



## 2022년 1월

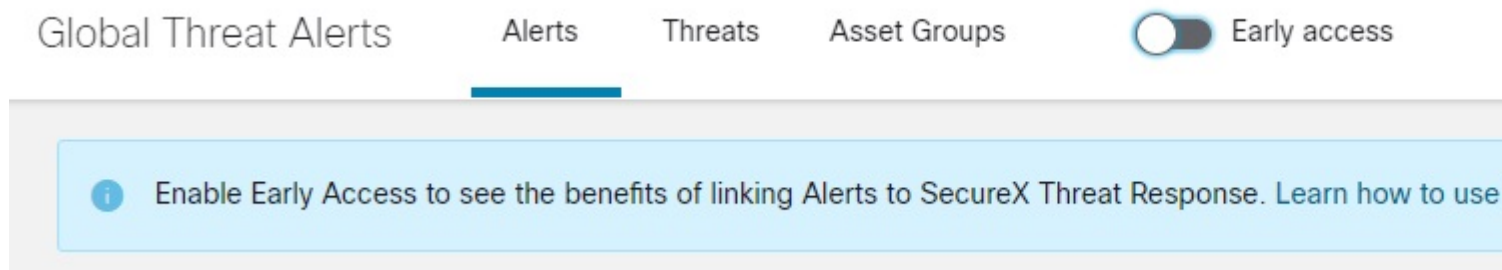
2022년 1월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

- [SecureX 인시던트 관리자로 알림 승격, 1 페이지](#)
- [추가 위협 탐지, 6 페이지](#)

## SecureX 인시던트 관리자로 알림 승격

전역 위협 알림의 알림을 SecureX 인시던트 관리자로 승격하는 기능을 추가했습니다. 이 기능을 켜려면 전역 위협 알림 콘솔의 헤더에서 **Early Access**(얼리 액세스)를 활성화해야 합니다.

그림 1: 이 새 기능을 활성화하려면 **Early Access**(얼리 액세스)를 클릭해야 합니다.



활성화되면 SecureX 인시던트 관리자가 전역 위협 알림의 기존 워크플로우를 대체합니다. 알림은 **New**(신규), **Accepted**(수락됨) 또는 **Rejected**(거부됨)로 분류됩니다.

그림 2: SecureX 인시던트 관리자 내의 알림

Global Threat Alerts  Early access

**Detections**

- Alerts
  - New 3 5 6
  - Accepted
  - Rejected

**New Alerts**  
Alerts pointing to risks on your network

Active from  to

Risk level  Critical  High  Medium  Low

**Accept**(수락) 또는 **Reject**(거부) 버튼을 사용하여 새 알림을 두 가지 상태 중 하나로 전환할 수 있습니다.

그림 3: 알림 수락 또는 거부

**Critical Risk** ETA

When: November 12th - February 7th

Modified: 13 hours ago

---

Threats: WannaCry, Emotet, SMB service discovery

---

Asset Groups: Catch All

Affected Assets: 2 assets

Usernames: demo

IP Addresses: 10.0.0.1  10.0.0.3

글로벌 위협 알림은 확장된 탐지 및 효율적인 알림 분류 같은 핵심 역량에 계속 집중하지만, 이제 클릭 한 번으로 탐지를 SecureX의 인시던트 대응 워크플로우로 승격하는 SecureX 에코시스템을 이용해 더욱 긴밀하게 통합됩니다.

수락한 알림은 SecureX 인시던트 관리자에서 기존 또는 새 인시던트에 연결할 수 있습니다.

그림 4: 인시던트에 연결 옵션을 이용해 알림 수락

**Accept Alert** [X]

**Accept and link to a new incident**

Title (required)

Short description (required)

**Accept and link to existing incidents**

🔍 Use Lucene syntax to filter incidents [X]

Response to critical risk alert

[Empty]

[Empty]

[Empty]

**Accept only**

[Cancel] [Accept]

SecureX 인시던트 관리자에 있는 인시던트에는 **Summary**(요약) 및 원래 알림의 모든 보안 **Events**(이벤트)와 **Observables**(관찰 가능 항목)을 포함한 세부 정보가 포함됩니다. 조사, 강화 및 오케스트레이션 같은 SecureX 기능을 사용하여 추가로 조사하고 대응할 수 있습니다.

그림 5: 인시던트 요약의 예

## Response to critical risk alert

Critical risk alert has been promoted to an incident for purposes of incident response

New · Created by [Global Threat Alerts](#) on 2022-02-08T13:03:25.447Z

[Summary](#)

[Events](#)

[Observables](#)

[Timeline](#)

[Linked References \(9\)](#)

### Critical Risk alert

**When:** Friday, November 12th

**Duration:** 87 days

**Threats:**

[Emotet](#), [WannaCry](#), [SMB service discovery](#), [Excessive communication](#)

**Asset Groups:**

Catch All

**Username:**

[demo\\_keturah.gaunt](#), [dusti.hilton](#)

**IP Addresses:**

[10.102.77.196](#), [10.201.3.51](#)

[Edit Summary Markdown](#)

그림 6: 인시던트 관찰 가능 항목의 예

## Response to critical risk alert

Critical risk alert has been promoted to an incident for purposes of incident response

New · Created by [Global Threat Alerts](#) on 2022-02-08T13:03:25.447Z

Summary    Events    **Observables**    Timeline    Linked References (9)



10.102.77.196

**Network** · Targeted by 1 unique observable, 1 time in the last 11 hours

IP Address · 10.102.77.196

User · demo\_keturah.gaunt

First: 2022-02-08T03:00:55.334Z · Last: 2022-02-08T13:03:24.945Z



10.201.3.51

**Network** · Targeted by 5 unique observables, 9 times in the last 3 months

IP Address · 10.201.3.51

User · dusti.hilton

First: 2021-11-12T00:00:00.000Z · Last: 2022-02-07T04:14:58.000Z

Observables · 225 Total · [Investigate these Observables](#)



170.178.168.203

**Malicious IP Address** · 1 Target · 5 Sightings · 0 Snapshots

First: 2021-11-23T05:04:59.000Z · Last: 2022-02-08T13:03:24.945Z



70.32.1.32

**Malicious IP Address** · 1 Target · 3 Sightings · 0 Snapshots

First: 2021-11-23T05:04:59.000Z · Last: 2022-02-08T13:03:24.945Z



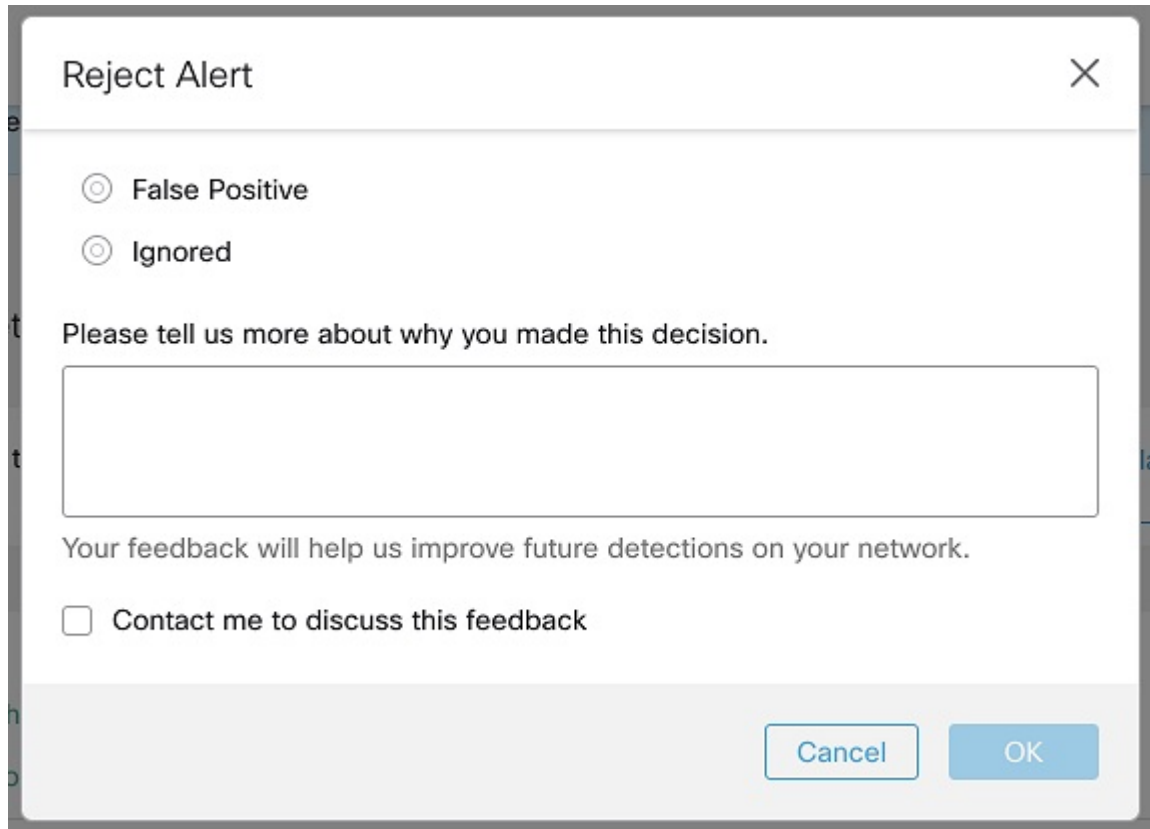
77.55.211.77

**Malicious IP Address** · 1 Target · 3 Sightings · 0 Snapshots

First: 2021-11-24T23:34:38.000Z · Last: 2022-02-08T13:03:24.945Z

알림을 인시던트로 승격하는 것이 바람직하지 않다면 거부하면 됩니다. 이 경우 Cisco 팀에 피드백을 보내 알림을 거부한 이유를 통보할 수 있습니다. 감사합니다. 귀하의 소중한 피드백은 네트워크에서의 향후 탐지를 개선하는 데 도움이 됩니다.

그림 7:알림 거부 및 피드백 제공



The image shows a 'Reject Alert' dialog box with a close button (X) in the top right corner. It contains two radio button options: 'False Positive' (selected) and 'Ignored'. Below these is a text input field with the prompt 'Please tell us more about why you made this decision.' Underneath the input field is the text 'Your feedback will help us improve future detections on your network.' At the bottom left, there is a checkbox labeled 'Contact me to discuss this feedback'. At the bottom right, there are two buttons: 'Cancel' and 'OK'.

## 추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- IcedID
- Lemon Duck

또한 다양한 저위험 위협 탐지가 강화되었습니다.

### IcedID

BokBot이라고도 하는 IcedID([S0483](#))는 금융 정보를 노리는 모듈형 뱅킹 트로이 목마입니다. 다양한 감염 벡터를 활용하며, 다른 악성코드에 대한 드로퍼 역할을 하기도 합니다([T1105](#)). 모듈형 구조와 드로퍼 기능 때문에 Emotet([S0367](#))의 후속으로 간주됩니다. IcedID는 브라우저 세션([T1185](#))에서 금융 정보 및 뱅킹 자격 증명을 훔쳐 사기 거래에 사용합니다. IcedID는 탐지([TA0005](#))를 방지하기 위해 자신을 원격 프로세스([T1055.004](#))에 삽입하기도 합니다.

사용자 환경에서 IcedID가 탐지되었는지 확인하려면 [IcedID Threat Detail\(IcedID 위협 세부 정보\)](#)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 8:

**IcedID**  
Modular malware designed to steal financial information

High Severity  **Confirmed** 10+ affected assets in 5+ companies

IcedID (S0483), also known as BokBot, is a modular banking trojan, targeting financial information. Besides leveraging different infection vectors, it can act as dropper for other malware (T1105). Considering its modular structure and dropper capabilities, it was seen as a successor to Emotet (S0367). IcedID is capable of stealing financial information and banking credentials from browser sessions (T1185), in order to use them for fraudulent transactions. To avoid detection (TA0005), IcedID can inject itself into remote processes (T1055.004).

Category: Malware - trojan

### Lemon Duck

Lemon Duck은 암호화폐 채굴을 위한 파일 없는 PowerShell 악성코드에 속합니다. 이 악성코드는 EternalBlue 익스플로잇, 해시 통과 및 비밀번호 무차별 대입을 사용하여 로컬 네트워크의 다른 시스템으로 확산됩니다. 암호화폐 채굴기는 대량의 CPU 또는 GPU 리소스를 사용하여 비트코인이나 모네로 같은 암호화폐를 채굴합니다.

사용자 환경에서 Lemon Duck이 탐지되었는지 확인하려면 [Lemon Duck Threat Detail\(Lemon Duck 위협 세부 정보\)](#)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 9:

**Lemon Duck**  
Software that uses your computing resources to mine cryptocurrencies

Critical Severity  **Confirmed** 10+ affected assets in 5+ companies

Lemon Duck is a file-less PowerShell malware family for mining cryptocurrency. This malware has been seen using EternalBlue exploits, pass-the-hash, and password bruteforcing to spread to other machines on the local network. Cryptocurrency miners use a large amount of CPU or GPU resources to mine cryptocurrency such as Bitcoin or Monero. This IOC alerts when PowerShell is seen executing Lemon Duck commands.

Category: Malware - crypto miner





## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.