



## 2022 年 1 月

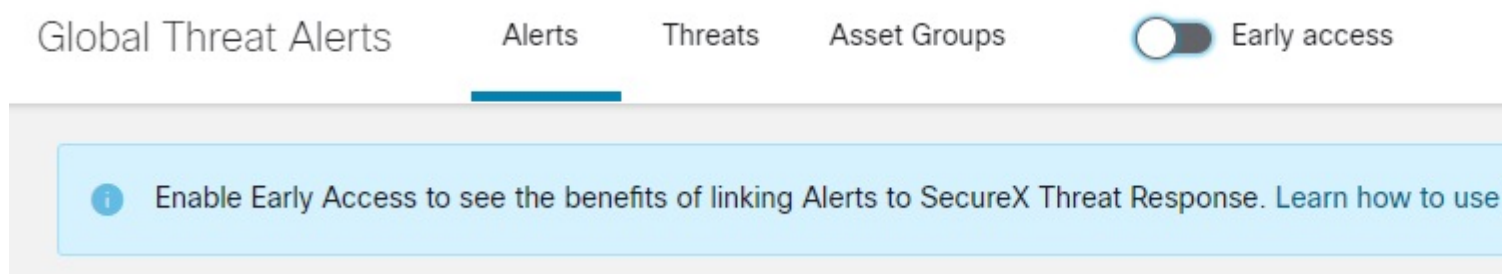
2022 年 1 月にリリースされた、シスコのクラウドベースの機械学習によるグローバル脅威アラートに関するアップデートです。

- [SecureX Incident Manager へのアラートプロモーション \(1 ページ\)](#)
- [追加の脅威検出 \(6 ページ\)](#)

## SecureX Incident Manager へのアラートプロモーション

SecureX Incident Manager へグローバル脅威アラートでアラートをプロモートする機能を追加しました。この機能を有効にするには、グローバル脅威アラートコンソールのヘッダーで [早期アクセス (Early access) ] を有効にします。

図 1: [早期アクセス (Early access) ] をクリックして新機能を有効化



有効にすると、SecureX Incident Manager は、グローバル脅威アラートの既存のワークフローを置き換えます。アラートは、[新規 (New) ]、[承認 (Accepted) ]、または [拒否 (Rejected) ] に分類されます。

図 2: SecureX Incident Manager のアラート

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

[承認 (Accepted)] または [拒否 (Rejected)] ボタンを使用して、新しいアラートをいずれかの状態に移動できます。

図 3: アラートの承認または拒否

**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**

グローバル脅威アラートは、拡張された検出や効率的なアラートトリアージなどのコアコンピテンシーに引き続き重点を置いています。現在は SecureX エコシステムとより緊密に統合され、ワンクリックで SecureX のインシデント対応ワークフローへ検出をプロモートします。

アラートを承認すると、SecureX Incident Manager の既存または新しいインシデントにリンクできます。

図 4: インシデントにリンクするオプションでアラートを承認

Accept Alert

Accept and link to a new incident

Title (required)

Response to critical risk alert

Short description (required)

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

Accept and link to existing incidents

Use Lucene syntax to filter incidents

Response to critical risk alert

Accept only

Cancel Accept

SecureX incident manager では、インシデントには、[概要 (Summary)] や、元のアラートからのすべてのセキュリティ [イベント (Events)] と [監視対象 (Observables)] などの詳細が含まれています。その後、調査、エンリッチメント、オーケストレーションといった SecureX の機能を使用して、より詳細に調査して対応することができます。

図 5: インシデントサマリーの例

# 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](#)


図 6: インシデントオブザーバブルの例

## 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

アラートをインシデントとしてプロモートすることが望ましくない場合は、拒否できます。この場合、アラートを拒否した理由をシスコのチームにフィードバックすることもできます。貴重なフィードバックは、ネットワークでの今後の検出を改善に活用されます。

図 7: アラートを拒否してフィードバックを提供

Reject Alert

False Positive

Ignored

Please tell us more about why you made this decision.

Your feedback will help us improve future detections on your network.

Contact me to discuss this feedback

Cancel OK

## 追加の脅威検出

以下の新しい脅威検出をポートフォリオに追加しました。

- IcedID
- Lemon Duck

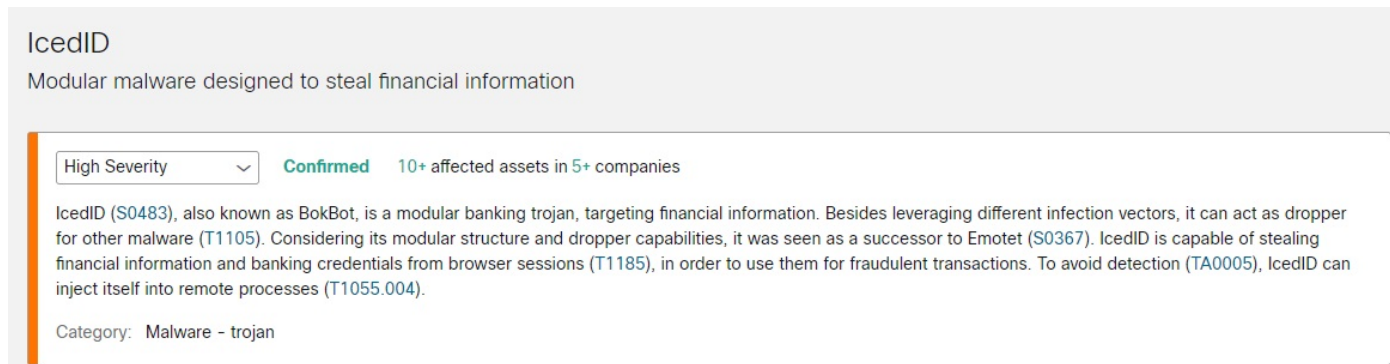
低リスクの脅威検出も多数強化されています。

### IcedID

BokBot とも呼ばれる IcedID ([S0483](#)) は、金融情報を標的とするモジュール型のバンキング型トロイの木馬です。さまざまな感染ベクトルを利用するだけでなく、他のマルウェア ([T1105](#)) のドロップパーとしても機能します。そのモジュール構造とドロップパー機能から、Emotet ([S0367](#)) の後継と見なされていました。IcedID は、不正取引への使用を目的とし、ブラウザセッション ([T1185](#)) から財務情報と銀行のログイン情報を盗むことができます。検出 ([TA0005](#)) を回避するために、IcedID は自身をリモートプロセス ([T1055.004](#)) に挿入できます。

お使いの環境で IcedID が検出されたかどうかを確認するには、[\[IcedID 脅威の詳細 \(IcedID Threat Detail\)\]](#) をクリックして、グローバル脅威アラートで詳細を表示します。

図 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).

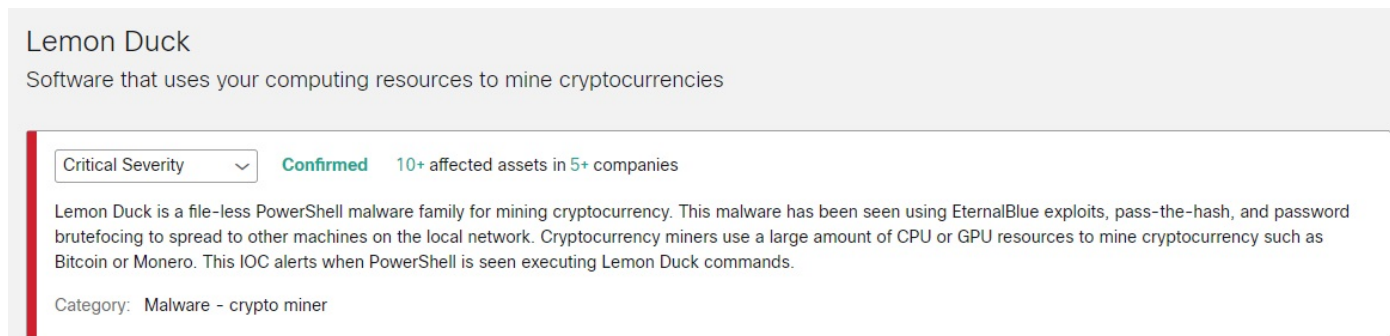
Category: Malware - trojan

### Lemon Duck

Lemon Duck は、暗号通貨をマイニングするためのファイルレス PowerShell マルウェアファミリーです。このマルウェアは、EternalBlue エクスプロイト、pass-the-hash、パスワードブルートフォースを使用して、ローカルネットワーク上の他のマシンに拡散することが確認されています。暗号通貨マイナーは、大量の CPU または GPU リソースを使用して、ビットコインや Monero などの暗号通貨をマイニングします。

お使いの環境で Lemon Duck が検出されたかどうかを確認するには、[\[Lemon Duck 脅威の詳細 \(Lemon Duck Threat Detail\)\]](#) をクリックして、グローバル脅威アラートで詳細を表示します。

図 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





## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。