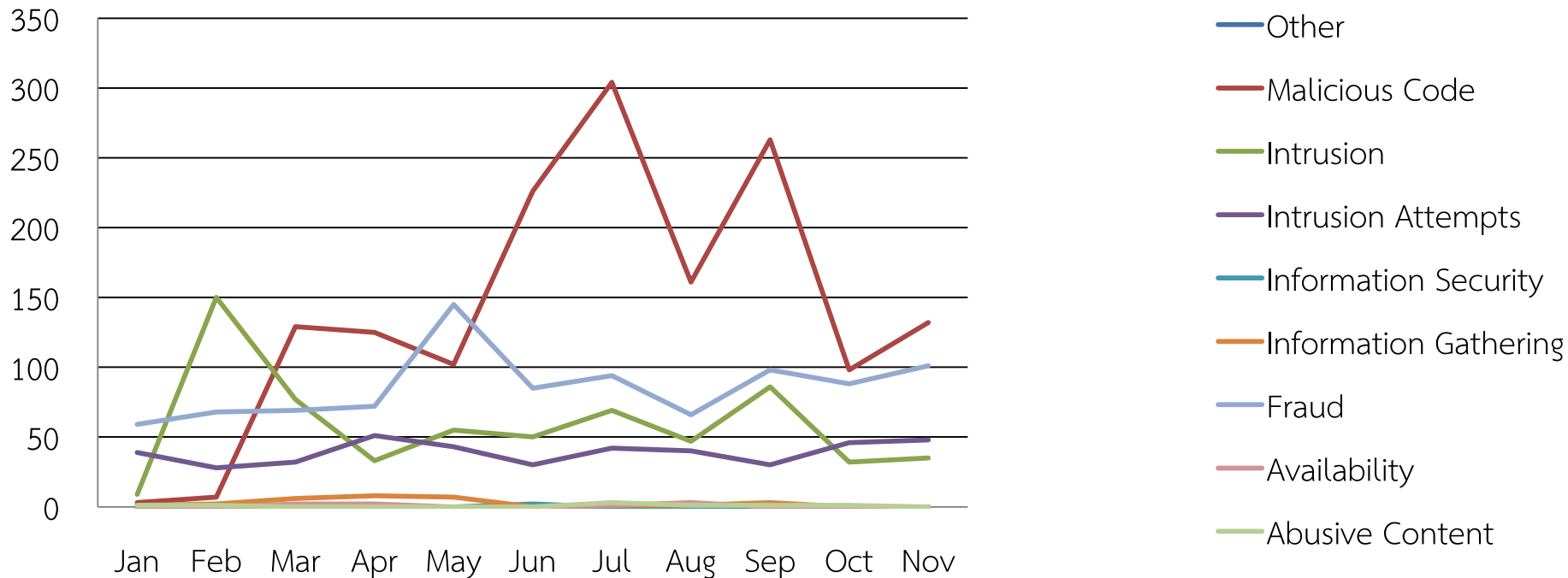


Total number of unique IPs:
4,925,615

Top 3
1. Botnet 54%
2. Open DNS Resolver: 45%
3. Scanning: 0.2%

Data from Jan – Nov 2557

Directly Reported Incidents To ThaiCERT In 2014 Per Type



Number of reports: 3,616

1. Malicious Code: 1,550 reports (43%)
2. Fraud: 945 reports (26%)
3. Intrusion Attempts: 643 reports (18%)

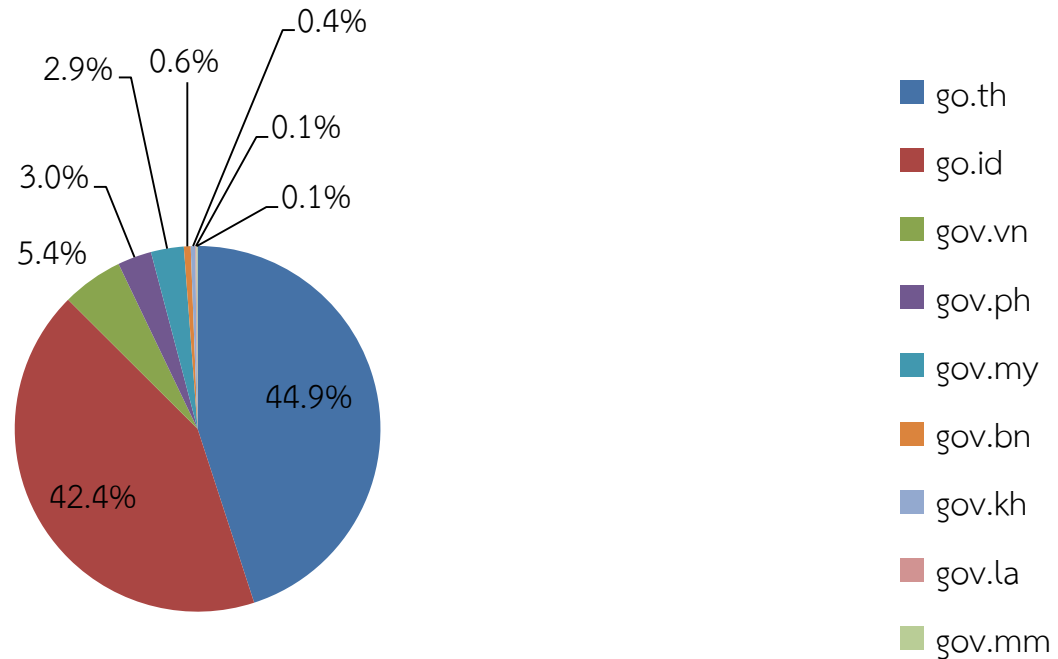
Web Defacements

n [REDACTED] n.go.th/index.php



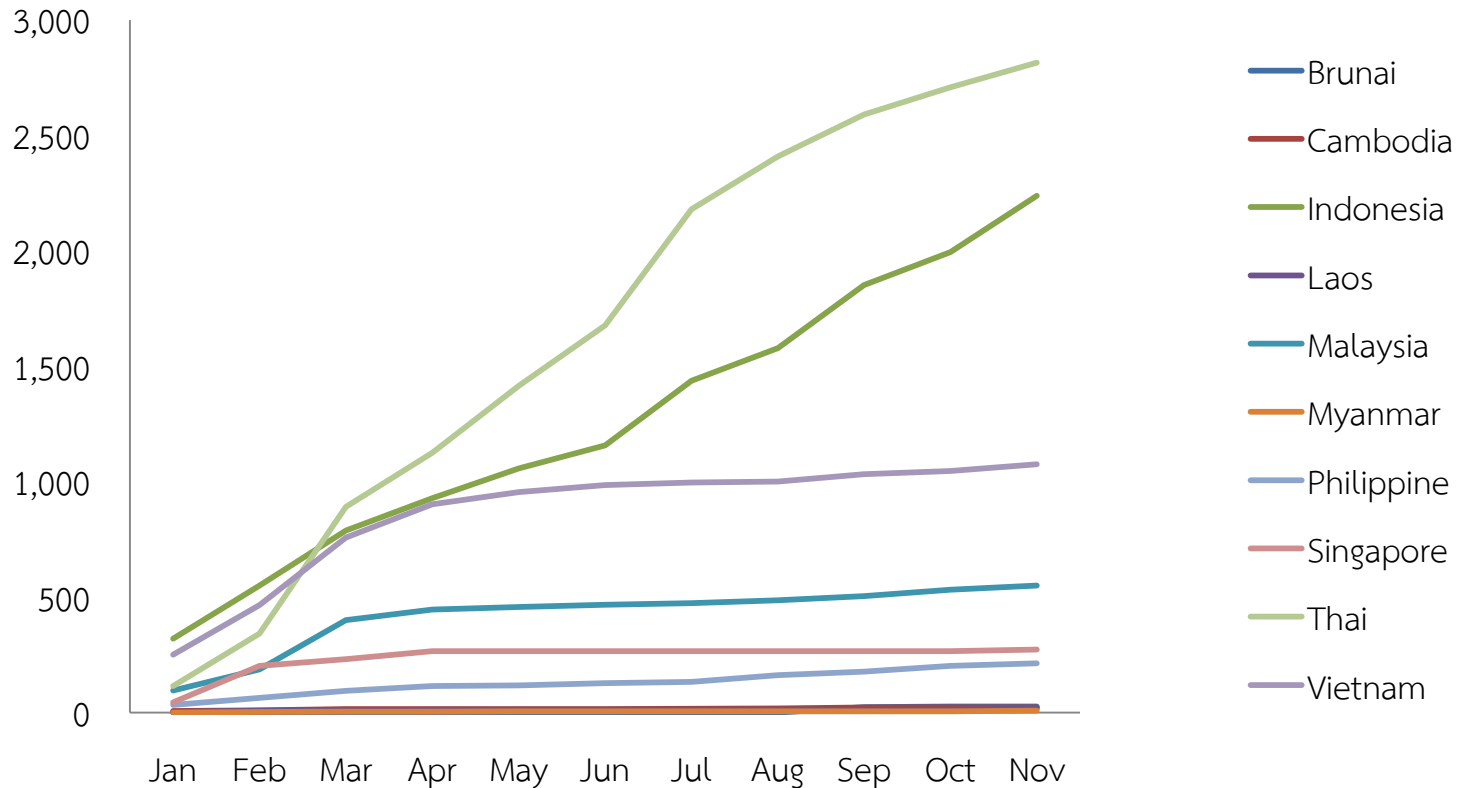
./Hacked Error 7rB

Web Defacements Of Government Websites In ASEAN In 2014



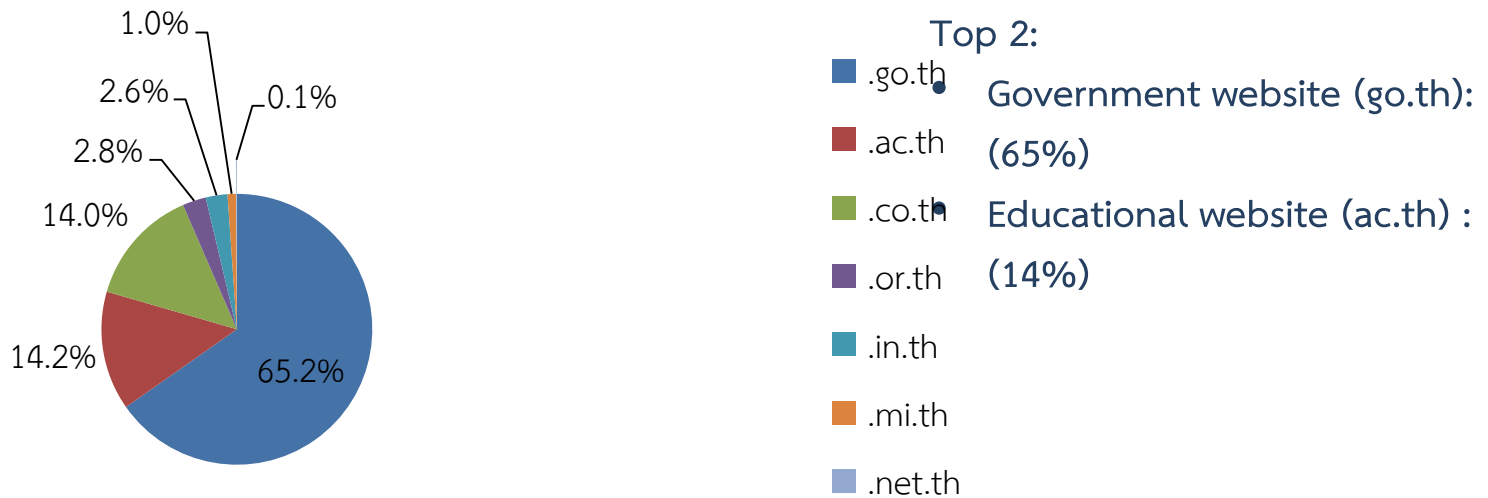
Data source: Zone-H from Jan – Nov 2557

Web Defacements In ASEAN In 2014



Data source: Zone-H from Jan - Nov 2557

Web Defacements In Thailand In 2014



Total number of reports: 1,400

Data source: Zone-H from Jan – Nov 2557

Example ticket

#43662: แจ้งปัญหา พบ x Hacked By Error 7rB x

RT-Send-CC: support@idc.cattellecom.com, abuse@idc.cattellecom.com, narin422@hotmail.com

Reply Comment Forward

Download (untitled) / with headers
text/html 5.9k

เรียน ผู้ดูแลระบบและผู้เกี่ยวข้อง

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ได้รับข้อมูลจากหน่วยงานภายในเครือข่ายของไทยเซิร์ต โดยมีเนื้อหาแจ้งว่าเว็บไซต์ภายในเครือข่ายของท่าน มีหน้าเว็บไซต์ที่ผิดปกติ ซึ่งอาจเกิดจากการถูกบุกรุกและเข้าถึงส่วนควบคุมเว็บไซต์จากผู้ไม่ประสงค์ดี โดยรายละเอียดดังกล่าวสามารถตรวจสอบได้จากข้อมูลดังต่อไปนี้

เวลาที่ตรวจสอบล่าสุด 9 มกราคม 2558 เวลา 16:15 น. อ้างอิงเวลาสากลเชิงพิกัดของประเทศไทย (UTC+7)
โดเมน / หมายเลขไอพี: [redacted]an.go.th / 122.155.10.196
URL ที่ได้รับรายงาน: hxxp://[redacted]n.go.th/index.php
เว็บไซต์อ้างอิง: http://www.zone-h.org/mirror/id/23513[redacted]

การดำเนินการ (เร่งด่วน)

- 1.ให้ตัดการเชื่อมต่อของเว็บไซต์นี้กับเครือข่ายอินเทอร์เน็ตในทันที และให้เจ้าหน้าที่ทางเทคนิคตรวจสอบ Log ต่างๆในระบบเพื่อหาช่องทางที่ระบบถูกปรับปรุงแก้ไขโดยไม่ได้รับอนุญาต
2. ในกรณีที่ต้องการความช่วยเหลือในการวิเคราะห์ปัญหาที่เกิดขึ้น ให้เก็บรวบรวมโปรแกรมหรือ Source code ฐานข้อมูลเว็บไซต์และข้อมูล Log ของบริการต่างๆ ที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลในการพิจารณาการโจมตี และการป้องกันการโจมตีในอนาคต

คำแนะนำเพิ่มเติม

- 1.ควรตรวจสอบรายการช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์ที่ใช้งาน กับแหล่งข้อมูลที่นำเชื่อถือ เช่น เว็บไซต์ผู้พัฒนาซอฟต์แวร์นั้นๆ เว็บไซต์ฐานข้อมูลช่องโหว่ CVE (Common Vulnerabilities and Exposures) และดำเนินการพิจารณาปรับปรุงซอฟต์แวร์ตามคำแนะนำเพื่อป้องกันการถูกโจมตี
- 2.ควรเปิดใช้งานบริการ (Services/Ports) ที่จำเป็นเท่านั้น เพื่อลดช่องทางการโจมตี เช่น การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
- 3.ควรดำเนินการตรวจสอบ Log ของบริการต่างๆที่เกี่ยวข้อง เพื่อตรวจสอบความผิดปกติของการใช้งาน เช่น มีความพยายามในการโจมตีช่องโหว่บนเว็บไซต์ใดๆหรือไม่
- 4.สามารถศึกษาแนวทางการพัฒนาเว็บไซต์อย่างมั่นคงปลอดภัยตามเอกสาร Website Security Standard (<http://thcert.co/9rX5PX>)

ทีมงานหวังเป็นอย่างยิ่งว่าจะได้รับความร่วมมือจากท่านในการดำเนินการเพื่อแก้ไขภัยคุกคามนี้ และหากมีความคืบหน้าประการใดเกี่ยวกับเหตุการณ์นี้ กรุณาแจ้งกลับมายังไทยเซิร์ต โดยระบุรหัสหมายเลข [THAICERT.OR.TH #43662] เพื่ออ้างอิงถึงเรื่องการแจ้งเหตุนี้ในชื่ออีเมลหรือหัวข้อ อีเมล(Subject) ที่ใช้ในการติดต่อกับไทยเซิร์ต

ขอแสดงความนับถือ
ไทยเซิร์ต

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) บริหารจัดการและดำเนินการโดย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์(องค์การมหาชน)

<https://www.thaicert.or.th>

ThaiCERT Point-of-Contact

Please register your official contact details with us, so we can contact you when we need to report an incident to your company.

- Our contact details if you wish to report an incident to us or need help:
- email: report@thaicert.or.th
- telephone: 0 2123 1212