NICTER Dataset 2024

笠間 貴弘

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研究室　室長

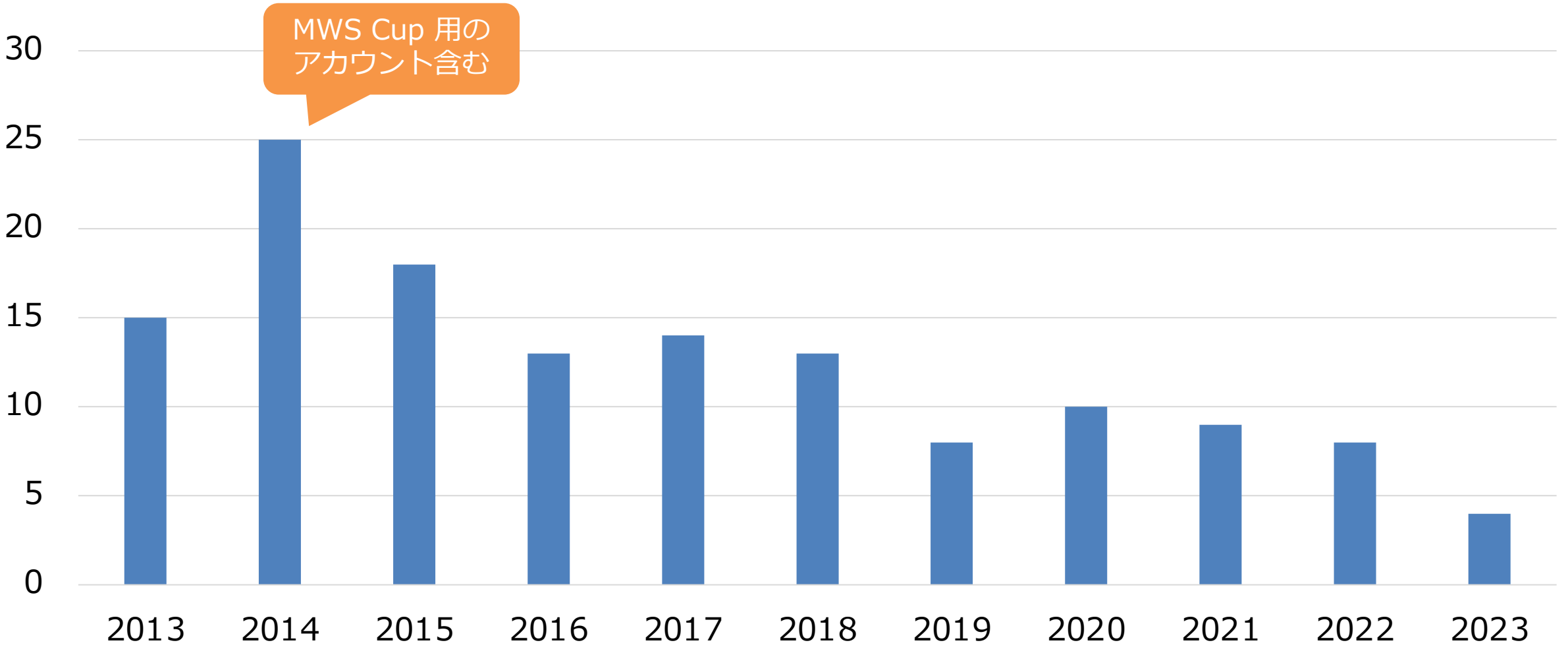
NICT National Institute of Information and Communications Technology

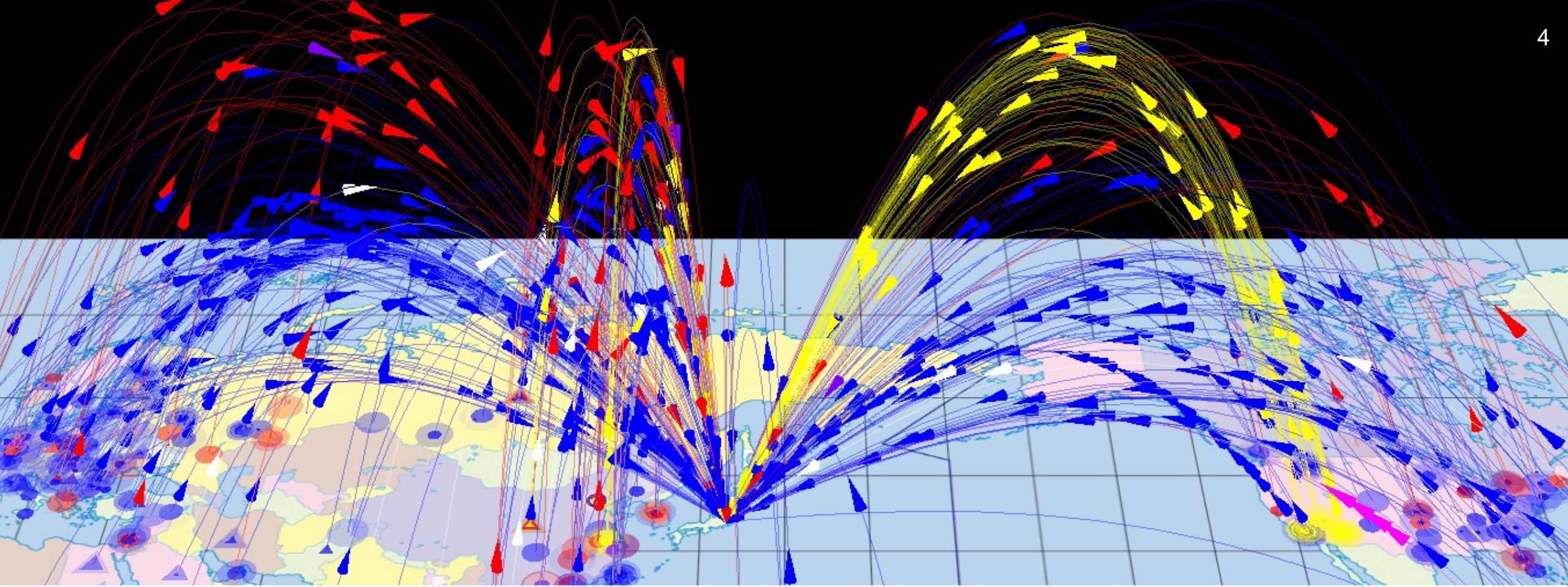
CYBERSECURITY Laboratory

NICTER Dataset は今年で提供開始から12年

MWS Datasets	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
CCC DATAset (CCC)	■	■	■	■	■	■											
MARS for MWS (NICT)	■	■	■														
D3M (NTT研)			■	■	■	■	■	■									
IIJ MITF DATAset (IIJ)					■												
PRACTICE Dataset (Ncom)						■											
PRACTICE(AmpPot) Dataset (YNU)								■									
FFRI Dataset (FFRI)						■	■	■	■	■	■	■	■	■	■	■	■
NICTER Dataset (NICT)						■	■	■	■	■	■	■	■	■	■	■	■
BOS (日立)							■	■	■	■	■	■					
NCD in MWS Cup (MWS)							■										
MWS Cup Dataset (MWS)									■	■	■	■	■	■	■	■	■
Soliton Dataset (ソリトン)											■	■	■	■	■		
Augma Dataset (nao_sec)													■	■			

[参考] NICTER Dataset 利用者数



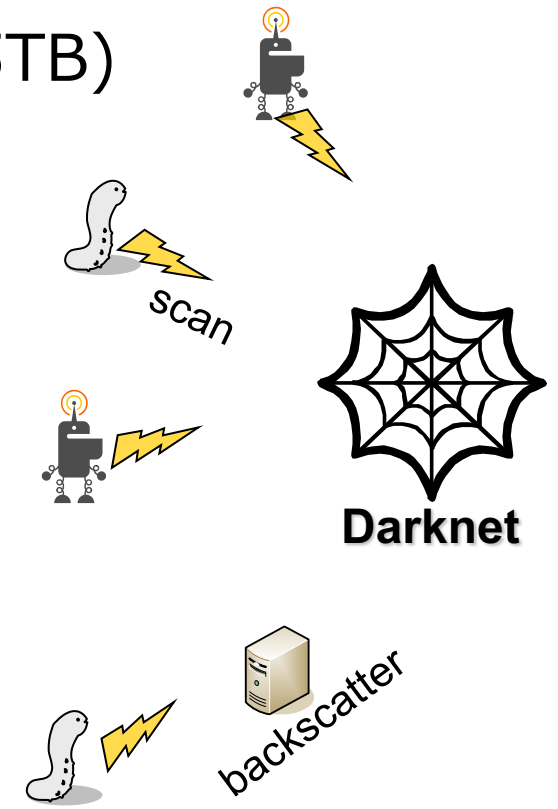


NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム
- 国内外で30万の未使用IPアドレス“**ダークネット**”を観測
- 無差別型サイバー攻撃の大局的な傾向把握に有効

NICTER Dataset 2024

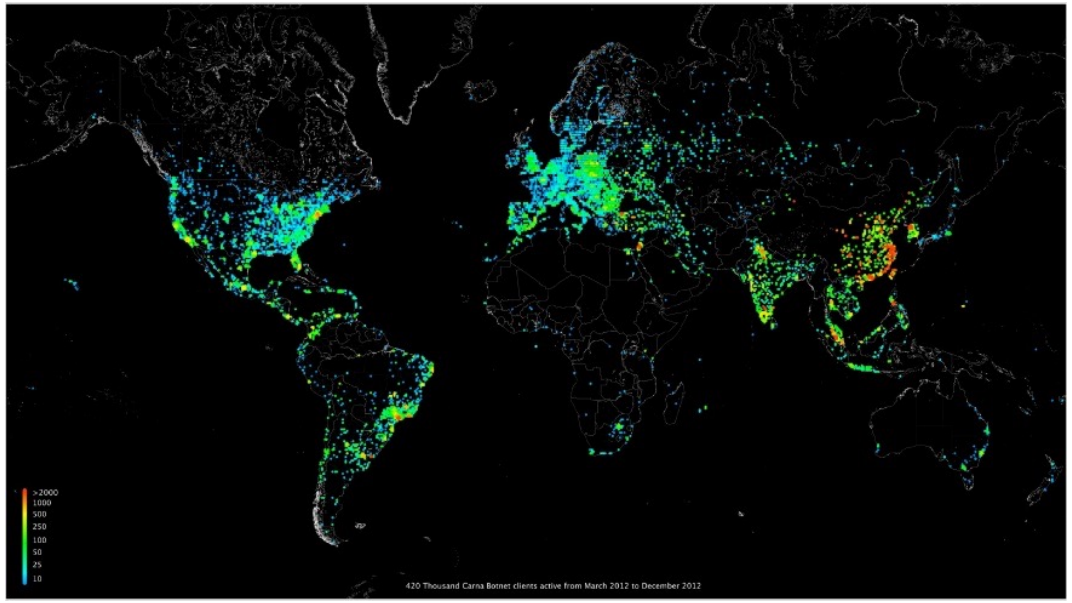
- **未使用のIPアドレス宛に届いたトラフィックデータ**
  - ✓/20(約4,000アドレス)の未使用アドレス(ダークネット)を観測
  - ✓観測は期間は2011年1月1日から現在(約546億パケット, 5TB)
  - ✓独自システムのVM内からアクセス可能(pcap+DB)
- **様々な悪性通信が含まれるデータセット**
  - ✓マルウェア感染機器によるスキャン
  - ✓DDoS攻撃の跳ね返り
  - ✓最近は研究組織や企業による調査スキャンも多数
  - ✓etc.



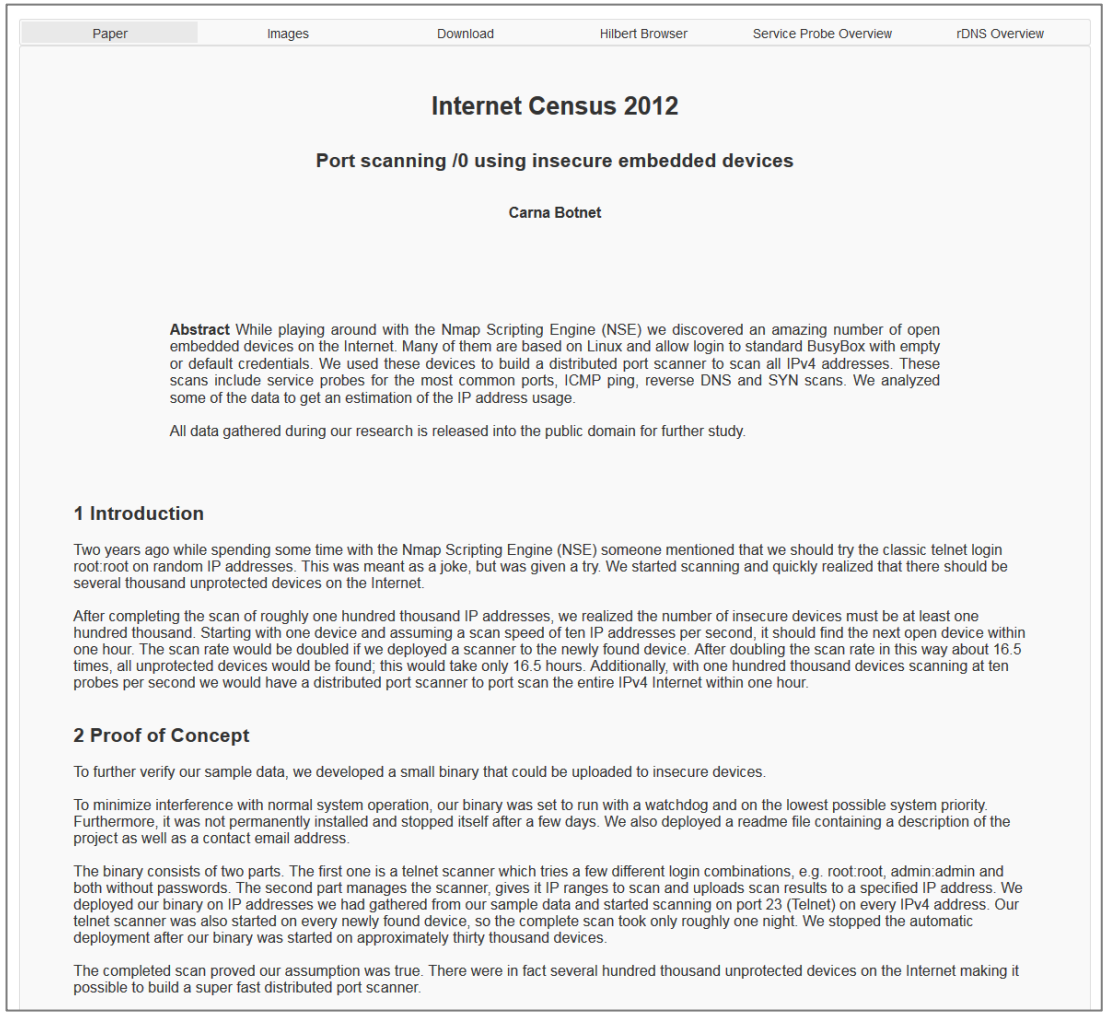
Internet Census 2012

● Carna Botnet

- ✓ Telnet経由で世界中のIoT機器に感染
  (匿名の開発者の報告では約42万台に感染)
- ✓ 開発者は感染機器を用いてインターネット全体に対してインターネットスキャンを行い、その結果をWebサイト上で公開



感染機器の分布



Paper | Images | Download | Hilbert Browser | Service Probe Overview | rDNS Overview

Internet Census 2012

Port scanning /0 using insecure embedded devices

Carna Botnet

Abstract While playing around with the Nmap Scripting Engine (NSE) we discovered an amazing number of open embedded devices on the Internet. Many of them are based on Linux and allow login to standard BusyBox with empty or default credentials. We used these devices to build a distributed port scanner to scan all IPv4 addresses. These scans include service probes for the most common ports, ICMP ping, reverse DNS and SYN scans. We analyzed some of the data to get an estimation of the IP address usage.

All data gathered during our research is released into the public domain for further study.

1 Introduction

Two years ago while spending some time with the Nmap Scripting Engine (NSE) someone mentioned that we should try the classic telnet login root:root on random IP addresses. This was meant as a joke, but was given a try. We started scanning and quickly realized that there should be several thousand unprotected devices on the Internet.

After completing the scan of roughly one hundred thousand IP addresses, we realized the number of insecure devices must be at least one hundred thousand. Starting with one device and assuming a scan speed of ten IP addresses per second, it should find the next open device within one hour. The scan rate would be doubled if we deployed a scanner to the newly found device. After doubling the scan rate in this way about 16.5 times, all unprotected devices would be found; this would take only 16.5 hours. Additionally, with one hundred thousand devices scanning at ten probes per second we would have a distributed port scanner to port scan the entire IPv4 Internet within one hour.

2 Proof of Concept

To further verify our sample data, we developed a small binary that could be uploaded to insecure devices.

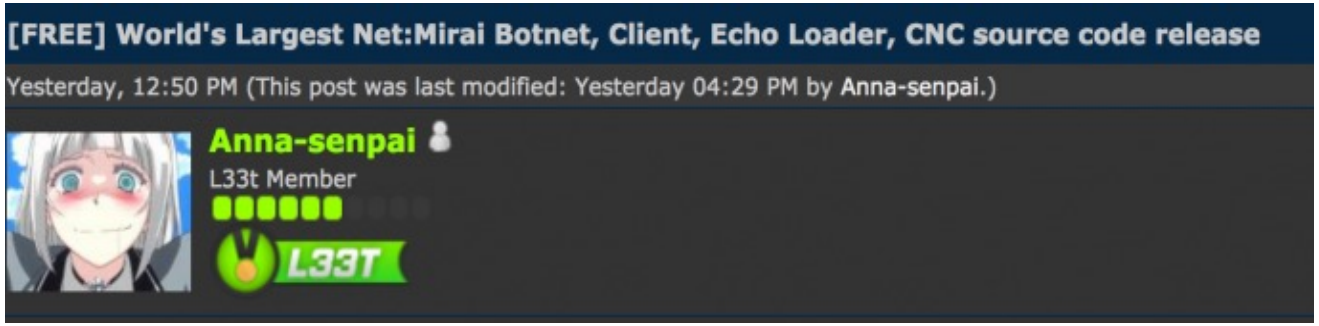
To minimize interference with normal system operation, our binary was set to run with a watchdog and on the lowest possible system priority. Furthermore, it was not permanently installed and stopped itself after a few days. We also deployed a readme file containing a description of the project as well as a contact email address.

The binary consists of two parts. The first one is a telnet scanner which tries a few different login combinations, e.g. root:root, admin:admin and both without passwords. The second part manages the scanner, gives it IP ranges to scan and uploads scan results to a specified IP address. We deployed our binary on IP addresses we had gathered from our sample data and started scanning on port 23 (Telnet) on every IPv4 address. Our telnet scanner was also started on every newly found device, so the complete scan took only roughly one night. We stopped the automatic deployment after our binary was started on approximately thirty thousand devices.

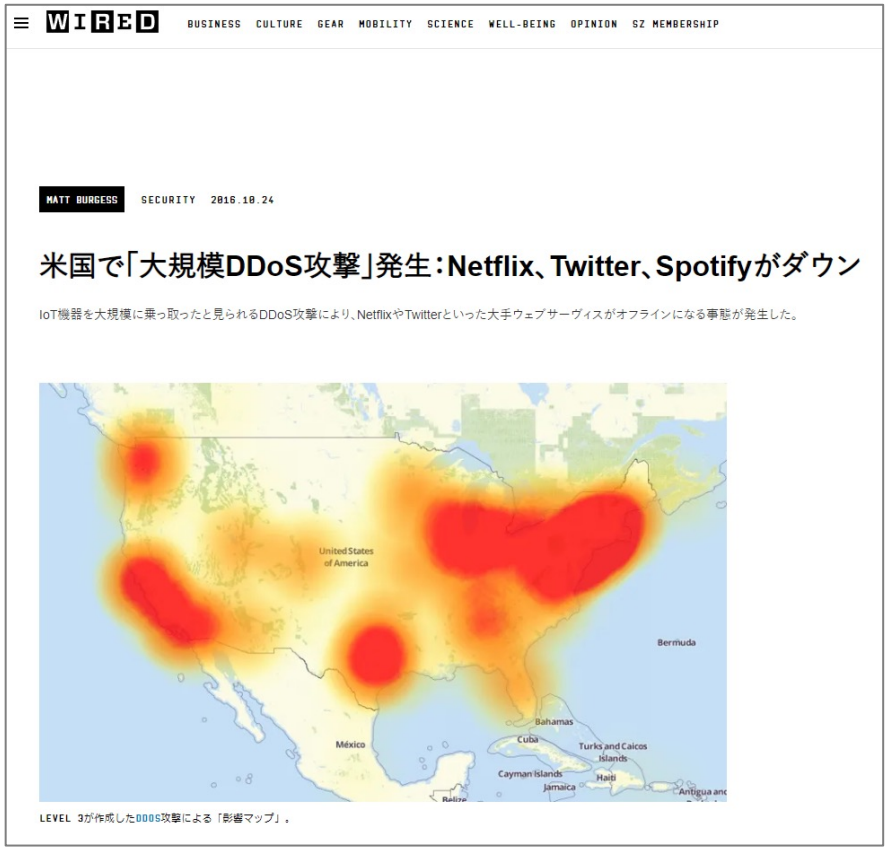
The completed scan proved our assumption was true. There were in fact several hundred thousand unprotected devices on the Internet making it possible to build a super fast distributed port scanner.

IoTマルウェアMiraiによる大規模DDoS攻撃

- **Mirai: 2016年に登場した主に家庭用ルータやWebカメラ等のIoT機器に感染を拡げるマルウェア**
  - ✓ Telnet(23/TCP, 2323/TCP)へのスキャン機能
  - ✓ ID/Passの辞書攻撃による感染機能
  - ✓ 様々なDDoS攻撃機能を持ち**約600Gbps**の攻撃を実行
  - ✓ 海外掲示板でソースコードが公開される
  - ✓ 2017年12月に容疑者3名が罪状を認めた
    (FBIへの各種捜査協力で実刑は免れた)



ハッカーフォーラムへの開発者の投稿



https://wired.jp/2016/10/24/internet-down-dyn-october-2016/

NICTダークネット観測オペレーション (2022年頃)

データの自動集計

前日のデータを送信元ホスト毎に集計（深夜、毎時）
- GRE
- SYN-ACK
- 大量パケット送信元（Herder追跡）

＋

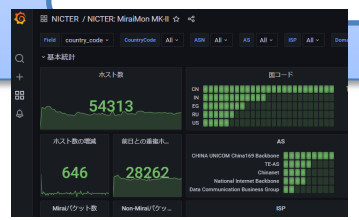
データエンリッチメント

外部データ収集（Hagure、Cure、外部ソース）
バナー収集
機器判定、Bot判定
Hadoopプラットフォーム上で横断分析

＋

可視化

推移をグラフ化しSlackに投稿
Grafanaで可視化
GoogleDataPortalで可視化



毎朝
トリアージ

- ダークネット観測データを元に国内の具体的な感染機器を特定し、速やかに機器を入手
- ファームウェア解析、脆弱性検証からゼロデイ脆弱性を発見し、ベンダー調整の上公開　（2022年度 公開実績1件、公開予定2件）

機器調査・Bot調査

- **ファームウェア解析**
- **脆弱性検証**
  （w/AA-T、ローレイヤ-T）
- **実機ハニーに繋いで in the wildの攻撃を観測**

ダウンロードサーバ監視

プロトタイプシステムを開発し運用中
- 検体の移り変わりを把握
- VTにあがっていない検体を捕獲

マルウェア解析

Joesandboxで動的解析
アーティファクト分析チーム

Output

インシデントレスポンス（JPCERT/CC）

脆弱性報告（IPA）

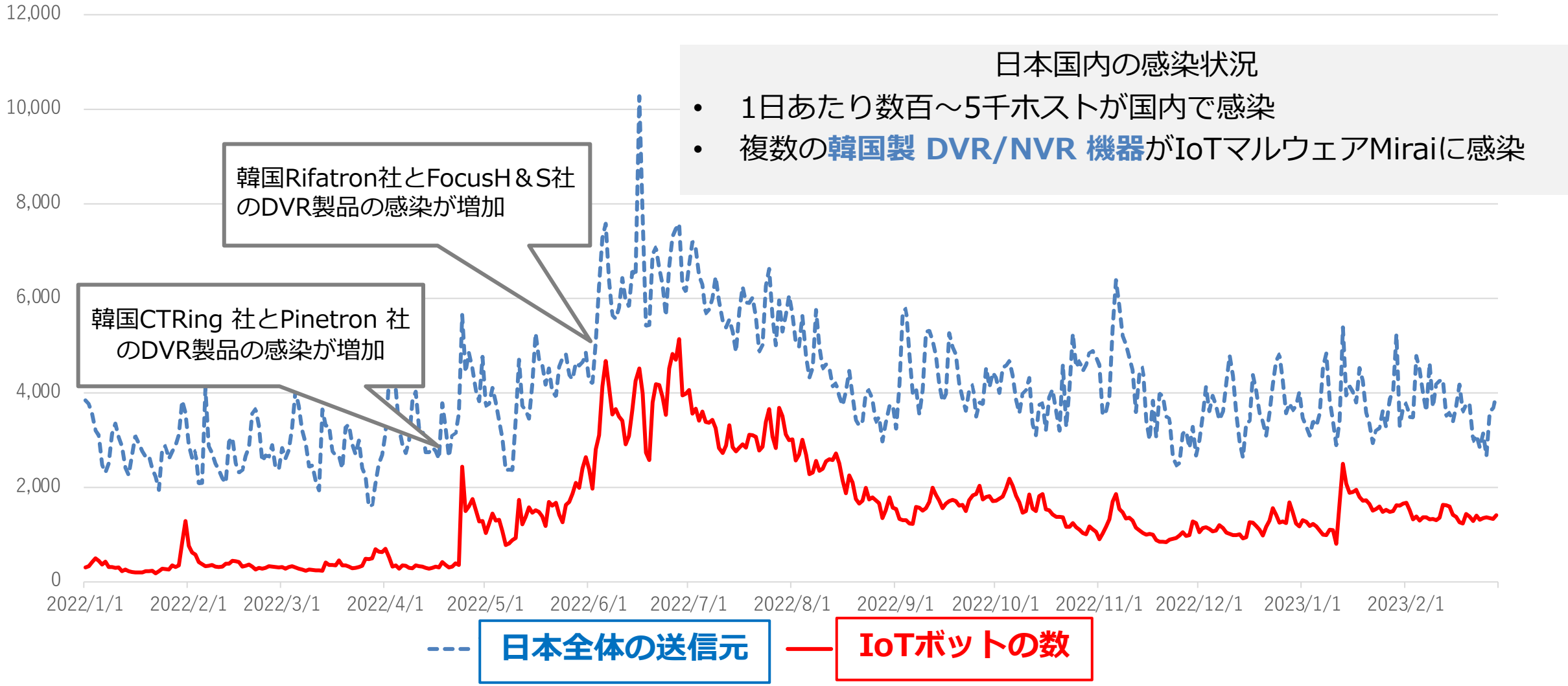
ベンダー調整（機器の国内販売元等）

関連機関との情報共有
- SIGMON、DoS-WG、NISC、総務省

外部情報発信
- Twitter、Blog、観測レポート

（2022年）

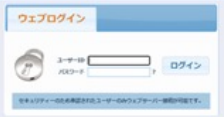
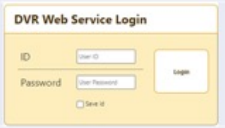
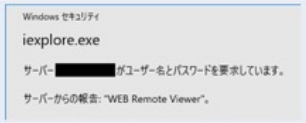
韓国OEM製DVR/NVR製品の脆弱性(1/2)



国内の感染機器の観測統計(2022年～2023年)

韓国OEM製DVR/NVR製品の脆弱性(2/2)

- **国内で販売されている5社8機種の韓国製機器をNICTで調査**
  - ✓ **7機種にメンテナンス用バックドア**（未公開の脆弱性）を確認
  - ✓ そのうち**4社の製品のバックドアが実際に攻撃者によって悪用**されていた
  - ✓ 脆弱性[1,2,3]をベンダに報告し、ファームウェアの修正に協力

製造元	筐体（一例）	管理ログイン画面
FocusH&S		
Rifatron		
Pinetron		
CTRing		
ITX		

脆弱性を発見した韓国製DVR/NVR

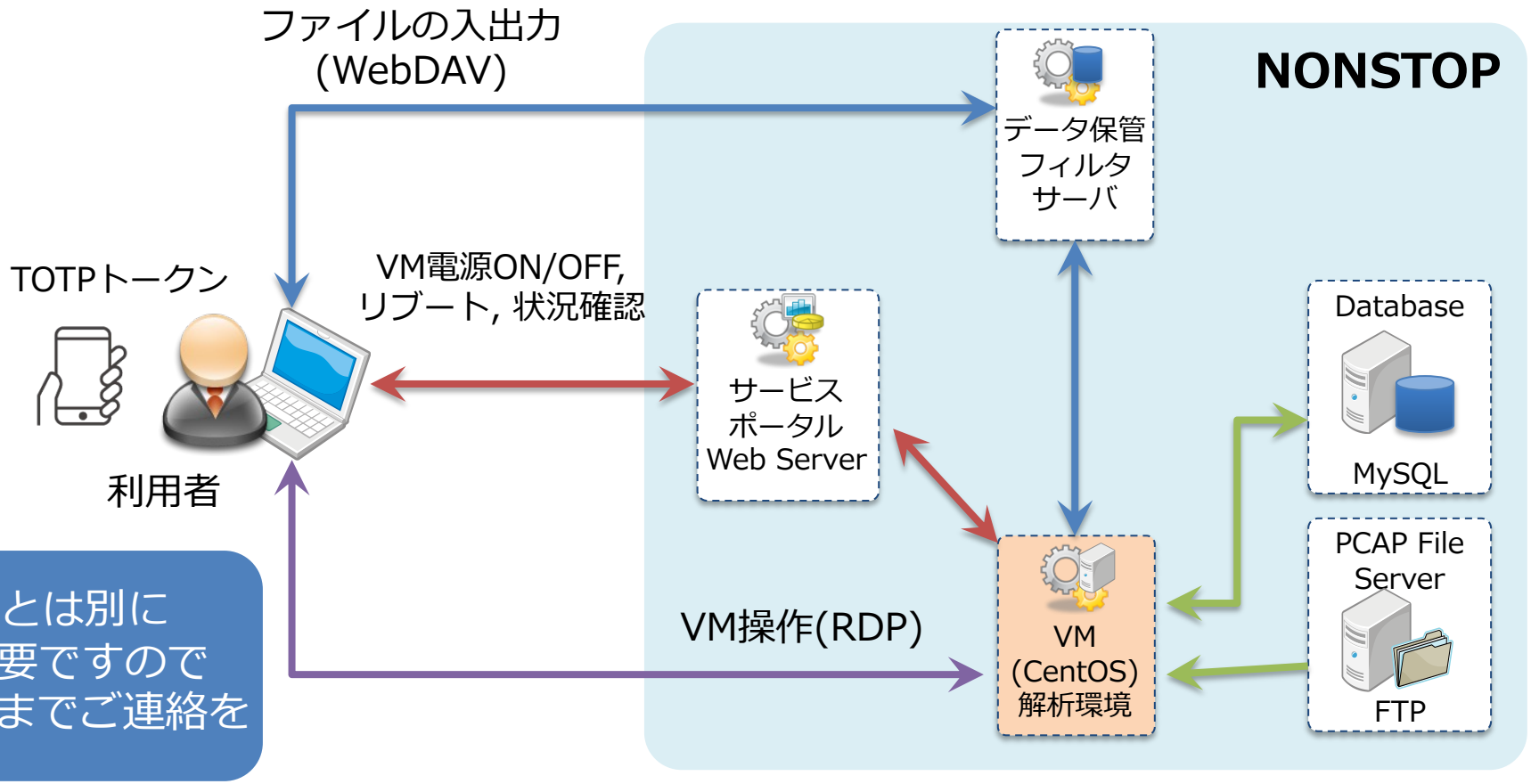
[1] JVNDB-2022-002337 ユニモテクノロジー製デジタルビデオレコーダにおける重要な機能に対する認証の欠如の脆弱性
https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002337.html

[2] JVNDB-2022-002768 ユニモテクノロジー製デジタルビデオレコーダにおける複数の脆弱性
https://jvndb.jvn.jp/ja/contents/2022/JVNDB-2022-002768.html

[3] JVNDB-2023-002055 ケービデバイス製デジタルビデオレコーダにおける複数の脆弱性
https://jvndb.jvn.jp/ja/contents/2023/JVNDB-2023-002055.html

NICTER DatasetはNONSTOP上で提供

- セキュリティ研究情報を遠隔から安全に利用してもらうための環境



データセット利用契約とは別に
NONSTOP利用申請が必要ですので
nontop@ml.nict.go.jp までご連絡を

[参考] 観測結果は NICTERWEB 等でも一般公開

NICTERWEB

Home Atlas Cube Stats Top10 Report NICTER Blog About Us English

Top10

<<前月 2023年6月 次月>>

日	月	火	水	木	金	土
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

CSVファイルをダウンロード（一日毎）：2023/06/26

CSVファイルをダウンロード（一月毎）：5月 4月 3月

※カレンダーの日付を選択して一日毎のCSVファイルをダウンロード可能

2023/06/26のデータを表示中

国別ユニークホスト数 Top10

国名（国コード）	ホスト数	割合
中国（CN）	35,454	15%
インド（IN）	23,799	10%
ベネズエラ（VE）	22,647	10%
アメリカ（US）	15,569	7%
エジプト（EG）	13,411	6%
ロシア連邦（RU）	10,083	4%
イラン（IR）	9,255	4%
ブラジル（BR）	9,150	4%
メキシコ（MX）	6,296	3%
韓国（KR）	6,155	3%

TCP 宛先ポート別ユニークホスト数 Top10

宛先ポート	ホスト数	割合
23	103,983	3%
445	38,156	1%
80	30,824	1%
8080	29,632	1%
2323	18,931	1%
60023	17,419	1%
52869	14,907	< 1%
81	8,163	< 1%
5555	7,185	< 1%
22	6,504	< 1%

UDP 宛先ポート別ユニークホスト数 Top10

宛先ポート	ホスト数	割合
64884	11,639	10%
56042	7,473	6%
161	3,005	3%
5060	2,126	2%
5353	2,091	2%
1900	2,076	2%
6881	1,817	2%
11211	1,628	1%
500	1,609	1%
8000	1,572	1%

NICTER Blog

ABOUT TAGS NICTER WEB

DVR 機器への感染を狙う攻撃の観測

Posted on 2022-10-20 | Yoshiki Mori, Yurina Takase

はじめに

本記事では，IoT機器を攻撃対象とするDDoS ボットへの感染活動のうち，韓国の FocusH&S が製造する防犯カメラ用デジタルビデオレコーダー（以下DVR）を狙った攻撃の観測結果を紹介します．

FocusH&S 社は DVR の製造を行う韓国の企業です． 本調査では，国内販売代理店の一つであるユニモテクノロジー株式会社から販売されていた機器およびファームウェア（Ver.2.0.19.1）を用いて脆弱性の調査や実機に対する攻撃観測を行いました．

マルウェアに悪用された当該機器の脆弱性 (CVE-2022-35733) はすでに修正済みで，販売元であるユニモテクノロジー株式会社からも脆弱性情報[1]と修正済みファームウェア[2]が公開されています．当該機器のユーザは速やかにファームウェアアップデートを適用してください．

脆弱なDVR機器に対する攻撃の実態

発見に至った経緯

NICTでは，ダークネット宛にパケットを送信してきたホストを日々調査しています．FocusH&S 社製 DVR は 2019年に Mirai に感染した韓国国内のホストとして観測していましたが，当時はホスト数が少なく，感染機器の特定には至らず，その後は経過観察の状況が続いていました． しかし，2022年の4月以降，日本国内において FocusH&S 社製 DVR を含む，Mirai に感染した韓国製の DVR 機器が目立つようになりました． そこで，日本で販売されている DVR 製品の取扱説明書を収集して調査したところ機器の特定に至り，

宣伝(1) IEEE DSC 2024

- **IEEE DSC 2024 が 11月6-8日に東京日本橋で開催されます**
  - ✓ **https://attend.ieee.org/dsc-2024/**

- **論文投稿締切：2024年7月18日**
  - ✓ IEEEフォーマット 2カラムで8ページ
  - ✓ 学生の国際会議投稿に最適
  - ✓ 採録論文はIEEEから出版

- **その他**
  - ✓ Experience and Practice Trackや ポスターセッションなども予定
  - ✓ 例年のDSCよりも参加費は半額程度(予定)

宣伝(2) NICTの採用情報

- **サイバーセキュリティ研究室では人材を絶賛募集中**
  - ✓研究員：6名、研究技術員：9名、RA：5名
- **様々なキャリアパス**
  - ✓博士卒採用
  - ✓修士卒採用後に博士課程進学
  - ✓RAから研究員/技術員
- **興味がある人はぜひ**

https://csri.nict.go.jp/careers.html

まとめ

- **NICTER Dataset は変わらず提供12年目に突入**
  - ✓ご利用に興味のある方はMWS Dataset利用のための契約締結後に、NICT 笠間(nonstop@ml.nict.go.jp) までご連絡ください
  - ✓2023年度に利用していた方も継続利用を希望される場合はご連絡ください(連絡が無い場合はどこかのタイミングでアカウントを停止します)

- **MWS Dataset 提供期間 ≒ NICTER Dataset提供期間**
  - ✓大規模データ観測は途中で止めないことが重要
  - ✓独自のデータを持っていることは大きなアドバンテージ