MISP Node Status Report

รายงานฉบับนี้จัดทำขึ้นเพื่อสรุปผลการตรวจสอบสถานะของเซิร์ฟเวอร์/โหนด (Nodes) MISP ในช่วงเดือนมกราคมที่ผ่านมา โดยทำการเก็บข้อมูลในแต่ละวันว่าได้รับสถานะตอบกลับแบบใด เช่น Compatible, Could not POST, Version Incompatible หรือ Down ทั้งนี้เพื่อใช้ประเมินความพร้อมในการให้บริการ พร้อมทั้งหาแนวโน้มปัญหาหรือความผิดปกติที่อาจเกิดขึ้น และใช้ข้อมูลดังกล่าวเป็นแนวทางในการปรับปรุงหรือแก้ไขต่อไป

ความหมายของสถานะ

- Compatible: เซิร์ฟเวอร์ทำงานปกติ, ใช้งานได้ตามปกติ, ไม่พบปัญหา
- Couldn't POST: ไม่สามารถส่งข้อมูลผ่านเมธอด POST ได้ (เช่น ติดปัญหากับ API)
- Version Incompatible: มีข้อผิดพลาดเกี่ยวกับเวอร์ชัน เช่น เวอร์ชันไม่ตรงกัน
- Down: ระบบล่ม, ติดต่อเซิร์ฟเวอร์ไม่ได้ หรือเซิร์ฟเวอร์ไม่ตอบสนอง

ตารางสรุปผลของเดือนกุมภาพันธ์ 2568

ตารางสรุปผลนี้บันทึกสถานะของโหนดในแต่ละหน่วยงานในช่วงเดือนมกราคมที่ผ่านมา, โดยคอลัมน์แต่ละช่องจะระบุจำนวนวันที่พบสถานะแต่ละแบบ (เช่น Compatible, Couldn't POST, Version Incompatible, Down) และระบุหมายเหตุเพิ่มเติมเพื่อบอกรายละเอียดต่างๆเพิ่มเติมของความผิดพลาด, โดยตัวเลขสถิติในตารางจะนับเป็นวัน, เช่น Compatible เท่ากับ 31 หมายถึงเซิร์ฟเวอร์ปลายทางทำงานปกติทั้ง 31 วันโดยไม่มีข้อผิดพลาดในเดือนนั้น

หน่วยงาน PARTNER	Compatible	Couldn't POST	Version Incompatible	Down	หมายเหตุ
CII_MISP	31				
NIA	31				
TB-CERT		31			ไม่สามารถรับ feed จากทาง สกมช. ได้
TTC-CERT				31	Server หมดอายุ อยู่ระหว่างรองบ
DGA	31				
Energy-CERT	31				
Health-CERT	31				
MOT-CERT	16			15	Server Down ตั้งแต่วันที่ 18 จนถึงสิ้นเดือนกุมภาพันธ์
NCERT	31				
MOD-CERT	31				
Backup-MISP	31				
public-MISP	31				
Gov-MISP	31				
TCM-CERT			31		Version ของ MISP ไม่เข้ากัน แต่ยังสามารถรับ feed จากทาง สกมช. ได้
METRO			13	15	Version ของ MISP ไม่เข้ากัน แต่ยังสามารถรับ feed จากทาง สกมช. ได้

ตารางที่ 1 ตารางสรุปผลสถานะโหนดปลายทางของ Partner ของเดือนกุมภาพันธ์

หน่วยงาน CII	Compatible	Couldn't POST	Version Incompatible	Down	หมายเหตุ
EGAT	31				
RTARF	31				
PEA	31				
MSDHS	31				
MOJ	31				
CPD	31				
QSDS	31				
DOH	31				
DOE	31				
EXCISE	31				
DOPA	31				
NSC				31	
DRT	31				
ONDE	31				
MDES				31	
CGD	31				
MOF	30			1	Server Down ใน วันที่ 19 กุมภาพันธ์
SPM	31				
DOAE	31				
CCIB				31	
DRRAA	31				
RD	31				
UDH	31				
NSO	31				
MOC	31				

ตารางที่ 2 ตารางสรุปผลสถานะโหนดปลายทางของ CII ของเดือนกุมภาพันธ์

หน่วยงาน GOV	Compatible	Couldn't POST	Version Incompatible	Down	หมายเหตุ
DOL	31				
CMU			14	14	Version ของ MISP ไม่เข้ากัน แต่ยังสามารถรับ feed จากทาง สกมช. ได้
GPF	31				
RMUTL	31				
DLT	31				

ตารางที่ 3 ตารางสรุปผลสถานะโหนดปลายทางของ Gov ของเดือนกุมภาพันธ์

วิเคราะห์และสรุปผล

PARTNER

ตรวจสอบทั้งหมด 465 ครั้งจาก 15 Node, พบว่าเซิร์ฟเวอร์ตอบกลับด้วยสถานะ Compatible จำนวน 308 ครั้ง (ประมาณ 66.2% จากทั้งหมด), Couldn't POST จำนวน 28 ครั้ง (6.0%), Version Incompatible 41 ครั้ง (8.8%), และ Down 43 ครั้ง (9.2%), แสดงให้เห็นว่าระบบส่วนใหญ่ยังคงทำงานได้ปกติ แต่ก็มีสัดส่วนของ Version Incompatible และ Down รวมกว่า 18% ที่ควรเฝ้าระวังและตรวจสอบสาเหตุต่อไป

CII

ตรวจสอบทั้งหมด 775 ครั้งจาก 25 Node, พบว่าเซิร์ฟเวอร์ตอบกลับด้วยสถานะ Compatible จำนวน 615 ครั้ง (ประมาณ 79.4% ของทั้งหมด), Couldn't POST จำนวน 0 ครั้ง (0%), Version Incompatible 0 ครั้ง (0%), และ Down 85 ครั้ง (11.0%), ซึ่งแสดงให้เห็นว่าระบบของปลายทางส่วนใหญ่ยังทำงานได้ดี แต่ยังต้องควรติดตามและหาแนวทางลดปัญหา Down ที่มีสัดส่วนสูงถึง 11% เพื่อให้บริการต่อเนื่องยิ่งขึ้น

GOV

ตรวจสอบทั้งหมด 140 ครั้งจาก 5 Node, พบว่าเซิร์ฟเวอร์ตอบกลับด้วยสถานะ Compatible จำนวน 109 ครั้ง (ประมาณ 77.9% ของทั้งหมด), Couldn't POST จำนวน 0 ครั้ง (0%), Version Incompatible 14 ครั้ง (10.0%), และ Down 17 ครั้ง (12.1%), ซึ่งแสดงให้เห็นว่าระบบของปลายทางส่วนใหญ่ยังทำงานได้ดี แต่ยังต้องควรติดตามและหาแนวทางลดปัญหา Version Incompatible และ Down รวมกว่า 22.1% เพื่อให้บริการต่อเนื่องยิ่งขึ้น

การตรวจสอบและกรอง Indicators of Compromise (IoC

การตรวจสอบและกรอง Indicators of Compromise (IoC) ที่ได้รับจากหน่วยงานภายนอกก่อนนำเข้าระบบ MISP (Malware Information Sharing Platform) เป็นขั้นตอนที่สำคัญ เนื่องจาก

1. ลด False Positives และป้องกันข้อมูลที่ไม่น่าเชื่อถือ

IoC ปลอม (False Positives) อาจทำให้ระบบแจ้งเตือนเหตุการณ์ที่ไม่ใช่ภัยคุกคามจริง ซึ่งอาจส่งผลให้ทีม Incident Response สูญเสียเวลาในการตรวจสอบสิ่งที่ไม่ใช่ภัยคุกคามจริง

บางครั้งแหล่งที่มาของข้อมูลอาจมี ข้อมูลเก่าหรือไม่มีความถูกต้อง ซึ่งหากไม่กรองก่อน อาจทำให้เกิดการบล็อก IP หรือโดเมนที่ไม่เกี่ยวข้องกับการโจมตีจริง

2. ป้องกันข้อมูลอันตรายที่ถูกแทรกแซง

Supply Chain Attack ใน Threat Intelligence: มีกรณีที่ แฮกเกอร์ฝัง IoC ปลอม เข้าไปใน Threat Intelligence Feeds เพื่อหลอกให้หน่วยงานเป้าหมายบล็อก IP หรือโดเมนที่เป็นของผู้ให้บริการที่ถูกต้อง หรือแม้กระทั่งบล็อกโครงสร้างพื้นฐานของตนเอง

หาก IoC ถูก ป้อนเข้าสู่ MISP โดยไม่มีการตรวจสอบ อาจทำให้เกิดผลกระทบต่อการดำเนินงานขององค์กร เช่น การบล็อกเซิร์ฟเวอร์ที่จำเป็นต้องใช้

3. ป้องกันการ Over-blocking ที่อาจกระทบต่อการดำเนินงาน

หากองค์กรนำ IoC ที่ไม่ได้ตรวจสอบ มาใช้กับ Firewall, SIEM หรือ EDR อาจทำให้มีการบล็อกทราฟฟิกที่ไม่เป็นอันตราย ซึ่งอาจกระทบต่อระบบงานปกติ เช่น บล็อก API ของผู้ให้บริการที่สำคัญ หรือกระทบต่อการสื่อสารขององค์กร

4. ความสอดคล้องกับกฎหมายและ Compliance

ในบางกรณี IoC อาจมาจาก Threat Intelligence Feeds ที่ไม่เป็นทางการ หรือไม่ได้ผ่านการตรวจสอบจากแหล่งที่เชื่อถือได้ ซึ่งอาจนำไปสู่การบล็อกข้อมูลที่ละเมิดข้อกำหนดด้าน GDPR, NIST, ISO 27001 หรือกฎหมายอื่น ๆ

หากบล็อกทรัพยากรที่เกี่ยวข้องกับหน่วยงานภาครัฐ หรือองค์กรที่ได้รับการคุ้มครองโดยกฎหมาย อาจส่งผลให้เกิดปัญหาทางกฎหมายตามมา

5. ปรับแต่ง IoC ให้เหมาะสมกับสภาพแวดล้อมขององค์กร

แต่ละองค์กรมีโครงสร้างพื้นฐานทาง IT และเครือข่ายที่แตกต่างกัน IoC บางรายการอาจไม่มีผลกับองค์กรของเรา หรืออาจเป็น false positive ในบริบทของเครือข่ายของเรา

ควรมี ทีม Threat Intelligence หรือ SOC ทำการวิเคราะห์และประเมินผลกระทบ ก่อนนำเข้า IoC ทั้งหมดลงในระบบ MISP

แนวทางการตรวจสอบ IoC ที่ Feed เข้ามา

- ตรวจสอบแหล่งที่มา – แหล่งที่ให้ข้อมูลเชื่อถือได้หรือไม่ เช่น จาก CISA, FBI, CERT หรือจากแหล่ง OSINT ที่น่าเชื่อถือ
- เช็คความถูกต้องของข้อมูล – เปรียบเทียบกับ IoC ที่มีอยู่ในฐานข้อมูล เช่น VirusTotal, AlienVault OTX, AbuseIPDB
- ตรวจสอบว่าข้อมูลเป็นปัจจุบันหรือไม่ – IoC บางรายการอาจเป็นของเก่าหรือหมดอายุไปแล้ว
- ใช้ Threat Intel Platform เช่น MISP และ SIEM – วิเคราะห์ความสัมพันธ์ระหว่าง IoC และพฤติกรรมของภัยคุกคามที่พบในระบบ
- ทดสอบ IoC ใน Sandbox หรือระบบแยกต่างหากก่อนบังคับใช้ – เพื่อลดความเสี่ยงในการบล็อกทราฟฟิกที่จำเป็น

การตรวจสอบและกรอง Indicators of Compromise (IoC) ของเดือนกุมภาพันธ์ 2568

MISP เป็นแพลตฟอร์มสำหรับการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ที่สามารถจัดเก็บ วิเคราะห์ และกระจาย Indicators of Compromise (IoC) เพื่อช่วยในการป้องกันและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยไซเบอร์ โดยมีการตรวจสอบและกรอง IoC ด้วยกระบวนการดังนี้

การตรวจสอบ IoC ใน MISP มีหลายระดับ โดยครอบคลุมการตรวจสอบทางเทคนิคและบริบทที่เกี่ยวข้องกับ IoC นั้น ๆ

1. การตรวจสอบความถูกต้องของข้อมูล (Data Validation)

- ระบบจะทำการตรวจสอบข้อมูล IoC ที่เพิ่มเข้ามา เช่น รูปแบบ (format) และประเภท (type) ของข้อมูล
- ตรวจสอบว่า IoC นั้นซ้ำกับข้อมูลที่มีอยู่แล้วหรือไม่ (Deduplication)
- ใช้ Regular Expressions (Regex) เพื่อป้องกันการเพิ่มข้อมูลที่ผิดพลาด

2.การตรวจสอบความน่าเชื่อถือของ IoC (Reputation & Confidence Level)

- มีระบบ Sightings เพื่อระบุว่า IoC นั้นเคยพบในการโจมตีจริงหรือไม่
- ใช้ Warning Lists เพื่อตรวจจับ IoC ที่เป็น False Positive หรือไม่น่าเชื่อถือ เช่น IP ของ Google DNS, Cloudflare, หรือ Tor Exit Nodes
- ตรวจสอบแหล่งที่มาของ IoC ว่าเป็นแหล่งข้อมูลที่เชื่อถือได้หรือไม่

3. การเชื่อมโยงกับ Threat Intelligence (Correlation)

- IoC ที่เพิ่มเข้ามาจะถูกตรวจสอบว่ามีความเกี่ยวข้องกับข้อมูลภัยคุกคามที่มีอยู่แล้วหรือไม่
- ระบบ MISP ใช้ฟีเจอร์ Correlation Graphs เพื่อแสดงความสัมพันธ์ของ IoC กับเหตุการณ์อื่นๆ

สรุปผล การตรวจสอบและกรอง Indicators of Compromise (IoC) ของเดือนกุมภาพันธ์ 2568

วันที่	ผลการตรวจสอบ
3	Negative
4	Negative
5	Negative
6	Negative
7	Negative
10	Negative
11	Negative
12	Negative
13	Negative
14	Negative
17	Negative
18	Negative
19	Negative
20	Negative
21	Negative
24	Negative
25	Negative
26	Negative
27	Negative
28	Negative

ตารางสรุปผล การตรวจสอบและกรอง Indicators of Compromise (IoC) ของเดือนกุมภาพันธ์

ความหมายของสถานะ

- Positive: พบปัญหา , พบ IoCs แปลกปลอมหรือผิดปกติ
- Negative: ไม่พบปัญหา , IoCs แปลกปลอมหรือผิดปกติ

อ้างอิงจาก

Threat Intelligence ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์

จัดทำโดย

ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ สำนักประสานงาน
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทร: 02 114 3531 อีเมล: cti_misp@ncsa.or.th