NICTER Dataset 2023

MWS2023プレミーティング(2023/6/29)

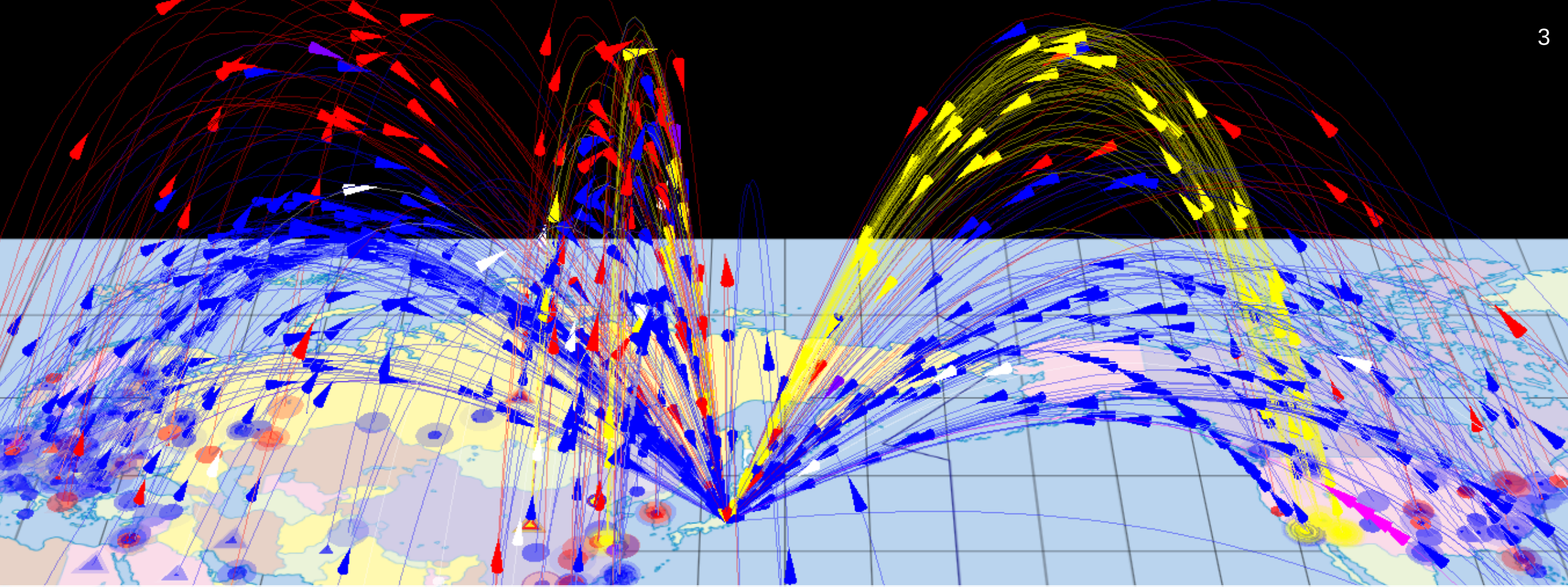
国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室

NICT National Institute of Information and Communications Technology

CYBERSECURITY Laboratory

MWS Dataset の変遷

MWS Datasets	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
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)													■	■		

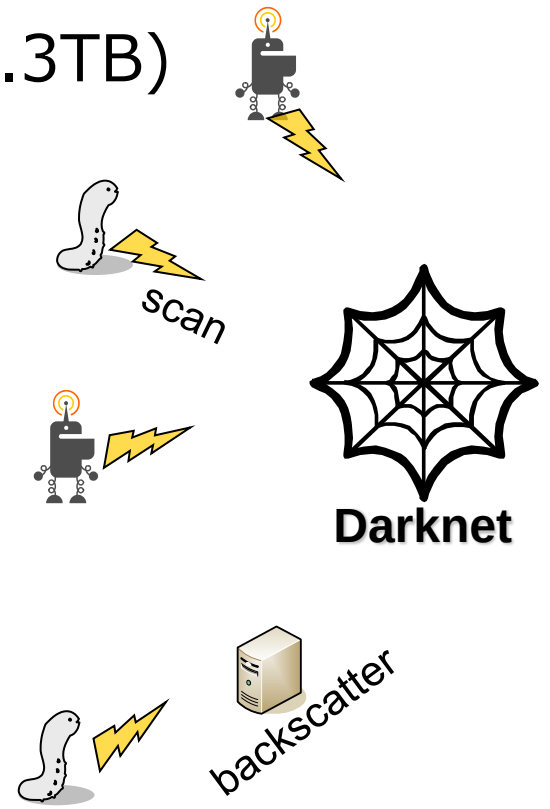


NICTER

- 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

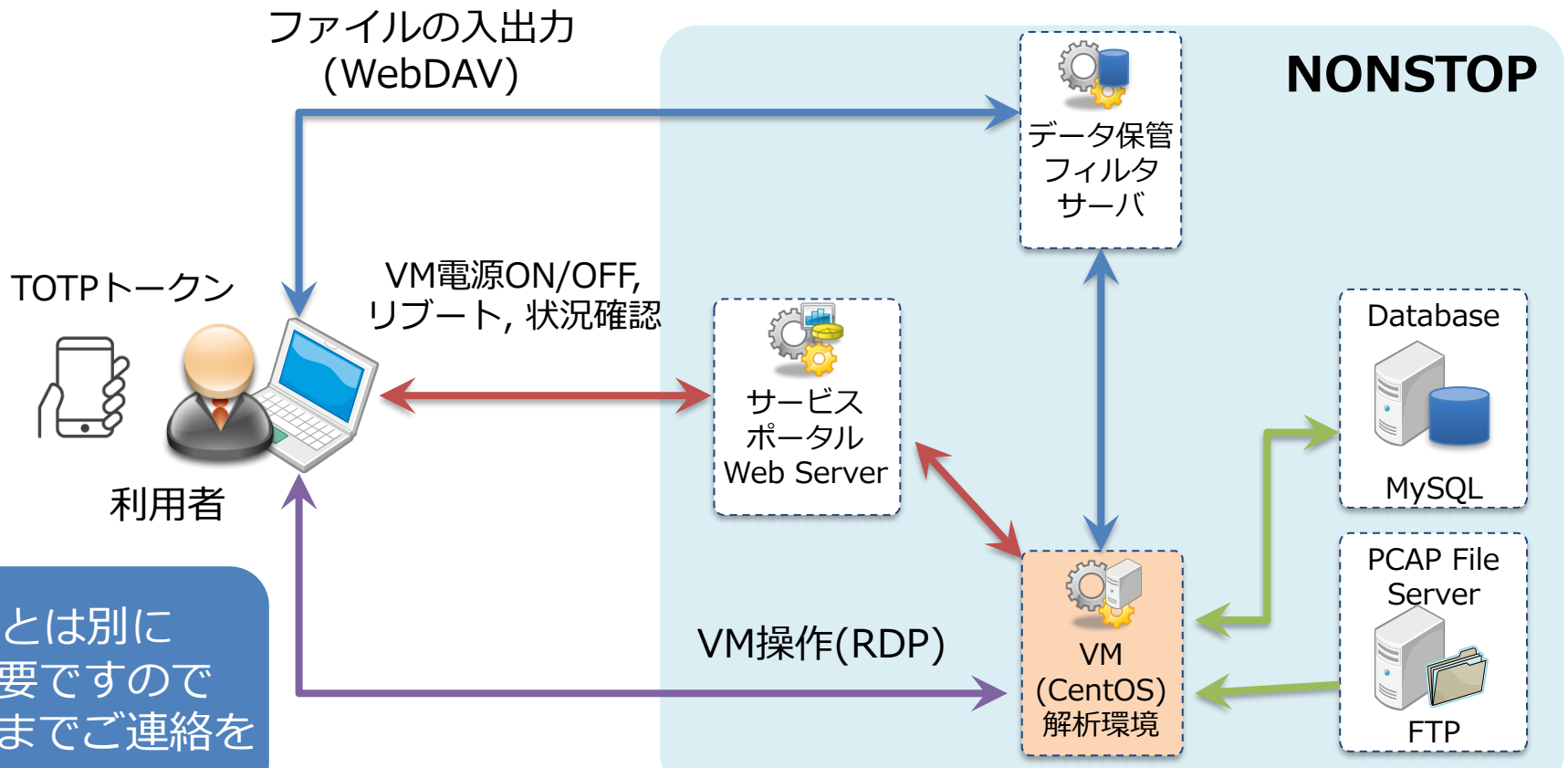
NICTER Dataset 2023

- **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4000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450億パケット, 8.3TB)
  - ✓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い
  - ✓etc.



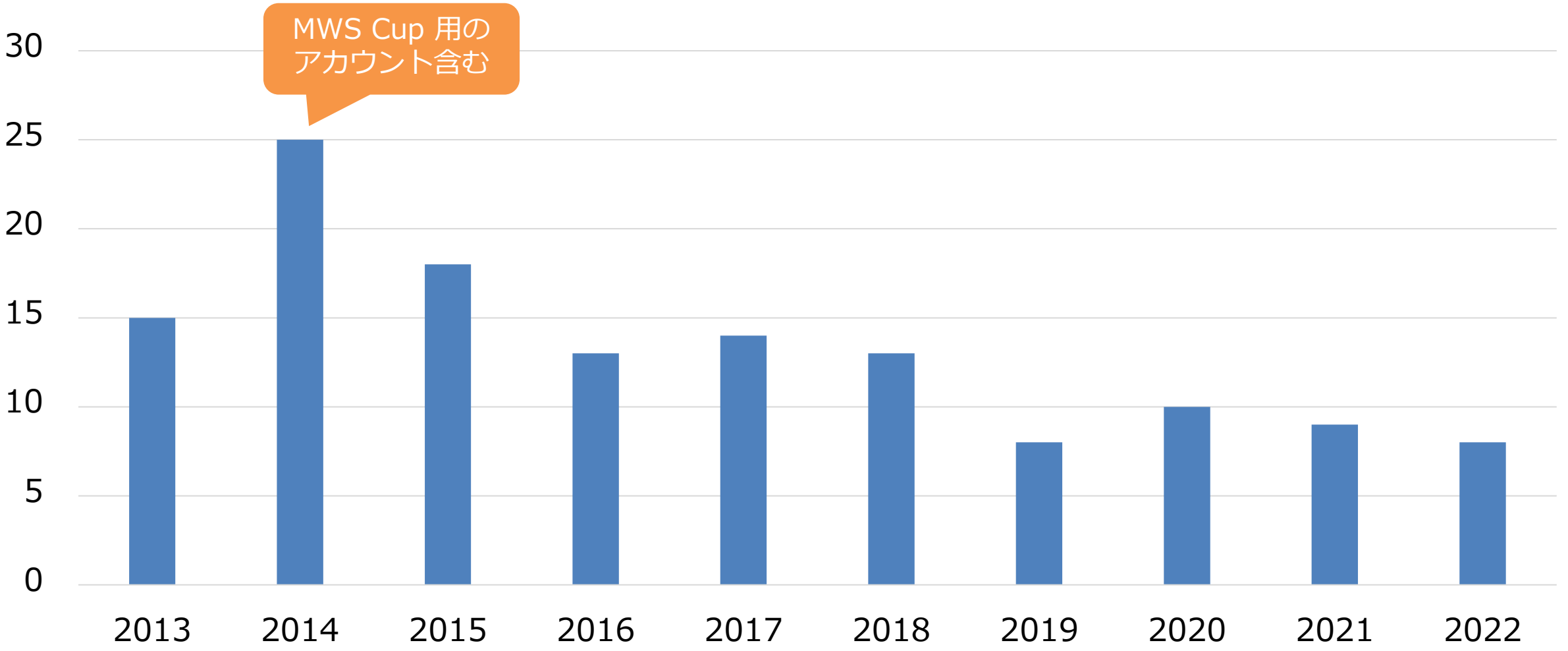
NICTER DatasetはNONSTOP上で提供

- 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] NICTER Dataset 利用者数



[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，

まとめ

- **NICTER Dataset は変わらず提供11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
  - ✓2022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 の更新は続くよどこまでも？**
  - ✓FFRI Dataset との一騎打ち次第？
  - ✓我々はMWS Dataset とは関係なくデータを集めているということもあり、基本的に続く限りは協力する想定ではいます