CLASSIFIED BRIEFING // CYBER DEFENSE


# กลุ่มแฮกเกอร์ APT ที่สำคัญ

## Understanding State-Sponsored Cyber Threats

ภัยคุกคามความมั่นคงไซเบอร์ระดับชาติ

# วัตถุประสงค์การบรรยาย

เข้าใจวิวัฒนาการและโครงสร้างของกลุ่ม
APT (Advanced Persistent Threat)

แยกแยะความแตกต่างระหว่าง
“อาชญากรไซเบอร์ทั่วไป” vs
“หน่วยปฏิบัติการระดับรัฐ”

เจาะลึก TTPs (Tactics, Techniques,
and Procedures) ที่ใช้ในการโจมตีจริง

ถอดบทเรียนจากกรณีศึกษาระดับโลก
(SolarWinds, Stuxnet)
เพื่อประยุกต์ใช้ในการป้องกัน

Strategic Intelligence Dark Mode

# APT: กองกำลังพิเศษทางไซเบอร์ (Cyber Special Forces)

## Advanced

ใช้เครื่องมือระดับสูง (Sophisticated Tools) และช่องโหว่ Zero-day ที่ปรับแต่งเฉพาะเจาะจง ไม่ใช่ Malware ทั่วไป

## Persistent

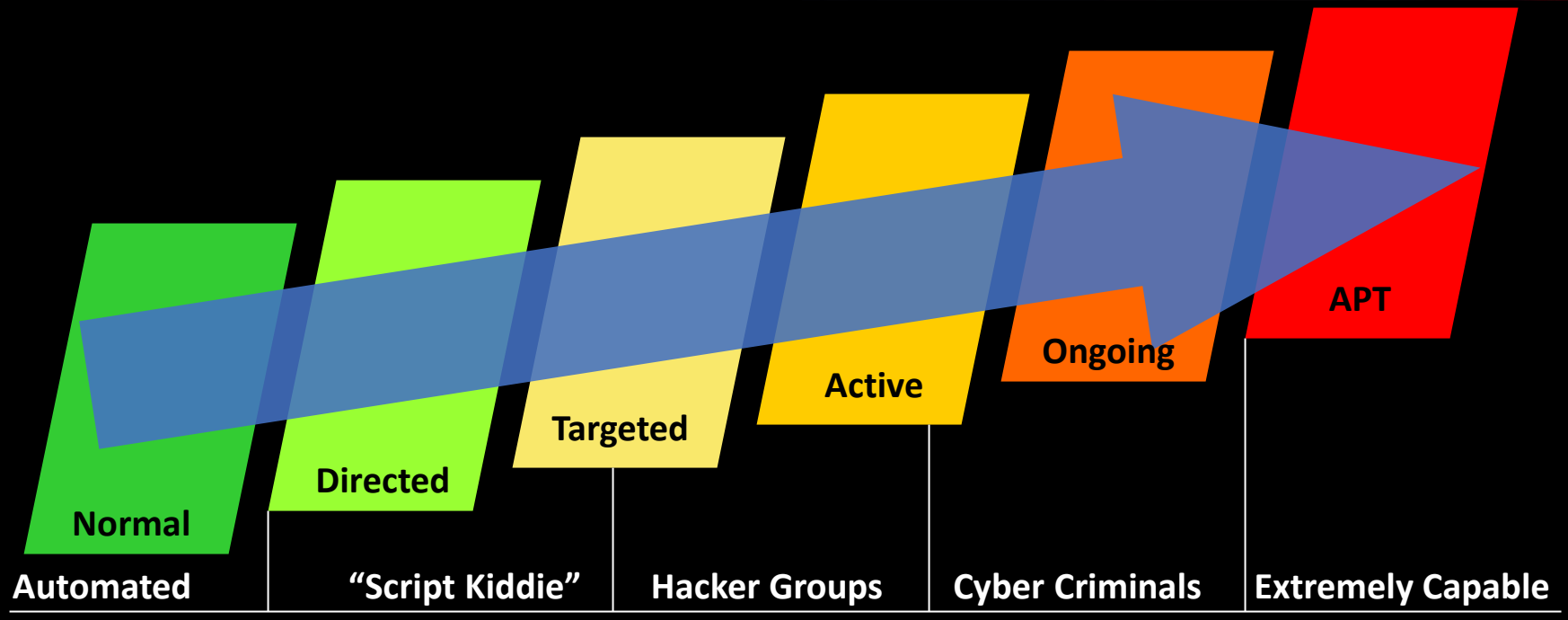
ภารกิจเน้นการ "ฝังตัว" ระยะยาว (Long-term Dwell Time) เป็นเดือนหรือปี เพื่อดึงข้อมูลอย่างต่อเนื่อง

## Threat

มีรัฐบาลหนุนหลัง (State-Sponsored) ทั้งงบประมาณ บุคลากร และหน่วยข่าวกรอง

"APT ไม่ใช่แฮกเกอร์ทั่วไป แต่คือหน่วยปฏิบัติการที่ทำสงครามนอกเขต (Grey Zone Warfare)"

# ระดับชั้นของภัยคุกคามทางไซเบอร์



Strategic Intelligence Dark Mode

# ความแตกต่างระหว่างอาชญากรไซเบอร์และหน่วยปฏิบัติการรัฐ

## Cyber Criminals
### อาชญากรไซเบอร์

- แรงจูงใจ: ผลประโยชน์ทางการเงิน (Financial Gain)
- เป้าหมาย: เหยื่อที่อ่อนแอ (Opportunistic)
- ระยะเวลา: โจมตีเร็ว จบเร็ว

## Nation-State APTs
### หน่วยปฏิบัติการรัฐ

- แรงจูงใจ: ความมั่นคง, การเมือง, และภูมิรัฐศาสตร์
- เป้าหมาย: โครงสร้างพื้นฐาน, ความลับทางทหาร, ข้อมูลพลเมือง
- ระยะเวลา: แฝงตัวนานและอดทน (Persistence)

Criminals want your money. APTs want your future.

# จุดกำเนิดของคำว่า 'APT'

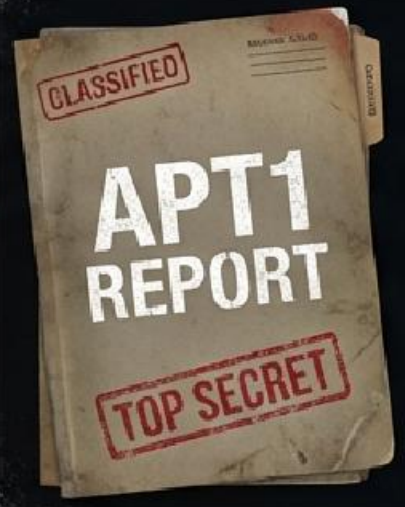
declassified file card

**ผู้ให้กำเนิด:**
กองทัพอากาศสหรัฐฯ (US Air Force)
**บุคคล:** พันเอก Greg Rattray
**วัตถุประสงค์:**
ใช้เรียกภัยคุกคามที่ซับซ้อนกว่าไวรัสทั่วไป และต้องอาศัยความร่วมมือภาคอุตสาหกรรมป้องกันประเทศ

## 2006: The Originator

## 2010: Operation Aurora

declassified file card




**เหตุการณ์:**
รายงาน APT1 จากบริษัท Mandiant
**ความสำคัญ:**
ครั้งแรกที่โลกได้รับรู้ถึง 'Unit 61398' หน่วยงานแฮกเกอร์ของกองทัพจีนอย่างเป็นทางการ

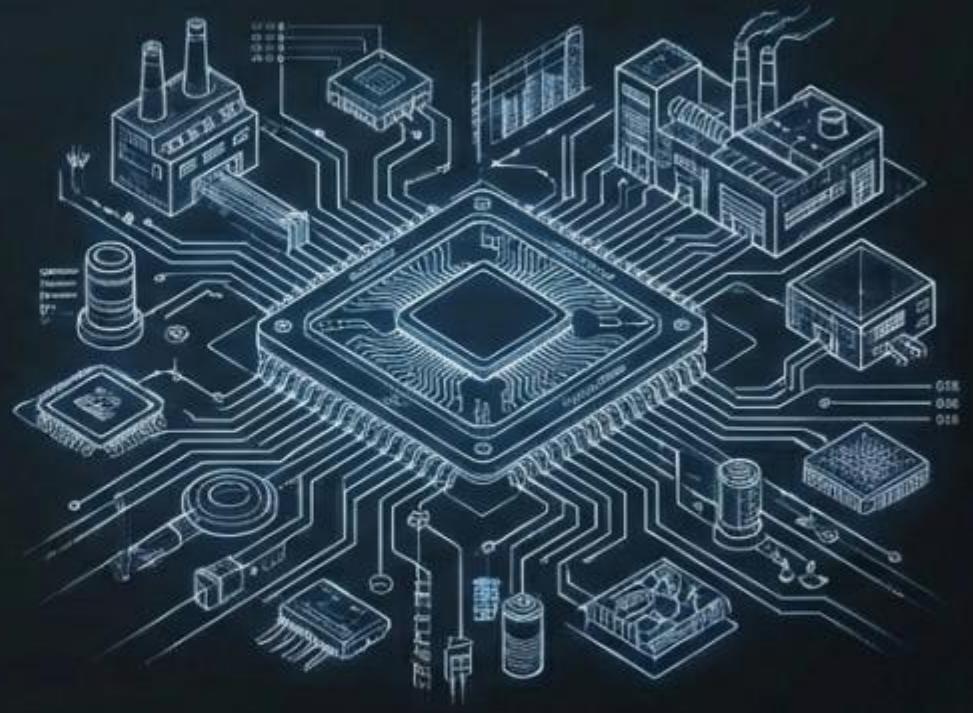
## 2013: The Revelation


Strategic Intelligence Dark Mode
มหาอำนาจในสงครามไซเบอร์ [redacted]
Russia: สงครามข้อมูล (Disinformation), แทรกแซงการเมือง, และการทำลายล้างระบบสาธารณูปโภค
China: จารกรรมทรัพย์สินทางปัญญาและเทคโนโลยี เพื่อการก้าวกระโดดทางเศรษฐกิจ (Belt and Road Initiative)
North Korea: อาชญากรรมไซเบอร์เพื่อหาเงิน (Crypto/SWIFT) ระดมทุนให้รัฐบาลและโครงการนิวเคลียร์
Iran: การสอดแนมภูมิภาค, จารกรรมข้อมูลพลังงาน, และการตอบโต้ทางภูมิรัฐศาสตร์
SYSTEM STATUS: CRITICAL
LAT/LONG: TARGET ACQUIRED

# สาธารณรัฐประชาชนจีน (PRC): จารกรรมเพื่อความมั่งคั่ง

## Key Groups

- **APT41 (Double Dragon):** กลุ่มที่มีความซับซ้อนสูง ทำทั้งจารกรรมรัฐและอาชญากรรมเพื่อกำไร
- **Mustang Panda:** มุ่งเน้นการโจมตีหน่วยงานทูตและองค์กร NGO
- **APT1 (Unit 61398):** หน่วยงานกองทัพที่มุ่งเป้าข้อมูลโครงสร้างพื้นฐานและเทคโนโลยี



## Strategy

Supply Chain Attacks และการเจาะระบบผ่าน Software Vendor ที่องค์กรเชื่อถือ

# รัสเซีย (Russian Federation): สงครามไฮบริดและการทำลายล้าง

## Key Groups

- **APT28 (Fancy Bear)**: สังกัดหน่วย GRU เน้นแทรกแซงการเลือกตั้งและเจาะระบบ NATO
- **Sandworm**: หน่วยสงครามไซเบอร์ ผู้เชี่ยวชาญด้านการทำลายระบบควบคุมอุตสาหกรรม (ICS/SCADA)

## Tactics

ใช้มัลแวร์ทำลายข้อมูล (Wiper) และโจมตีระบบไฟฟ้าเพื่อสร้างความโกลาหลทางกายภาพ

# ภัยคุกคามจากรัฐอันธพาล (Rogue States Threats)

## North Korea (DPRK): การหารายได้ (Revenue Generation)

**Lazarus Group:** ปฏิบัติการปล้นธนาคารโลก (Bangladesh Bank Heist) และขโมย Cryptocurrency

**Insight:** ใช้ไซเบอร์เป็นแหล่งรายได้หลักของประเทศ

## Iran (IRI): การล้างแค้น (Retaliation)

**APT33 / OilRig:** มุ่งเป้าอุตสาหกรรมน้ำมัน, การบิน, และพลังงาน

**Insight:** การสอดแนมฝ่ายตรงข้ามในตะวันออกกลาง

# ตารางสรุปขีดความสามารถ (Capability Matrix)

| ประเทศ (Country) | แรงจูงใจหลัก (Motivation) | เป้าหมายหลัก (Targets) |
|---|---|---|
| China | ทรัพย์สินทางปัญญา | Technology, Defense |
| Russia | การเมือง/ทำลายล้าง | Government, Grid, NATO |
| N. Korea | เงิน/คริปโต | Banks, Crypto Exchanges |
| Iran | การตอบโต้/ภูมิภาค | Energy, Oil & Gas |

# วงจรการโจมตี (The Cyber Kill Chain)

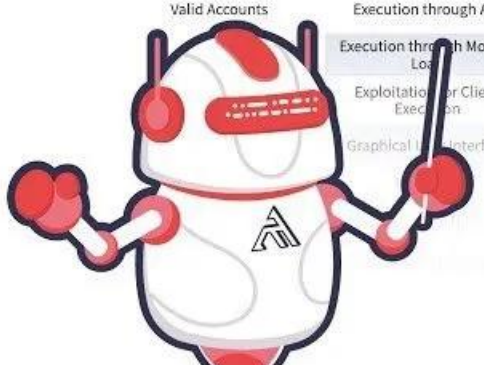
Cyber-Intelligence Briefing

# The MITRE ATT&CK Framework

**Tactics** →

**Techniques** ↓

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration |
|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | PowerShell | .bash_profile and .bashrc | Process Injection | Process Injection | Account Manipulation | Account Discovery | Windows Admin Shares | Audio Capture | Web Service | Automated Exfiltration |
| Exploit Public-Facing Application | Scheduled Task | Accessibility Features | Access Token Manipulation | Access Token Manipulation | Bash History | Application Window Discovery | AppleScript | Automated Collection | Commonly Used Port | Data Compressed |
| External Remote Services | Windows Management Instrumentation | Account Manipulation | Accessibility Features | Application Access Token | Brute Force | Browser Bookmark Discovery | Application Access Token | Clipboard Data | Communication Through Removable Media | Data Encrypted |
| Hardware Additions | AppleScript | AppCert DLLs | AppCert DLLs | Binary Padding | Cloud Instance Metadata API | Cloud Service Dashboard | Application Deployment Software | Data from Cloud Storage Object | Connection Proxy | Data Transfer Size Limits |
| Replication Through Removable Media | CMSTP | AppInit DLLs | AppInit DLLs | BITS Jobs | Credential Dumping | Cloud Service Discovery | Component Object Model and Distributed COM | Data from Information Repositories | Custom Command and Control Protocol | Exfiltration Over Alternative Protocol |
| Spearphishing Attachment | Command-Line Interface | Application Shimming | Application Shimming | Bypass User Account Control | Credentials from Web Browsers | Domain Trust Discovery | Exploitation of Remote Services | Data from Local System | Custom Cryptographic Protocol | Exfiltration Over Command and Control Channel |
| Spearphishing Link | Compiled HTML File | Authentication Package | Bypass User Account Control | Clear Command History | Credentials in Files | File and Directory Discovery | Internal Spearphishing | Data from Network Shared Drive | Data Encoding | Exfiltration Over Other Network Medium |
| Spearphishing via Service | Component Object Model and Distributed COM | BITS Jobs | DLL Search Order Hijacking | CMSTP | Credentials in Registry | Network Service Scanning | Logon Scripts | Data from Removable Media | Data Obfuscation | Exfiltration Over Physical Medium |
| Supply Chain Compromise | Control Panel Items | Bootkit | Dylib Hijacking | Code Signing | Exploitation for Credential Access | Network Share Discovery | Pass the Hash | Data Staged | Domain Fronting | Scheduled Transfer |
| Trusted Relationship | Dynamic Data Exchange | Browser Extensions | Elevated Execution with Prompt | Compile After Delivery | Forced Authentication | Network Sniffing | Pass the Ticket | Email Collection | Domain Generation Algorithms | Transfer Data to Cloud Account |
| Valid Accounts | Execution through API | Change Default File Association | Emond | Compiled HTML File | Hooking | Password Policy Discovery | Remote Desktop Protocol | Input Capture | Fallback Channels | |
| | Execution through Module Load | Component Firmware | Exploitation for Privilege Escalation | Component Firmware | Input Capture | Peripheral Device Discovery | Remote File Copy | Man in the Browser | Multi-hop Proxy | |
| | Exploitation for Client Execution | Component Object Model Hijacking | Extra Window Memory Injection | Component Object Model Hijacking | Input Prompt | Permission Groups Discovery | Remote Services | Screen Capture | Multi-Stage Channels | |
| | Graphical User Interface | Create Account | File System Permissions Weakness | Connection Proxy | Kerberoasting | Process Discovery | Replication Through Removable Media | Video Capture | Multiband Communication | |
| | | DLL Search Order Hijacking | Hooking | Control Panel Items | Keychain | Query Registry | Shared Webroot | | Multilayer Encryption | |
| | | Hidden Files and Directories | Image File Execution Options Injection | DCShadow | LLMNR/NBT-NS Poisoning and Relay | Remote System Discovery | SSH Hijacking | | Port Knocking | |



GROUPS

APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
APT41
APT42
APT5

# Associated Group Descriptions

| Name | Description |
|---|---|
| Comment Crew | [1] |
| Comment Group | [1] |
| Comment Panda | [2] |

# Techniques Used

ATT&CK® Navigator Layers

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1087 | .001 | Account Discovery: Local Account | APT1 used the commands `net localgroup`, `net user`, and `net group` to find accounts on the system.[1] |
| Enterprise | T1583 | .001 | Acquire Infrastructure: Domains | APT1 has registered hundreds of domains for use in operations.[1] |
| Enterprise | T1560 | .001 | Archive Collected Data: Archive via Utility | APT1 has used RAR to compress files before moving them outside of the victim network.[1] |
| Enterprise | T1119 | | Automated Collection | APT1 used a batch script to perform a series of discovery techniques and saves it to a text file.[1] |
| Enterprise | T1059 | .003 | Command and Scripting Interpreter: Windows Command Shell | APT1 has used the Windows command shell to execute commands, and batch scripting to automate execution.[1] |

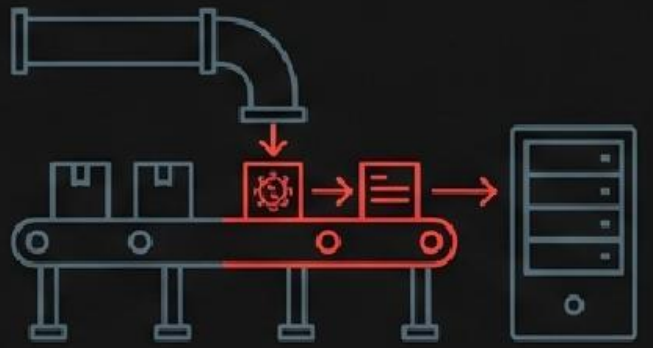
# ประตูบานแรก: พวกเขาเข้ามาได้อย่างไร? (Initial Access)

**Spear-Phishing**

อีเมลหลอกลวงที่แนบเนียนสูง เจาะจงตัวบุคคล (เช่น ปลอมเป็นคู่ค้า หรือ HR)

**Watering Hole**

การฝังมัลแวร์ในเว็บไซต์ที่เหยื่อเข้าใช้งานบ่อย



**Supply Chain Attack**

การโจมตีผ่านซอฟต์แวร์หรือ Vendor ที่องค์กรเชื่อถือ (ตรวจจับยากที่สุด)

# เทคนิคการพรางตัวและการฝังตัว (Evasion & Persistence)


**200+ Days**

Average Dwell Time
(ระยะเวลาแฝงตัวก่อนถูกตรวจพบ)

## Techniques

- **Living off the Land (LotL):** การใช้เครื่องมือที่มีอยู่แล้วในเครื่อง เช่น **Power Shell** เพื่อหลบเลี่ยงการตรวจจับ
- **Fileless Malware:** มัลแวร์ที่ทำงานในหน่วยความจำ (RAM) ไม่ทิ้งไฟล์ให้ตรวจสอบ
- **Lateral Movement:** การเคลื่อนที่ไปยึดเครื่องอื่นในเครือข่ายอย่างเงียบ

# Case Study 1 – SolarWinds: The Supply Chain Masterpiece

ผู้ก่อเหตุ: รัสเซีย
(APT29)

ฝัง Backdoor (Sunburst)
ลงในตัวอัปเดต Orion

เหยื่อดาวน์โหลดไปติดตั้ง
(18,000+ องค์กร)

**บทเรียน: องค์กรอาจปลอดภัย แต่ Vendor ของคุณอาจจะไม่**

ปี 2020

# Case Study 2 - Microsoft Exchange (Hafnium): The Zero-Day Blitz

- ผู้ก่อเหตุ: **จีน** (Hafnium)
- วิธีการ: ใช้ช่องโหว่ Zero-day 4 **จุด** ใน Exchange Server
- ลักษณะเด่น: ปฏิบัติการด้วยความเร็วสูง (Blitz) สแกนเหยื่อทั่วโลกแบบปูพรมก่อนที่ Patch จะออก

MASS SCANNING DETECTED

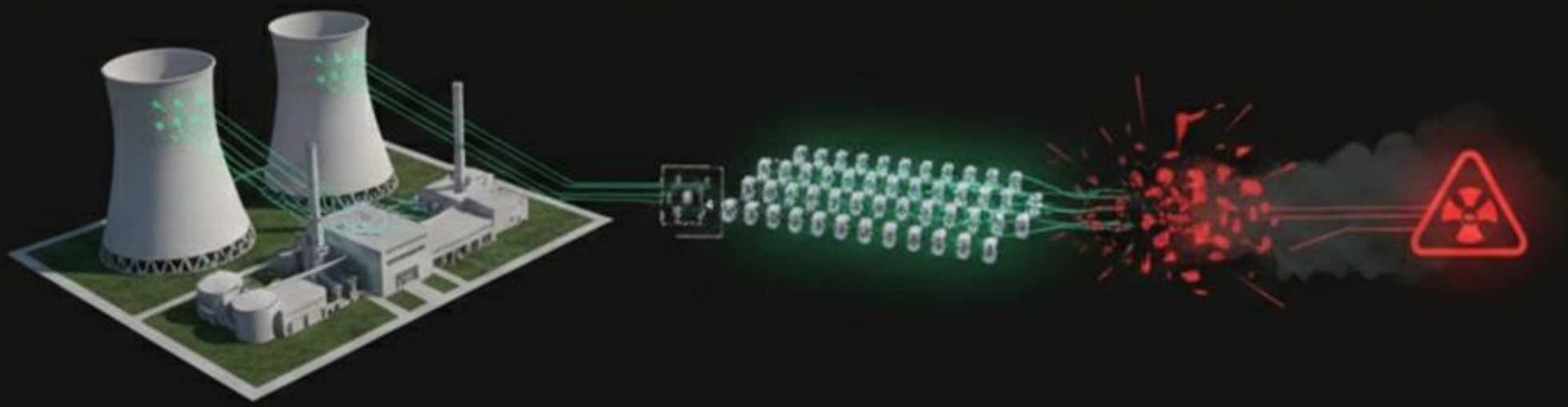
ปี 2021

# Case Study 3 – Ukraine Power Grid: The Kinetic Impact

- ผู้ก่อเหตุ: **รัสเซีย** (Sandworm) หรือ **APT**44
- เหตุการณ์: เจาะระบบ SCADA ตัดไฟประชาชนกว่า 2 แสนคน
- ความสำคัญ: การโจมตีไซเบอร์ส่งผลต่อโลกกายภาพ (Kinetic Impact)

ปี 2015

# Case Study 4 – Stuxnet: The World's First Cyber Weapon



- **ผู้ก่อเหตุ:** คาดว่าเป็นสหรัฐอเมริกาและอิสราเอล (**Operation Olympic Games**)
- **เหตุการณ์:** การใช้มัลแวร์เจาะระบบ **SCADA** ที่ใช้ควบคุมโรงไฟฟ้าพลังงานนิวเคลียร์อิหร่าน โดยแพร่กระจายผ่าน **USB** เข้าสู่ระบบที่ไม่ได้ต่ออินเทอร์เน็ต
- **ความสำคัญ:** เป็นมัลแวร์ตัวแรกของโลกที่มีเป้าหมายทำลายวัตถุทางกายภาพแบบจงใจ

ปี 2010

# Prompt | ยุทธวิธีป้องกัน: จากตั้งรับ สู่การล่าเชิงรุก (Proactive Defense)

## Cyber Threat Intelligence (CTI)

รู้เขา รู้เรา—ต้องมีข้อมูลข่าวกรอง
เกี่ยวกับกลุ่มผู้โจมตีและ TTPs

## Threat Hunting

ไม่รอสัญญาณเตือนภัย
แต่ค้นหาความผิดปกติใน
เครือข่ายตลอด 24/7

## Identity Security

ใช้ MFA และจำกัดสิทธิ์
(Least Privilege)
ป้องกันการเคลื่อนที่ในวงแลน

## Patch Management

ปิดช่องโหว่ Zero-day
และ 1-day ให้เร็วที่สุด

CLASSIFIED

# บทสรุป: สงครามไซเบอร์ไม่ใช่เรื่องของอนาคต

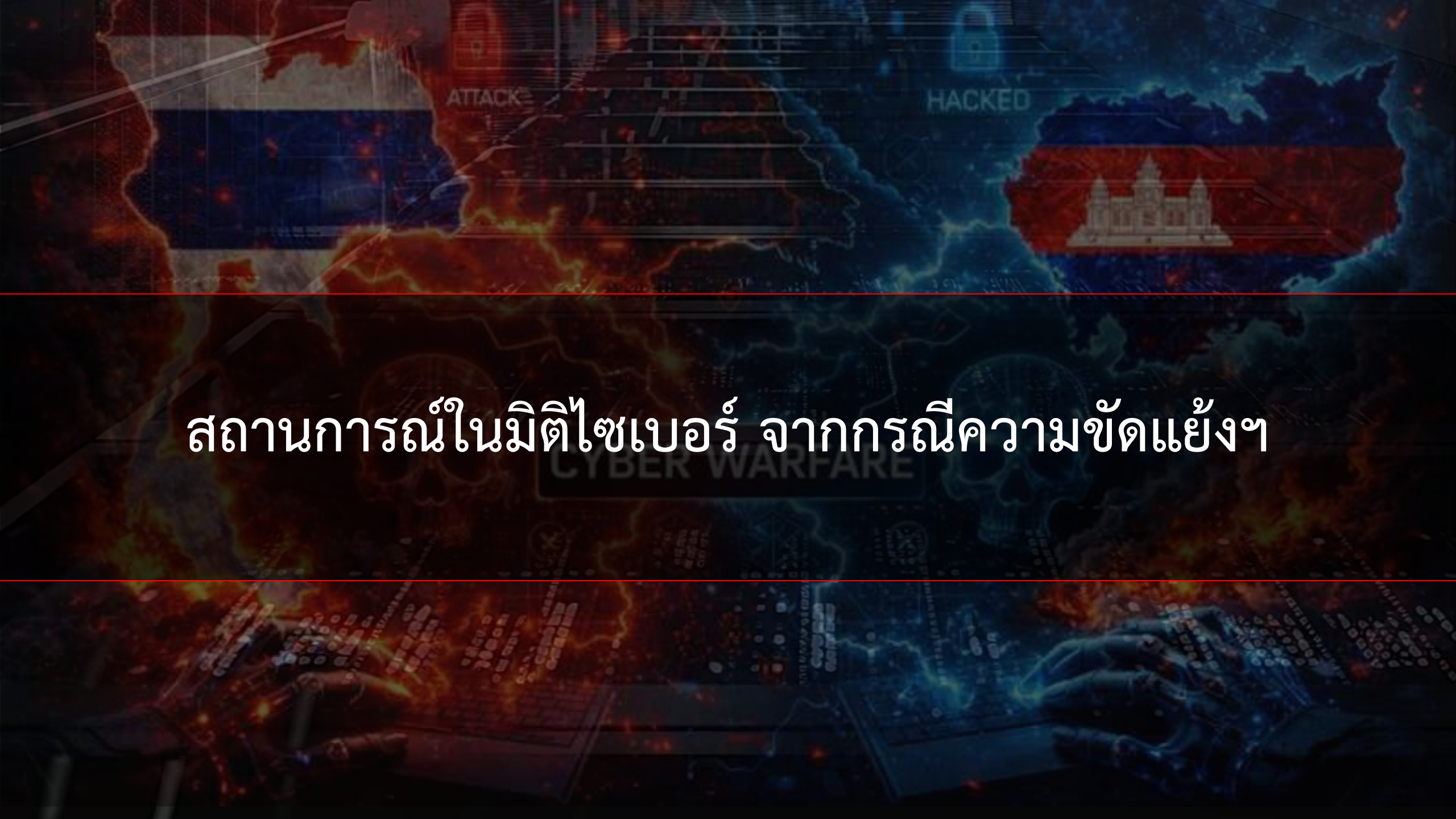
- APT คือกองกำลังพิเศษทางไซเบอร์ที่มีเป้าหมายชัดเจน
- Antivirus เพียงอย่างเดียวไม่สามารถป้องกันได้ ต้องใช้ Intelligence
- ศัตรูอาจอยู่ในเครือข่ายของเราแล้ว...

## คำถามคือ... เรารู้ตัวหรือยัง?_


# สถานการณ์ด้านไซเบอร์
# กรณีพิพาทตามแนวชายแดน

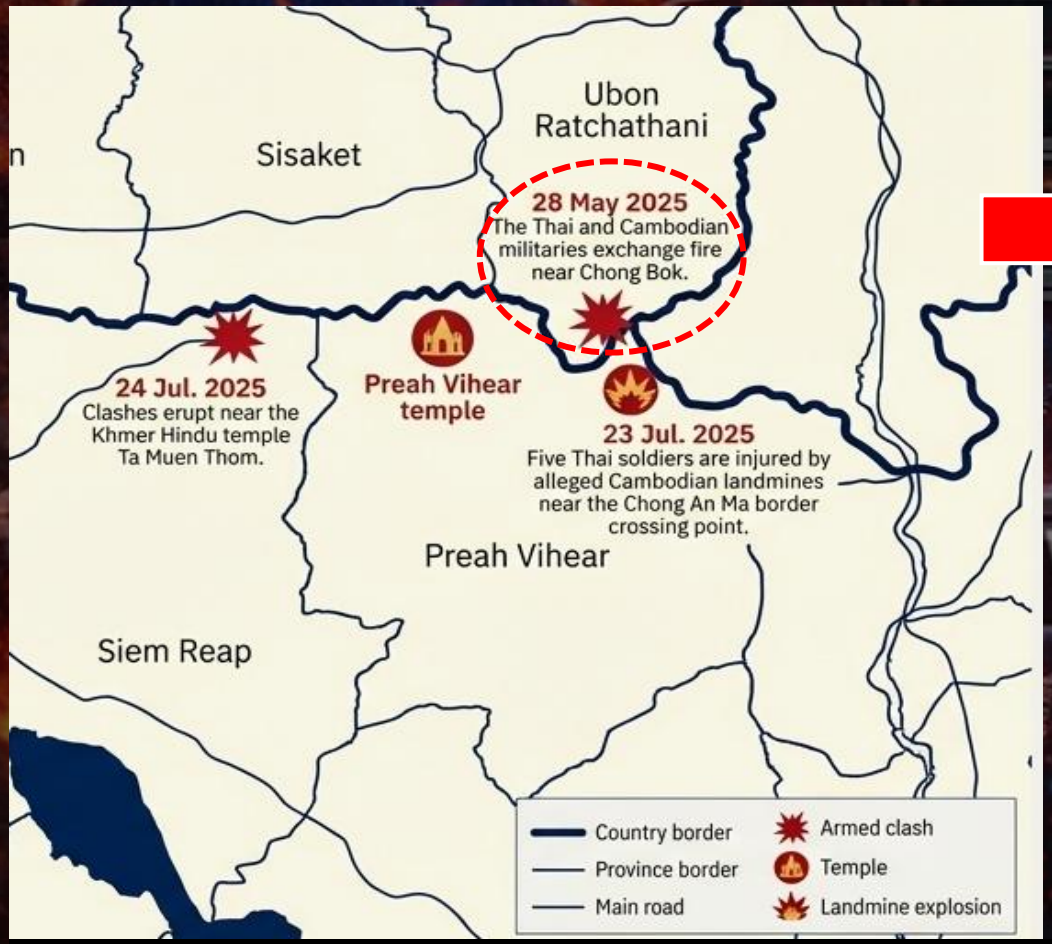
# หัวข้อการบรรยาย

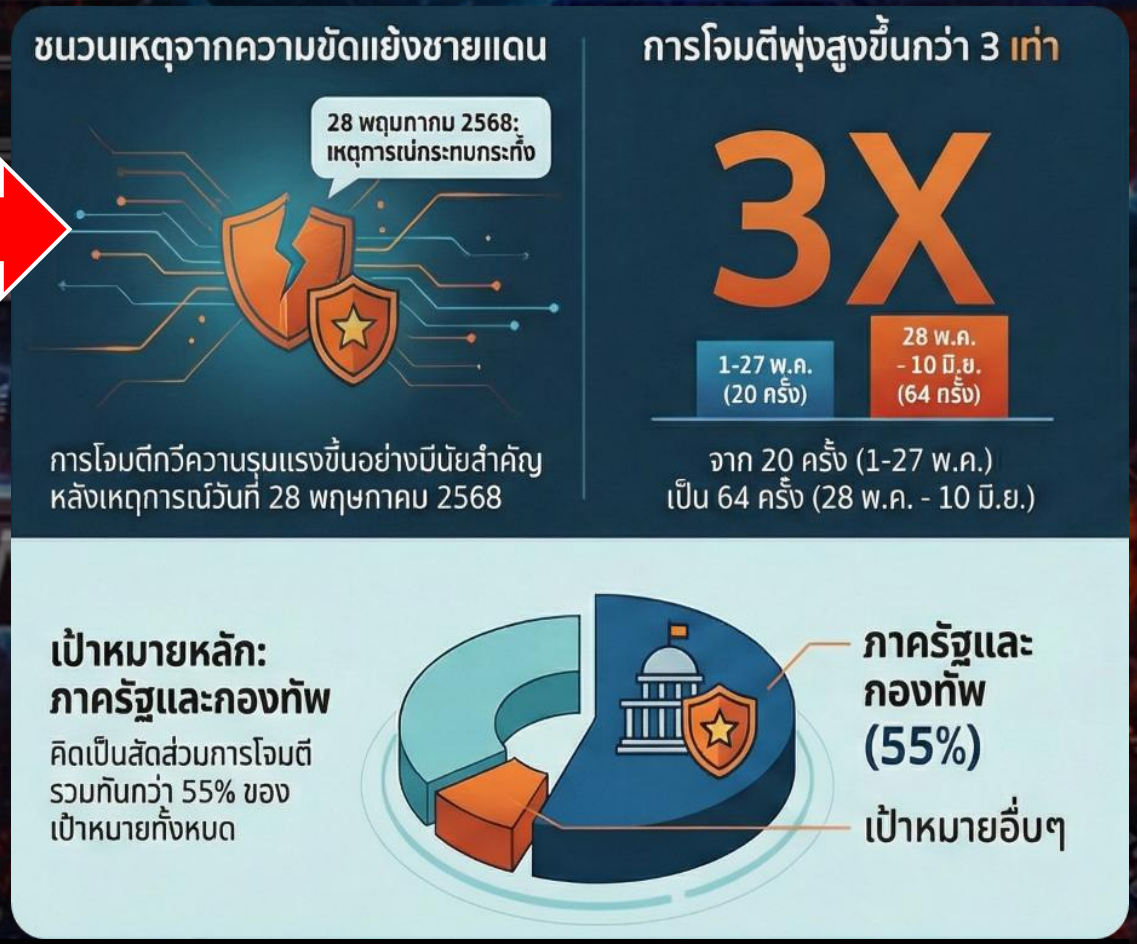
1. ภาพรวมสถานการณ์ในมิติไซเบอร์ จากกรณีความขัดแย้งฯ
2. เหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับกองทัพเรือ
3. การปฏิบัติการไซเบอร์ ที่ผ่านมา
4. การประเมินแนวโน้มสถานการณ์




# สถานการณ์ในมิติไซเบอร์ จากกรณีความขัดแย้งฯ

# จากการปะทะตามแนวชายแดนสู่สงครามไซเบอร์

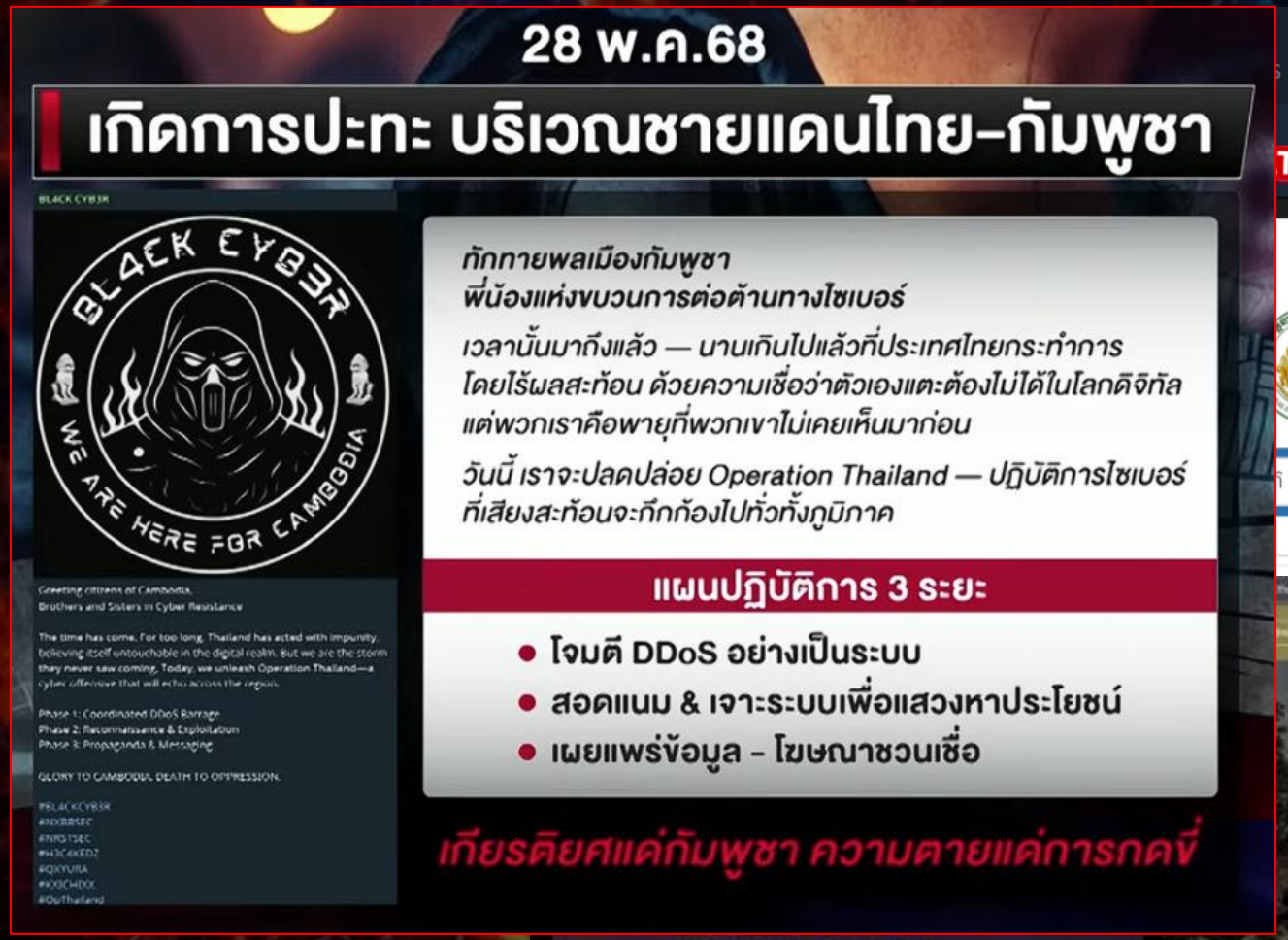


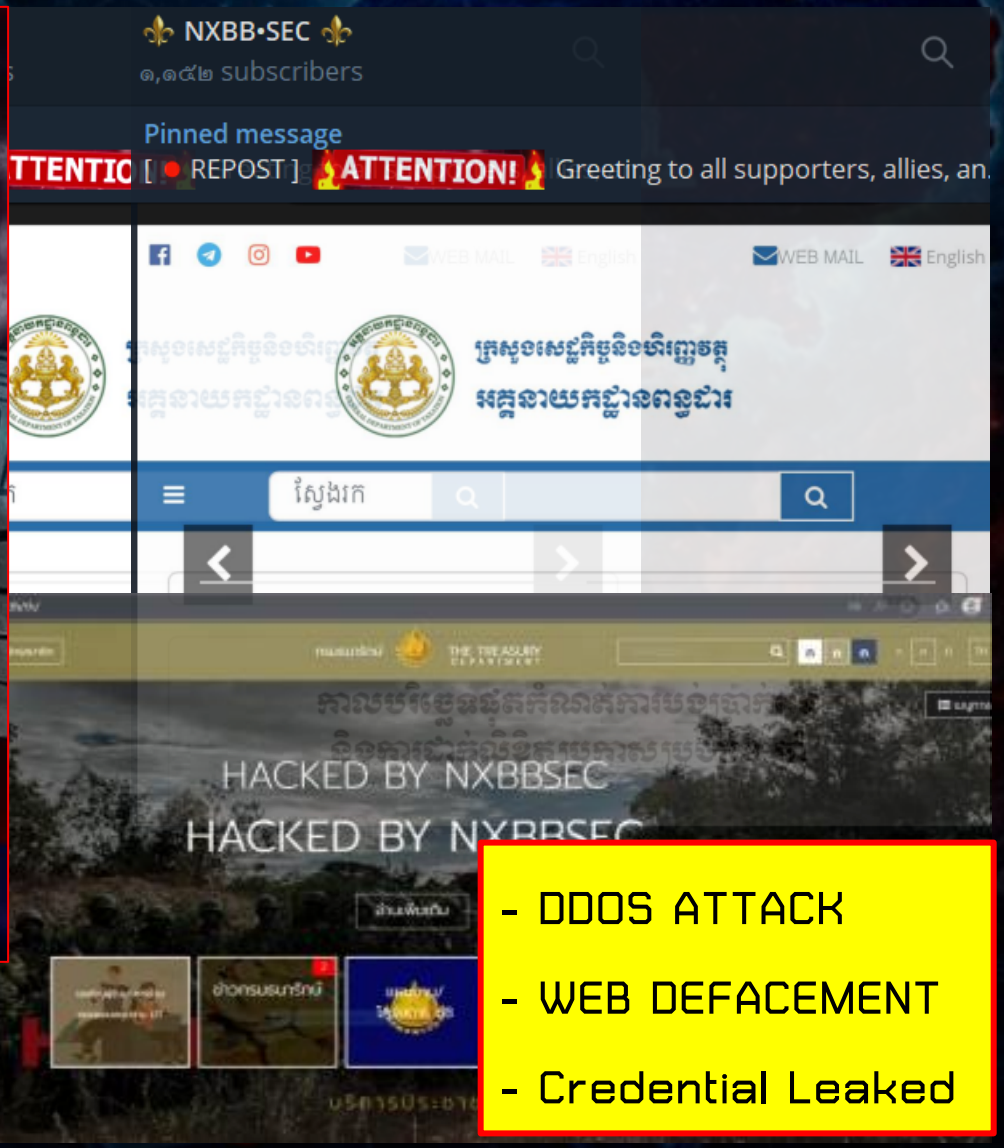




ความขัดแย้ง กรณีปราสาทพระวิหาร และการปะทะเมื่อ 28 พ.ค.68 ได้ลุกลามสู่มิติไซเบอร์

โดยมีแรงจูงใจจาก ลัทธิชาตินิยม และความพยายามใช้ปฏิบัติการไซเบอร์ เพื่อสร้างแรงกดดันทางการเมืองต่อไทย

# สถานการณ์ด้านไซเบอร์ จากกรณีความขัดแย้งตามแนวชายแดน




report/27111b94k77e
https://check-host.net/check-report/27111d9ckfe3

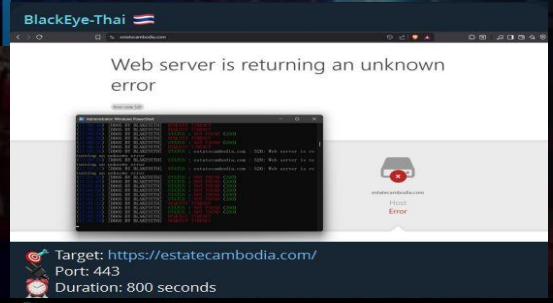
- DDOS ATTACK
- WEB DEFACEMENT
- Credential Leaked

# แจ้งเตือน

## การปฏิบัติการโจมตีทางไซเบอร์ จากกลุ่มแฮกเกอร์ ที่มีต้นทางจากประเทศกัมพูชา

โดยมีเป้าหมายมุ่งโจมตีระบบสารสนเทศของหน่วยงานต่าง ๆ ในประเทศไทย ทั้งภาคราชการ รัฐวิสาหกิจ และภาคเอกชน

ซึ่งอาจส่งผลกระทบต่อความมั่นคงของข้อมูล ความเชื่อมั่นของประชาชน รวมถึงเสถียรภาพในระดับประเทศ



# กลุ่มแฮกเกอร์ และเครือข่ายพันธมิตร

## AnonSecKH / NXBBSEC

กลุ่มหลักและเป็นผู้นำการโจมตี
มี S4ZZ เป็นสมาชิกหลัก
ประกาศตัวเป็นศัตรูของไทยอย่างชัดเจน


Visual Evidence


Visual Evidence

## BL4CK CYB3R

กลุ่มอิสระแต่เป็นพันธมิตรที่
ได้รับความไว้วางใจจาก
AnonSecKH/NXBBSEC
มีส่วนร่วมในการโจมตี DDoS
ต่อเป้าหมายรัฐบาล


Visual Evidence

## กลุ่มพันธมิตร (KOLZSEC, NULLSEC PH)

กลุ่มจากต่างชาติ (ฟิลิปปินส์)
ที่เข้าร่วมปฏิบัติการ #OpThailand
เพื่อสนับสนุนฝ่ายกัมพูชา
มีส่วนในการโจมตีเว็บไซต์กองทัพเรือ

Visual Evidence

# สถานการณ์ด้านไซเบอร์ จากกรณีความขัดแย้งตามแนวชายแดน

## ช่วงที่ 1: ก่อตัวและยกระดับ
(มี.ค. - มิ.ย.)

**มีนาคม: เริ่มต้นปฏิบัติการ**
โจมตีเชิงสัญลักษณ์ที่เว็บไซต์รัฐ
และประกาศจุดยืนผ่านโซเชียลมีเดีย

**พ.ค. – มิ.ย.: ยกระดับความรุนแรง**
เพิ่มความถี่การโจมตี DDoS
และขยายเป้าหมายสู่หน่วยงานทหาร

## ช่วงที่ 2: วิกฤตสูงสุด
(ก.ค. - ส.ค.)


**กรกฎาคม: เปลี่ยนยุทธวิธีสู่การเจาะข้อมูล**
ข้อมูลสำคัญของหน่วยงานรัฐและ Cloud
ถูกเจาะและนำมาเผยแพร่

**สิงหาคม: การโจมตีประสานงานครั้งใหญ่**
เกิดการโจมตี DDoS ขนาดใหญ่มาก
จนนำไปสู่การตั้ง War Room ร่วมมือ

## ช่วงที่ 3: แตกกลุ่มและยืดเยื้อ
(ก.ย. - ม.ค. ปีถัดไป)

**ก.ย. – พ.ย.: แนวร่วมแตกตัว**
เกิดกลุ่มย่อยปฏิบัติการอิสระ
และแรงจูงใจซับซ้อนขึ้น

**ธันวาคม: การปะทะระลอกสอง**
การโจมตีกลับบารุมแรงอีกครั้ง

**มกราคม ปีถัดไป:**
**เข้าสู่ภาวะสงครามระดับต่ำ**
การโจมตีกระจายตัว ไม่ต่อเนื่อง แต่ยังคง
ต้องเฝ้าระวังในระยะยาว

# สถานการณ์ด้านไซเบอร์ จากกรณีความขัดแย้งตามแนวชายแดน

## ธันวาคม 2568: ระลอกการโจมตีช่วงปลายปี

### โจมตีหน่วยงานรัฐและโครงสร้างพื้นฐาน

รัฐสภาไทย

ThaiCERT

ระบบ GIS ของ ปตท.

### รูปแบบการโจมตีหลากหลาย

เจาะระบบ

ขโมยข้อมูล (DITP)

DDoS

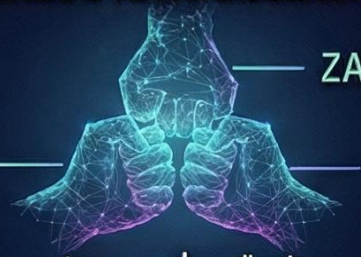
Web Defacement (ns.)

### แฮกเกอร์กัมพูชาเป็นผู้ก่อเหตุหลัก

กลุ่ม H3C4KEDZ
NXBBSEC
rxxhcyber

## มกราคม 2569: ยกระดับปฏิบัติการและสร้างพันธมิตร

### สร้างเครือข่ายพันธมิตรโจมตีไทย



ZAHER INFINITY

Dead killer

DIGIT4_CYB3R

ประกาศร่วมมือกัน

### ขยายเป้าหมายสู่ภาคเอกชนและสื่อ

เว็บไซต์ อย.

บริษัทเอกชน

โรงเรียน

สมาคมผู้ผลิตข่าวออนไลน์

### พัฒนาเครื่องมือสร้างความตื่นตระหนก

กลุ่ม NXBB•SEC เผยแพร่ Fake Ransomware
เพื่อข่มขู่มากกว่าเรียกค่าไถ่จริง

# สถิติภาพรวมการโจมตีทางไซเบอร์ (ประเทศไทย)

## สรุปภาพรวมการโจมตีทางไซเบอร์จากกัมพูชา

ภาพรวมการติดตามความเคลื่อนไหวของกลุ่มแฮกเกอร์กัมพูชาจำนวน 42 กลุ่ม และสถิติการโจมตีทางโซเบอร์ต่อไทยซึ่งมีจำนวนรวมกว่า 1,200 ครั้ง โดยมุ่งเน้นที่ประเภทการโจมตีและกลุ่มผู้ก่อเหตุหลัก

ติดตาม

**42**

**กลุ่มแฮกเกอร์**

คือจำนวนกลุ่มแฮกเกอร์จากกัมพูชาที่ถูกเฝ้าระวังความเคลื่อนไหว


## โจมตีรวม

**1,209** ครั้ง

คือจำนวนการโจมตีทั้งหมดที่ถูกบันทึกไว้ในช่วงเวลาที่รวบรวมข้อมูล

## DDoS คือการโจมตีที่พบบ่อยที่สุด

คิดเป็นจำนวน

**617** ครั้ง

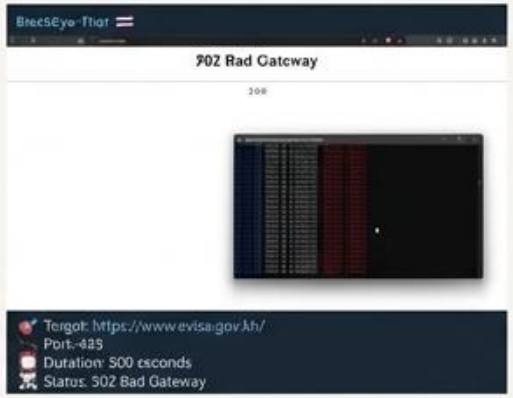
ของการโจมตีทั้งหมด


## 3 กลุ่มที่โจมตีมากที่สุด

# รูปแบบการโจมตี และยุทธวิธีที่ใช้

## DDoS (Denial of Service)

การโจมตีที่พบบ่อยที่สุด
เพื่อทำให้เว็บไซต์ของหน่วย
งานเป้าหมายใช้งานไม่ได้
เป็นการแสดงศักยภาพและ
สร้างผลกระทบเชิงสัญลักษณ์

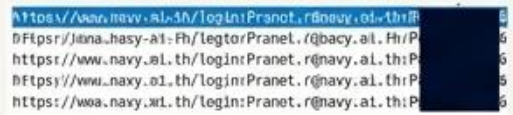



## Defacement

การเปลี่ยนแปลงหน้าเว็บไซต์
เป้าหมายเพื่อประกาศ
ข้อความโฆษณาชวนเชื่อ
หรือแสดงสัญลักษณ์ของกลุ่ม

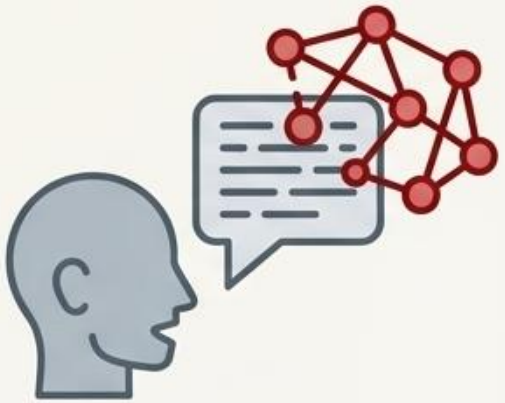

## Data Breaches

การเจาะระบบเพื่อขโมย
ข้อมูลสำคัญ รวมถึงข้อมูล
ส่วนบุคคลและข้อมูล
Credential ของผู้ใช้งาน




## Disinformation

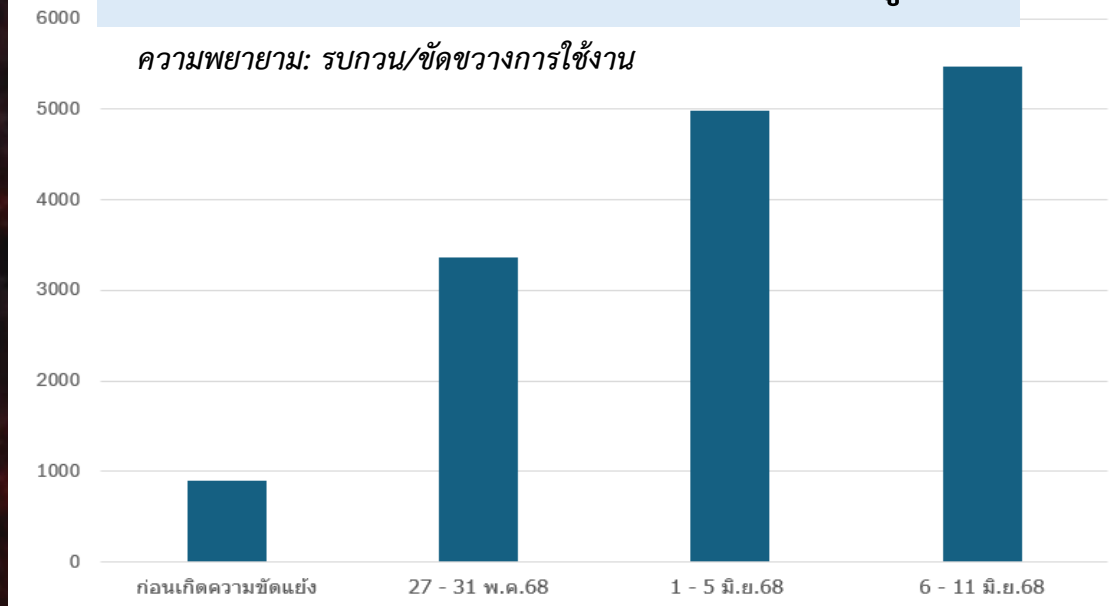
การเผยแพร่ข่าวปลอม
โดยใช้เทคโนโลยี AI
เพื่อสร้างความสับสนและ
บ่อนทำลายความน่าเชื่อถือ
ของฝ่ายไทย




# เหตุการณ์ทางไซเบอร์ ที่เกี่ยวข้องกับกองทัพเรือ

# สถิติการเฝ้าระวังการโจมตีทางไซเบอร์โดย CSOC

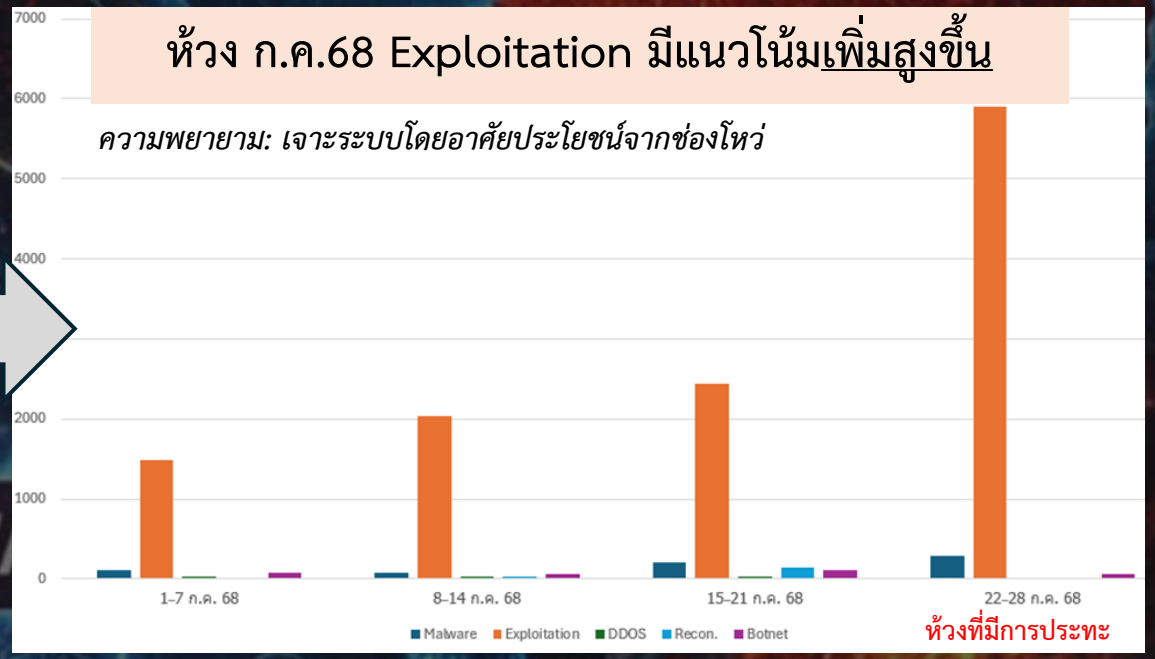
## ห้วง มิ.ย.68 DDoS Attack มีแนวโน้มเพิ่มสูงขึ้น




| | ก่อนเกิดความขัดแย้ง | ๒๗ - ๓๑ พ.ค.๖๘ | ๑ - ๕ มิ.ย.๖๘ | ๖ - ๑๑ มิ.ย.๖๘ |
|---|---|---|---|---|
| DDOS | ๘๙๕ | ๓,๓๕๘ | ๔,๙๘๕ | ๕,๔๖๙ |

ระบบป้องกันการโจมตีทางไซเบอร์
สามารถปิดกั้นและตอบสนองเหตุการณ์ที่เกิดขึ้นได้
- ไม่ส่งผลกระทบต่อระบบสารสนเทศของ ทร.

## ห้วง ก.ค.68 Exploitation มีแนวโน้มเพิ่มสูงขึ้น




| URL | User | Password |
|---|---|---|
| http://proxy.navy.mi.th/ | niwat.sangthong | saraburi |
| http://proxy.navy.mi.th:8080/ | niwat.sangthong | saraburi |
| http://proxy.navy.mi.th/ | somyot.phro | 220109 |
| http://proxy.navy.mi.th:8080/ | somyot.phro | 220109 |
| moz-proxy://proxy.navy.mi.th:8080 | somyot.phro | 220109 |
| http://proxy.navy.mi.th/ | niwat.sangthong | saraburi |
| http://proxy.navy.mi.th:8080/ | niwat.sangthong | saraburi |
| http://proxy.navy.mi.th/ | somyot.phro | 220109 |
| http://proxy.navy.mi.th:8080/ | panyatad.in | 02831835 |
| http://proxy.navy.mi.th/ | kasem.rod | kr2503 |

ตรวจพบข้อมูลบัญชีผู้ใช้งานระบบสารสนเทศ ทร. บนแหล่งข้อมูลต่าง ๆ

# การปรับระดับสถานการณ์ด้านไซเบอร์

เงื่อนไขและสิ่งบอกเหตุ *(** รปจ.ศสซ.ศปก.ทร. ๒๕๖๘ **)*

๑. การตรวจพบข้อมูลที่สำคัญรั่วไหล

๒. ตรวจพบเหตุการณ์ที่ผิดปกติและมีแนวโน้มส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน เกิดขึ้นเป็นจำนวนมาก

๓. ตรวจพบระบบสารสนเทศถูกโจมตี ส่งผลให้ระบบฯ มีประสิทธิภาพการทำงานลดลง และเกิดการรั่วไหลของข้อมูลสำคัญของ ทร.

๔. ตรวจพบสิ่งบ่งชี้ (จากแหล่งข่าวภายนอก) ระบุได้ว่าฝ่ายตรงข้ามมีความเคลื่อนไหว เพื่อปฏิบัติการไซเบอร์เชิงรุกเพิ่มขึ้น

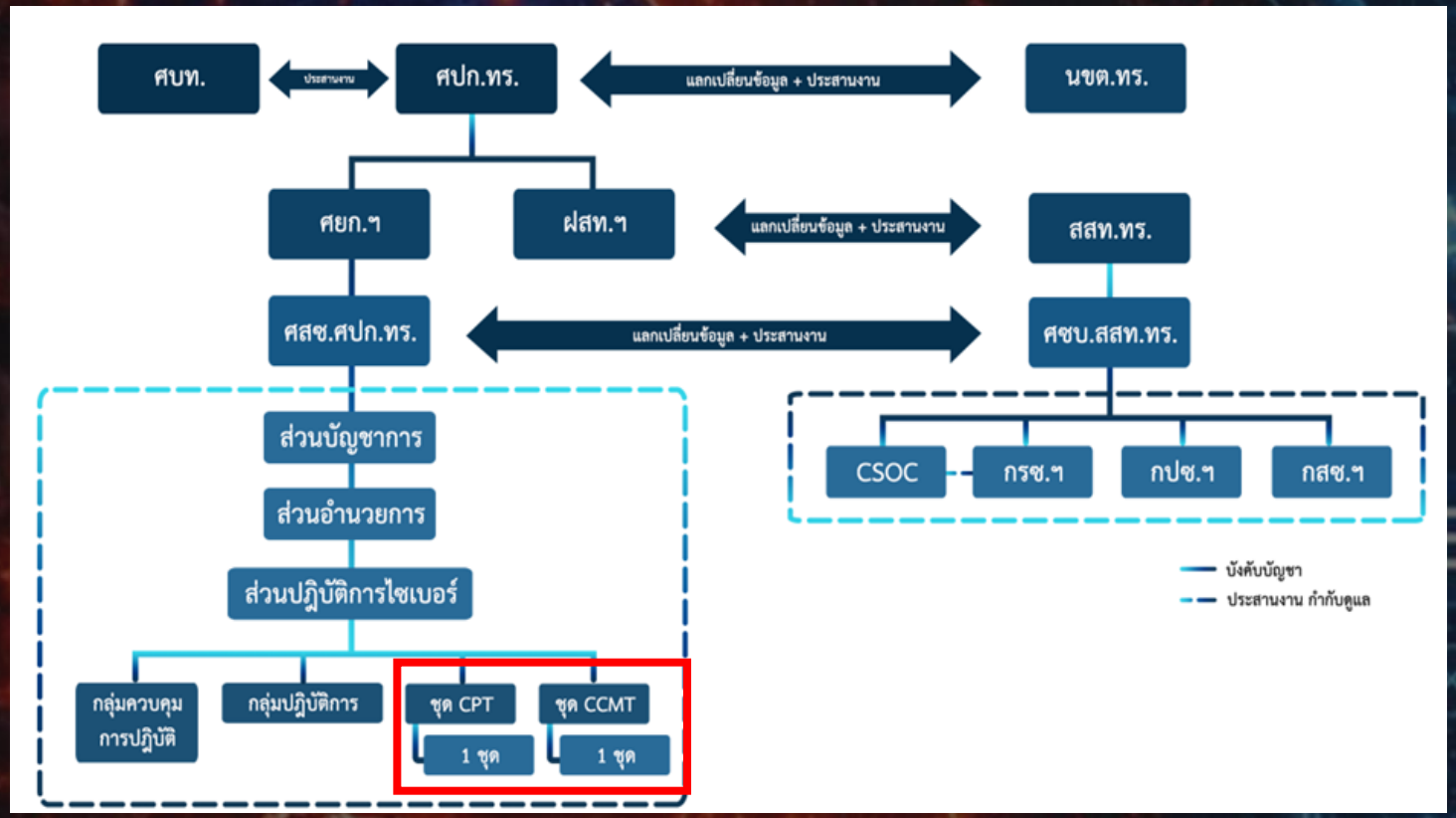
๕. ตรวจพบการโจมตีทางไซเบอร์ ซึ่งส่งผลกระทบต่อการให้บริการระบบสารสนเทศ อยู่ในระดับร้ายแรง

๖. ตรวจพบการลาดตระเวนทางไซเบอร์ ภายในเครือข่ายระบบ C4ISR จากผู้ที่ไม่มีส่วนเกี่ยวข้องเพิ่มขึ้น และมีความเสี่ยงที่จะส่งผลกระทบต่อระบบฯ

๗. มีการปรับระดับตามที่หน่วยเหนือสั่งการ

ตรวจสอบพบโจมตีต่อระบบเครือข่ายสารสนเทศของ ทร. แนวโน้มสูงขึ้น ทำให้ประสิทธิภาพการให้บริการลดลง และอาจส่งผลกระทบต่อภารกิจ ซึ่งจำเป็นต้องปรับระดับสถานการณ์ฯ เพื่อให้ ทร. มีความพร้อมในการรับมือเหตุการณ์ทางไซเบอร์ รองรับสถานการณ์ดังกล่าว

# การปรับระดับสถานการณ์ด้านไซเบอร์




**Cyber Protection Team : CPT**

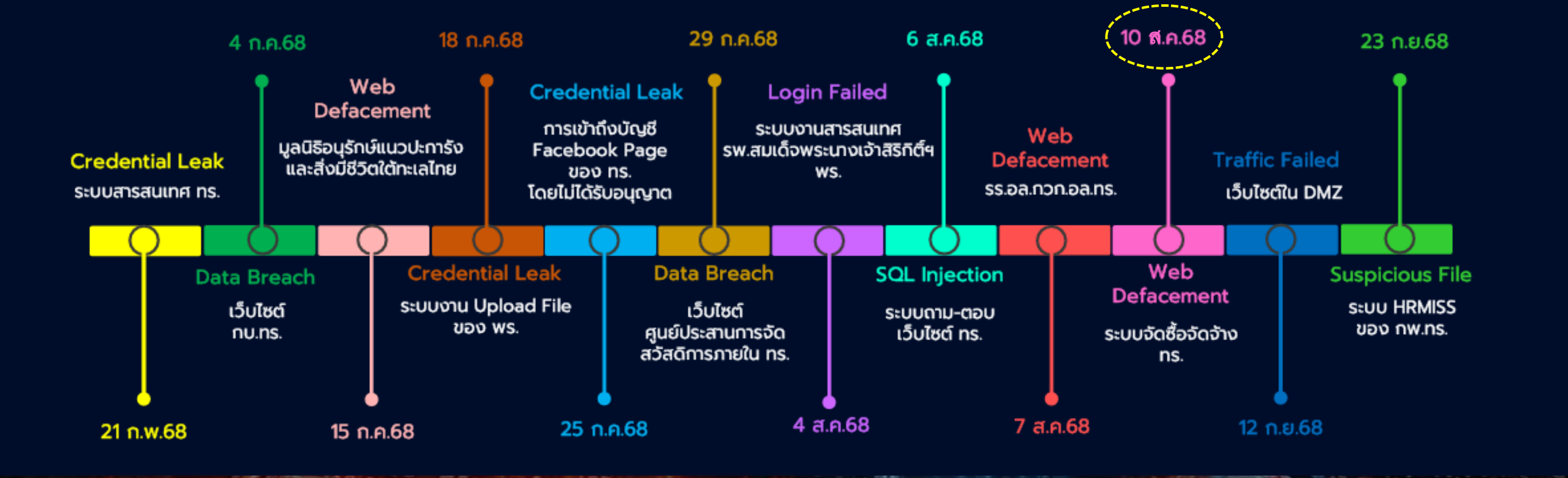
๑. หน.ชุด
๒. จนท.เฝ้าระวัง
๓. จนท.ระบบเทคโนโลยีสารสนเทศ
๔. จนท.ระบบเครือข่าย
๕. จนท.พิสูจน์หลักฐานทางดิจิทัล
๖. จนท.ตอบสนองเหตุการณ์
๗. ประสานงาน

**Cyber Combat Mission Team : CCMT**

๑. หน.ชุด
๒. จนท.ปฏิบัติการ (๑)
๓. จนท.ปฏิบัติการ (๒)
๔. จนท.ปฏิบัติการ (๓)
๕. จนท.ปฏิบัติการ (๔)

จัดชุด CPT (๗) และ CCMT (๕) เพิ่มเติมให้กับ ศสช.ศปก.ทร.
รองรับสถานการณ์ทางไซเบอร์ที่มีแนวโน้มสูงขึ้น

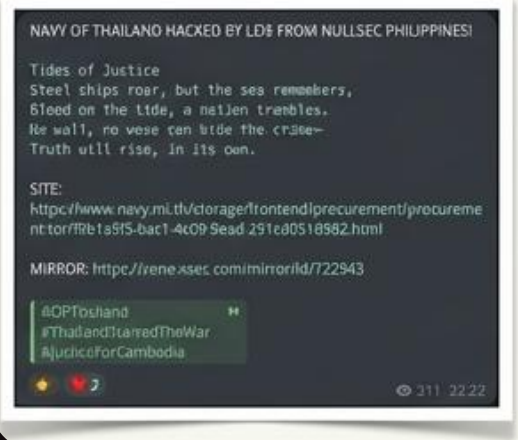
# เหตุการณ์ทางไซเบอร์ที่เกี่ยวข้องกับกองทัพเรือ



# เหตุการณ์ Credential Leaked

## สรุปเหตุการณ์

- **เหตุการณ์:** เมื่อวันที่ 10 สิงหาคม 2568 เวลา 01.00 น. สกมช. แจ้งตรวจพบการโพสต์ข้อมูล Credential ของผู้ใช้งานเว็บไซต์กองทัพเรือบน Telegram
- **กลุ่มผู้ก่อเหตุ:** NULLSEC PHILIPPINES ร่วมกับ KOLZSEC
- **ผลกระทบ:** ข้อมูล login ของผู้ใช้งาน [redacted]@navy.mi.th ถูกเปิดเผย





## ผลการตรวจสอบและสาเหตุของช่องโหว่

1. ระบบไม่มีการตรวจสอบและจำกัดประเภทไฟล์ที่อัปโหลด (Unrestricted File Upload)
2. ผู้ใช้งานระบบมีการบันทึกรหัสผ่านไว้บนเบราว์เซอร์ (Saved Passwords in Browser)
3. เครื่องคอมพิวเตอร์ของผู้ใช้งานไม่มีการติดตั้งโปรแกรม Antivirus ที่มีประสิทธิภาพ
4. ขาดการใช้งานระบบยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA)

# ความเสี่ยงต่อภัยคุกคามทางไซเบอร์

## ภาพรวมและช่องโหว่สำคัญ

### ประเภทภัยคุกคามไซเบอร์ที่พบบ่อย

**การเปลี่ยนหน้าเว็บไซต์ (Web Defacement)**

แฮกเกอร์บุกรุกเข้ามาแก้ไขหน้าเว็บ ทำให้ส่งผลกระทบต่อภาพลักษณ์และความน่าเชื่อถือขององค์กร

**มัลแวร์และเว็บเชลล์ (Malware / Webshell)**

การฝังไฟล์อันตรายที่เปิดช่องให้ผู้โจมตีสามารถเข้ามาควบคุมระบบได้จากระยะไกล

**การโจมตีเพื่อขโมยข้อมูล (Data Theft Attacks)**

ใช้เทคนิค SQL Injection และ Brute Force เพื่อเข้าถึง แก้ไข หรือโขมยข้อมูลสำคัญในฐานข้อมูล

### 4 ช่องโหว่หลักที่เป็นต้นเหตุ


**รหัสผ่านคาดเดาง่าย**

การตั้งรหัสผ่านที่อ่อนแอ (เช่น 1234) เป็นประตูหลักให้ผู้โจมดีเข้าระบบได้สำเร็จ

**ระบบอัปโหลดไฟล์ไม่ปลอดภัย**

เปิดให้แฮกเกอร์สามารถอัปโหลดไฟล์อันตรายที่แฝงตัวเป็นไฟล์รูปภาพหรือเอกสารได้


**ขาดการยืนยันตัวตนหลายปัจจัย (MFA)**

การไม่มีระบบป้องกันขั้นที่สอง ทำให้บัญชีถูกยึดได้ง่ายเมื่อรหัสผ่านรั่วไหล

**ไม่ได้อัปเดตแพตช์ความปลอดภัย**

ระบบที่ไม่อัปเดตอย่างสม่ำเสมอจะมีช่องโหว่ที่รู้จักกันดีและจ่าขต่อการโจมดี


# การปฏิบัติการไซเบอร์ที่ผ่านมา

# แนวความคิดการปฏิบัติ

ขั้นปกติ - สถานการณ์วิกฤต (ระดับความพร้อม ๒)

## เชิงรุก (OCO)

- ประสานการปฏิบัติกับ ฝขว.ฯ สนับสนุนข้อมูลข่าวกรองไซเบอร์ ในพื้นที่สนใจหาข่าว (NAI)
- ตรวจสอบหาข้อมูลสำคัญที่รั่วไหล (Credential Leaked) เพื่ออาศัยประโยชน์ในการเข้าถึงระบบของฝ่ายตรงข้าม
- CCMT ดำเนินการตามขีดความสามารถเพื่อสร้างผลกระทบ และแสวงประโยชน์ในมิติไซเบอร์

## เชิงรับ (DCO)

- รับมือเหตุการณ์ทางไซเบอร์ในสถานการณ์วิกฤต โดยมุ่งเน้นการเฝ้าระวังในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับระบบเครือข่ายทางยุทธการ
- แจ้งเตือนกรณีตรวจพบภัยคุกคามฯ ให้กับหน่วยภายใน ทร. และแลกเปลี่ยนข้อมูลกับหน่วยภายนอก
- CPT เตรียมพร้อมตอบสนองเหตุการณ์ ฯ

# แนวทางการพัฒนาขีดความสามารถปฏิบัติการเชิงรุก

## การสร้างกำลังพล (Building the Force)

**สร้างชุมชนผู้เชี่ยวชาญไซเบอร์**

เน้นการทดสอบเจาะระบบ (penetration testing) และทีม Red Team


**จัดตั้งกลไกการรับบุคลากรแบบยืดหยุ่น**

เพื่อระดมกำลังสำรองและผู้เชี่ยวชาญในยามวิกฤต


## การยกระดับขีดความสามารถ (Enhancing Capabilities)


**จัดการองค์ความรู้จากการ (Systematize Knowledge from Operations)**

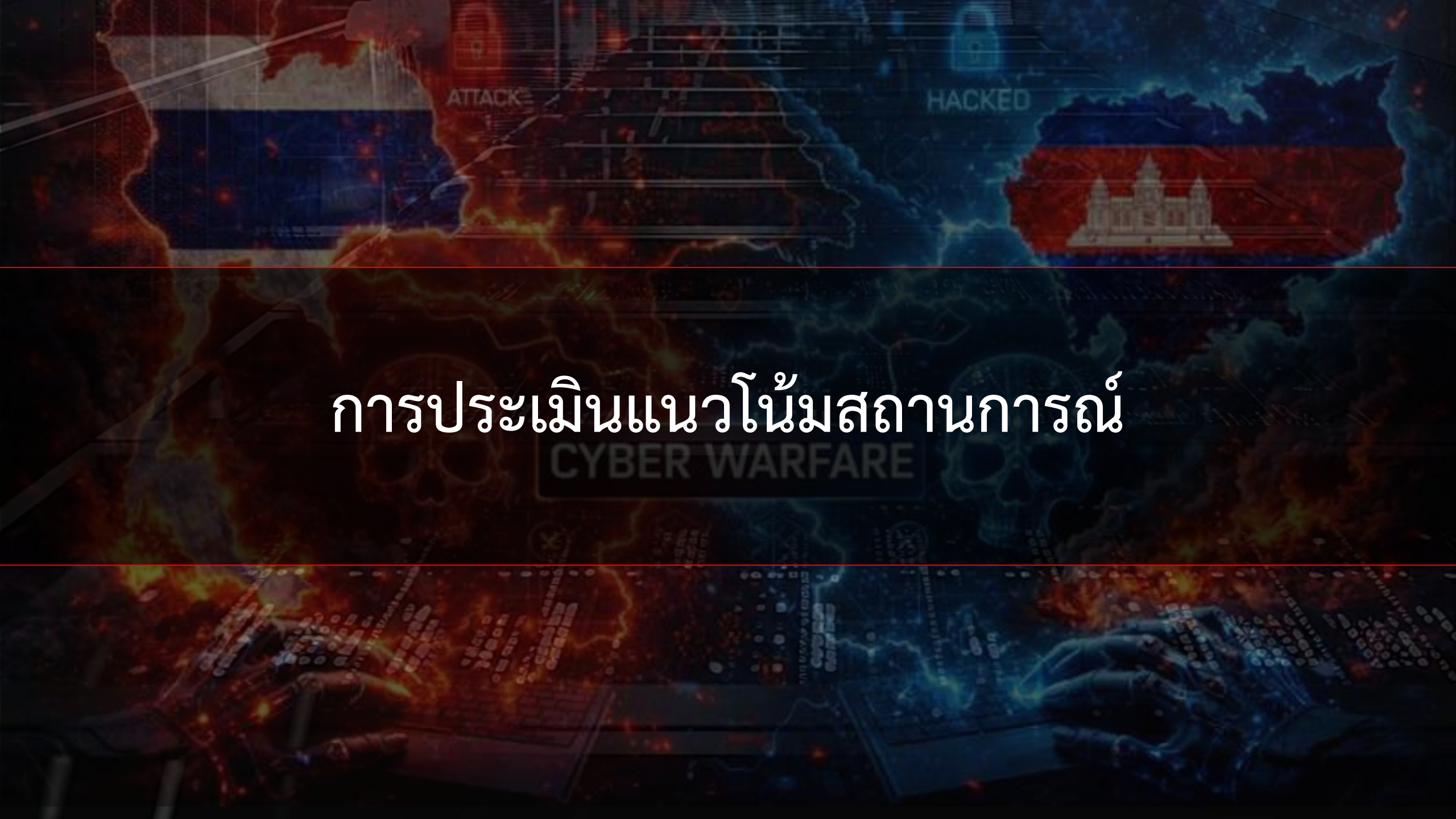
รวบรวมบทเรียนทั้งเชิงรุก เชิงรับ และผลกระทบต่างๆ

**วิเคราะห์ช่องว่างเพื่อปรับปรุงยุทธวิธี**


พัฒนา TTP, เครื่องมือ, และการฝึกฝนอย่างต่อเนื่อง


**บูรณาการ OCO สู่การปฏิบัติการร่วม**

เพื่อให้พร้อมใช้งานและมีประสิทธิภาพเชิงยุทธการ




# การประเมินแนวโน้มสถานการณ์

# สถานการณ์ด้านไซเบอร์

## ธันวาคม 2568: ระลอกการโจมตีช่วงปลายปี

### โจมตีหน่วยงานรัฐและโครงสร้างพื้นฐาน

รัฐสภาไทย

ThaiCERT

ระบบ GIS ของ ปตท.

### รูปแบบการโจมตีหลากหลาย

เจาะระบบ

ขโมยข้อมูล (DITP)

DDoS

Web Defacement (ns.)

### แฮกเกอร์กัมพูชาเป็นผู้ก่อเหตุหลัก

กลุ่ม H3C4KEDZ
NXBBSEC
rxxhcyber

## มกราคม 2569: ยกระดับปฏิบัติการและสร้างพันธมิตร

### สร้างเครือข่ายพันธมิตรโจมตีไทย

ZAHER INFINITY

Dead killer

DIGIT4_CYB3R

ประกาศร่วมมือกัน

### ขยายเป้าหมายสู่ภาคเอกชนและสื่อ

เว็บไซต์ อย.



บริษัทเอกชน

โรงเรียน

สมาคมผู้ผลิตข่าวออนไลน์

### พัฒนาเครื่องมือสร้างความตื่นตระหนก

กลุ่ม NXBB•SEC เผยแพร่ Fake Ransomware
เพื่อข่มขู่มากกว่าเรียกค่าไถ่จริง

# ประเมินภัยคุกคามทางไซเบอร์

## 1. การลดระดับของกลุ่มหลัก

กลุ่มแฮกเกอร์ชาตินิยมกัมพูชาชุดแรก (AnonSec-KH, NXBBSEC) ลดกิจกรรมที่เกี่ยวข้องกับความขัดแย้งชายแดนลง และมีแนวโน้มหันไปปฏิบัติการที่มุ่งเน้นผลประโยชน์ทางการเงิน (Profit-driven) มากขึ้น

## 2. การเกิดขึ้นของกลุ่มใหม่

ตลอดปี 2568 ได้เกิดกลุ่มแฮกเกอร์ใหม่ๆ เช่น **NOTCTBER** และ **NOTCTBER404** ซึ่งยังคงมีแรงจูงใจในการโจมตีเป้าหมายในประเทศไทยอย่างต่อเนื่อง





NOTCTBER Attack Claims


New Alliance Announcement

## คาดการณ์ (ไตรมาส 1 ปี 2569)

มีโอกาสสูงที่จะเกิดการโจมตีระลอกใหม่ในรูปแบบ DDoS และ Disinformation จากกลุ่มแฮกเกอร์รุ่นใหม่
หากเกิดเหตุการณ์ปะทะหรือความตึงเครียดบริเวณชายแดนอีกครั้ง

## คาดการณ์ (กลาง-ปลายปี 2569)

หากสถานการณ์ชายแดนยังคงสงบ ความเสี่ยงโดยรวมจะลดระดับลงสู่ระดับต่ำ

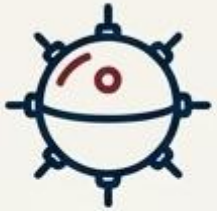
## ปัจจัยที่อาจเปลี่ยนแปลงสถานการณ์

### การเลือกตั้ง 2569

อาจถูกใช้เป็นประเด็นในการสร้างสถานการณ์โจมตีทางไซเบอร์เพื่อแทรกแซงหรือสร้างความวุ่นวาย

### การแทรกแซงจากมหาอำนาจ

การสนับสนุนกัมพูชาจากจีน หรือการเรียกร้องสันติภาพจากสหรัฐฯ อาจส่งผลต่อพลวัตของความขัดแย้ง



### ปัญหาทุ่นระเบิด

เหตุการณ์ที่เกี่ยวข้องกับทุ่นระเบิดตามแนวชายแดน อาจกลายเป็นชนวนเหตุความขัดแย้งรอบใหม่ได้เสมอ


กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ
กองทัพเรือ
CYBER
INTELLIGENCE
Q & A