
IoT Cybersecurity Now and Future

Katsunari Yoshioka
Yokohama National University

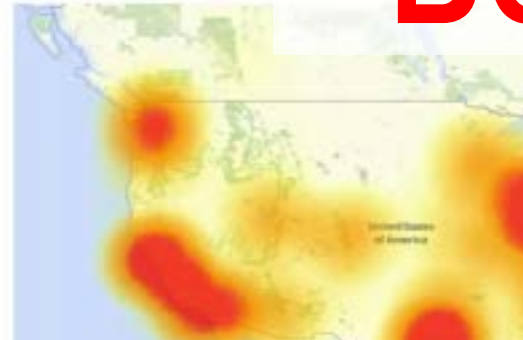
A part of this research was conducted in "MITIGATE" project among "Research and Development for Expansion of Radio Wave Resources(JPJ000254)", supported by the Ministry of Internal Affairs and Communications (MIC), Japan. A part of this research was conducted in "WarpDrive" project, supported by National Institute of Information and Communications Technology, Japan. A part of this research was supported by National Institute of Information and Communications Technology, Japan (05201).

How an army of vulnerable gadget web today

Malware known as Mirai is targeting the smart home

By Nick Statt | @nickstatt | Oct 21, 2016, 4:10pm EDT

f t SHARE



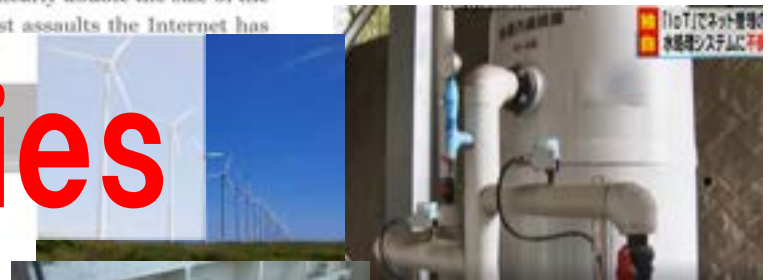
Botnet & DDoS



21 KrebsOnSecurity Hit With Record DDoS

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at Akamai, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

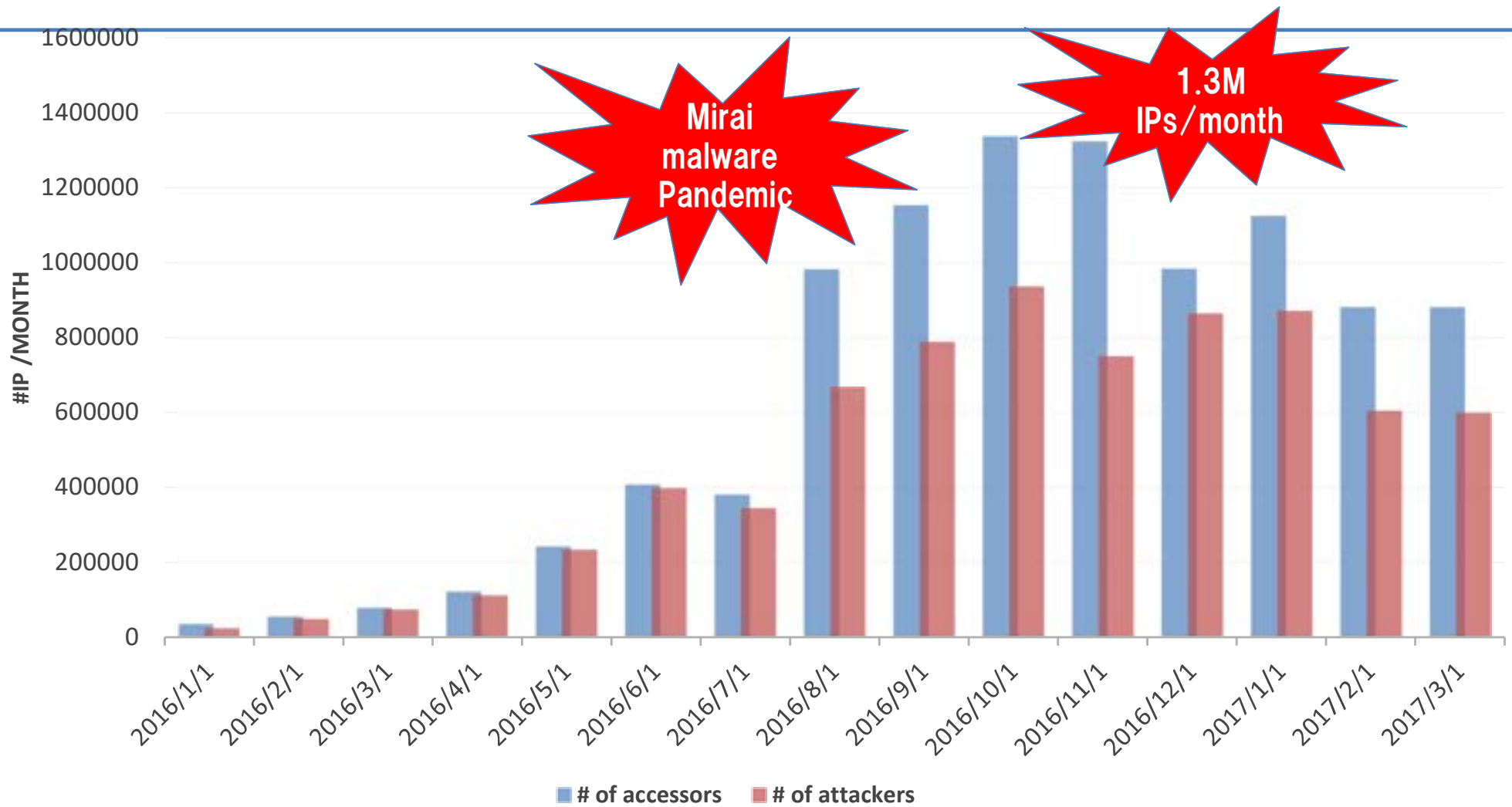
Targeted Facilities



Insecure Cameras

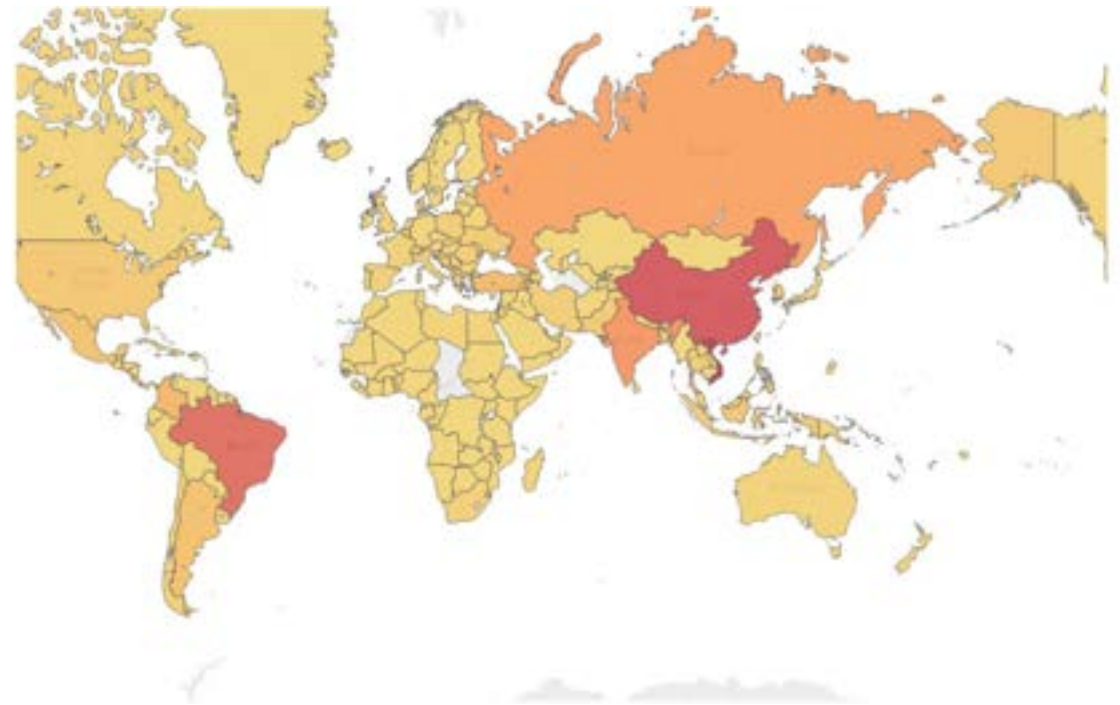
Industrial Control Systems

Mirai pandemic in 2016








Mirai pandemic in 2016

- Attacks from **Over 200 countries/regions**
- Especially **Asian and South American countries** had many infected devices



Categories of compromised devices observed by honeypot

- **Surveillance camera**
 - IP camera
 - DVR
 - **Network devices**
 - Router, Gateway 
 - Modem, bridges
 - WIFI routers 
 - Network mobile storage 
 - Security appliances
 - **Telephone**
 - VoIP Gateways
 - IP Phone
 - GSM Routers
 - Analog phone adapters
 - **Infrastructures**
 - Parking management system
 - LED display controller
- Devices are inferred by telnet/web banners

- **Control system**
 - Solid state recorder
 - Sensors
 - Building control system (bacnet)
- **Home/individuals**
 - Web cam, Video recorders
 - Home automation GW
 - Solar Energy Control System 
 - Energy demand monitoring system 
- **Broadcasting**
 - Media broadcasting
 - Digital voice recorder
 - Video codec
 - Set-top-box,
- **Etc**
 - Heat pump
 - Fire alert system
 - Medical device (MRI)
 - Fingerprint scanner

Variants, variants, variants...

- Early IoT attacks targeted Telnet service
- Recently, we found 68 different vulnerabilities were exploited by IoT malware

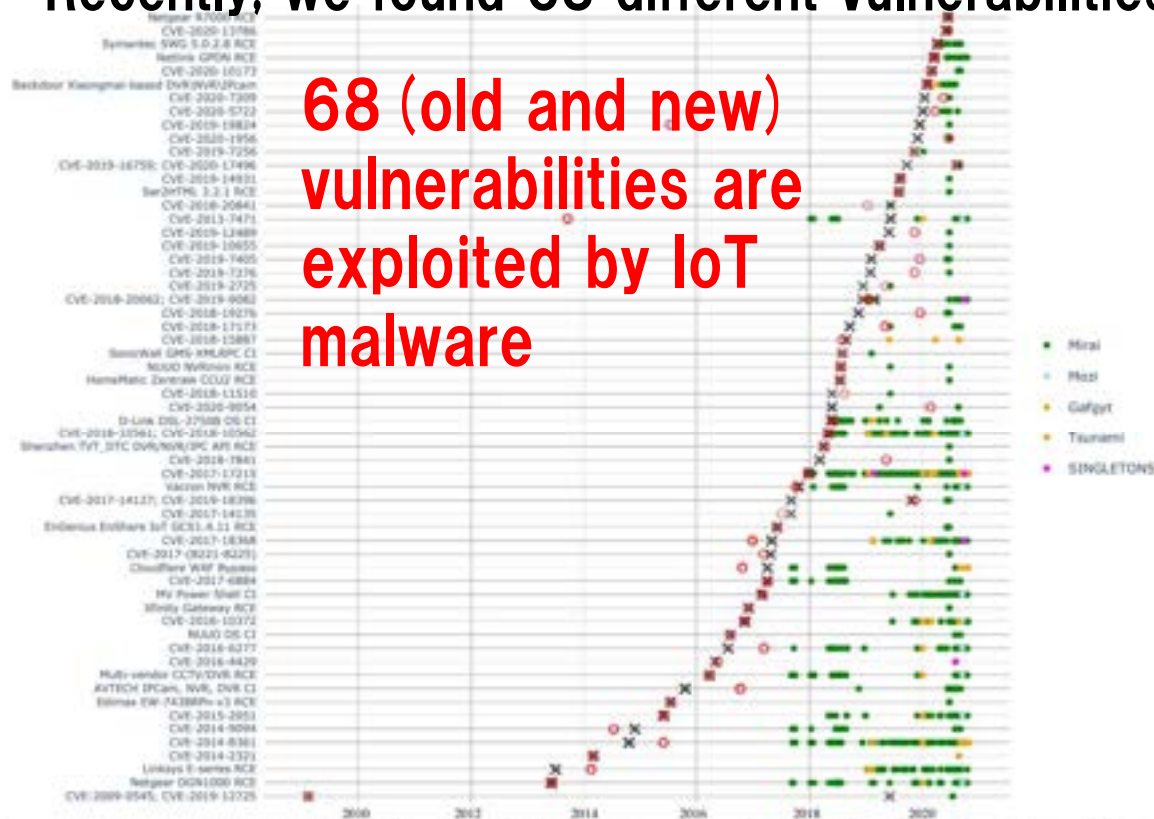
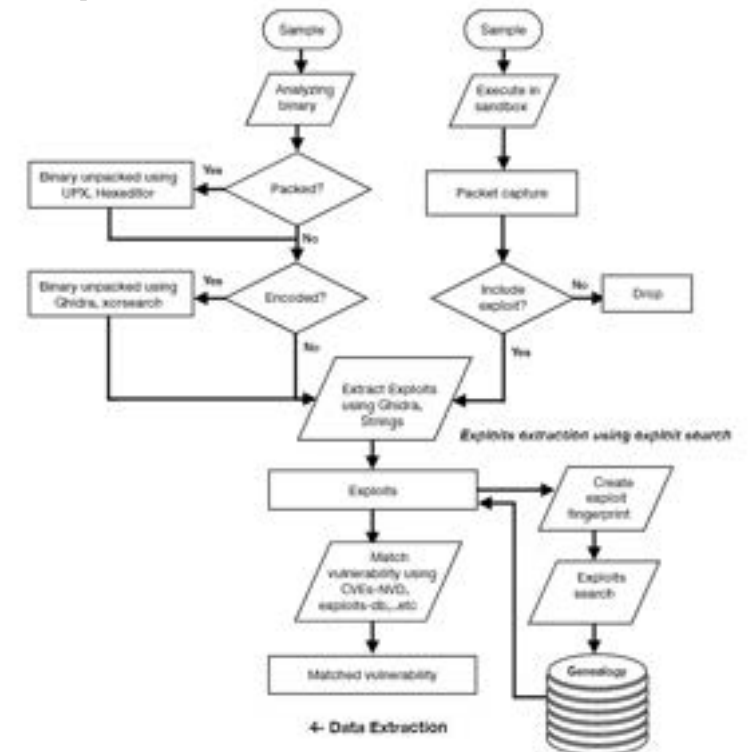


Figure 3: Occurrence of binaries that exploit vulnerabilities, per IoT malware family, ordered by vulnerability publication date. Each line represents a unique exploit. It might attack more than one vulnerability. The X symbol highlights the time the vulnerability was first published whereas the O symbol highlights the time the exploit was first discovered.



Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.

IoT Ransom Attack!

We developed bare-metal NAS (Network Attached Storage) honeypot to observe ransom attacks.

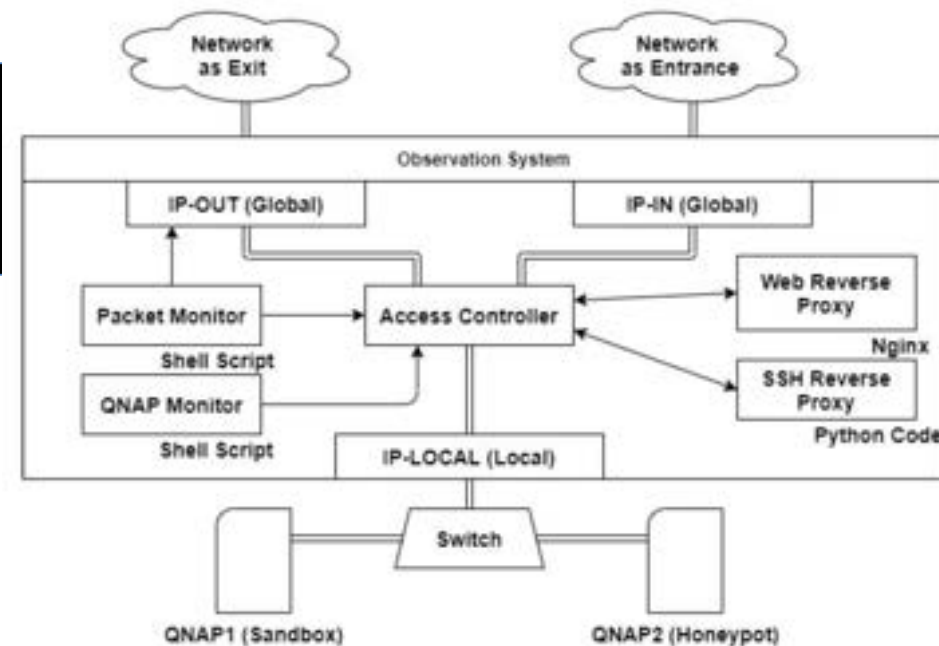
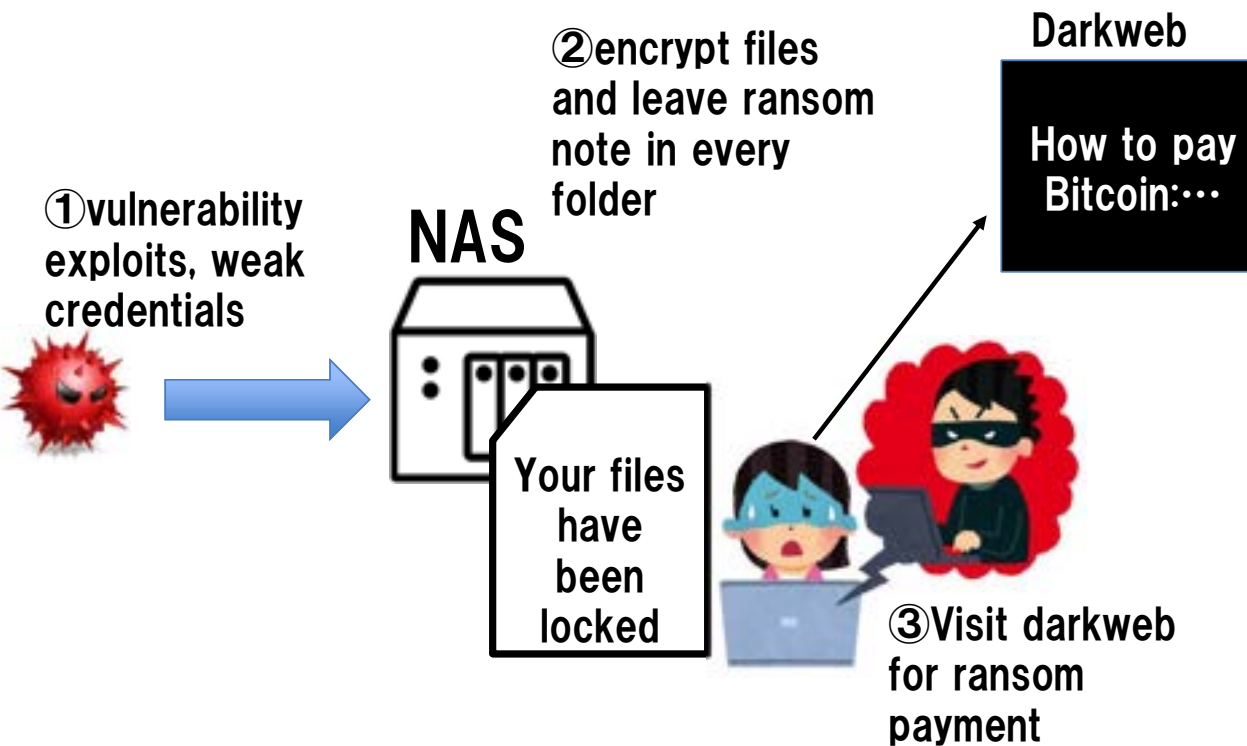


Fig. 1. Structure of SPOT

Ransom notes

名前	更新日時	種類	サイズ
[REDACTED]	2021/03/24 4:26	ENCRYPT ファイル	4,499 KB
[REDACTED]	2021/03/24 4:26	ENCRYPT ファイル	4,715 KB
[REDACTED]	2021/03/24 4:26	ENCRYPT ファイル	4,351 KB
README_FOR_DECRYPT.txtt	2021/03/24 4:26	テキストファイル	1,100 B
1.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
2.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
3.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	5,857 KB
4.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
5.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
6.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
7.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
8.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
9.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
0.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
1.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
2.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
3.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
4.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
5.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
6.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
7.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
8.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB
9.jpg.encrypt	2021/03/24 4:26	ENCRYPT ファイル	4,703 KB

← Leaves ransom note in every folder so that it can be easily found by the victims

README_FOR_DECRYPT.txtt - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

All your data has been locked(rypted).
How to unlock(decrypt) instruction located in this TOR webs
Use TOR browser for access .onion websites.
<https://duckduckgo.com/html?q=tor+browser+how+to>

Payment instruction sites on darkweb



Instructions
on how to use
crypto
currency to
pay ransom



eCh0raix order page

!!!HOT!!! Discount 30% for ALL! !!!HOT!!!


*The discount is valid from 2021-11-19 to 2021-11-26

Status: **Waiting Payment...**


All your data has been stolen and locked(rypted).

If you want decrypting your files send **0.03** BTC(bitcoin)

New price with discount BTC(bitcoin)

to this address: 

Or use QR code













is and

Exposed Network Cameras!

<http://insecam.org/>

World online live cameras directory Axis Panaso cameras Sitemap by cities

United States(6593)	 United States(3144)
Japan(3626)	 Japan(1487)
Italy(1315)	 Korea, Republic Of(959)
France(1119)	 Taiwan, Province Of (907)
Netherlands(1036)	 Italy(663)
Russian Federation(577)	 Germany(600)
United Kingdom(506)	 Russian Federation(557)
Germany(491)	 France(462)
Canada(406)	 Austria(241)
Korea, Republic Of(403)	 Czech Republic(240)
Sweden(367)	
Spain(360)	
Switzerland(336)	
Czech Republic(289)	
Mexico(279)	
Austria(266)	
Norway(232)	
Taiwan, Province Of (206)	
Belgium(180)	

City
Kitchen
Sport
Cofeehouse
Service
Entertainment
Interesting
Village
Server
Religion
Mall
Square
Barbershop
Airline
Animal
Warehouse
Bar
River
Beach

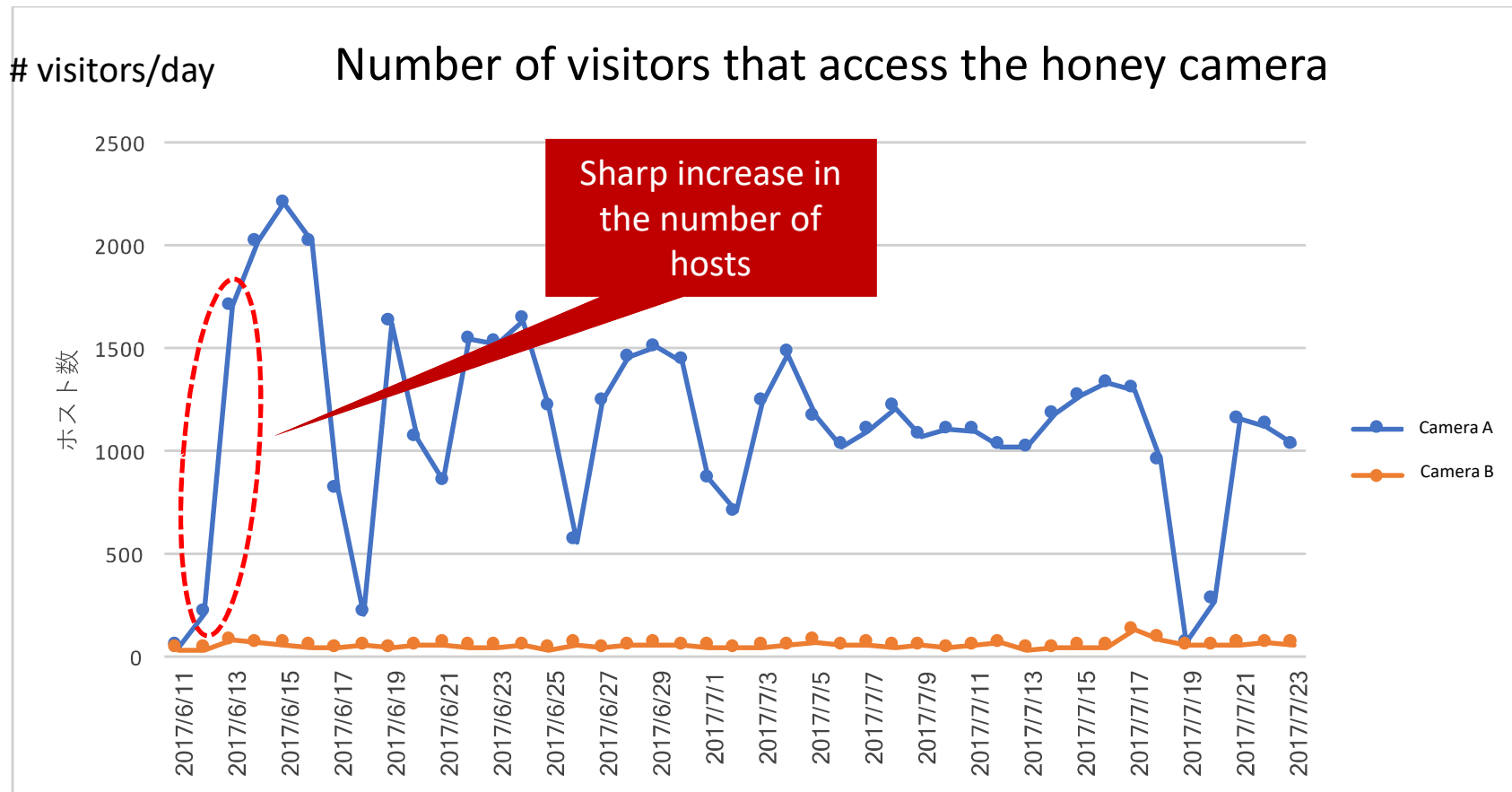
Honeypot of exposed cameras



From NHK news, 2018/1/26



Observation results of honey camera



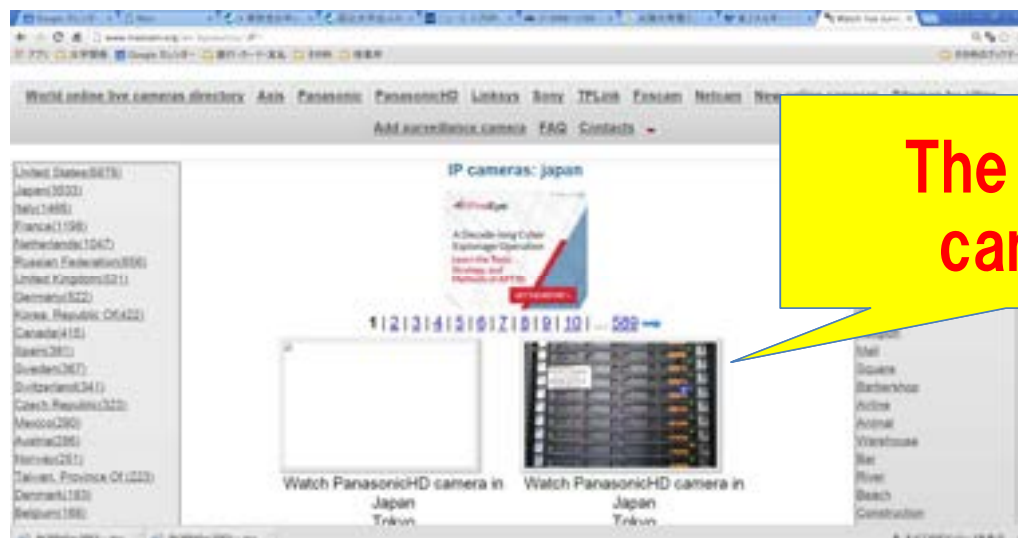
The honeycam was on Insecam...

- Many accesses via insecam were observed

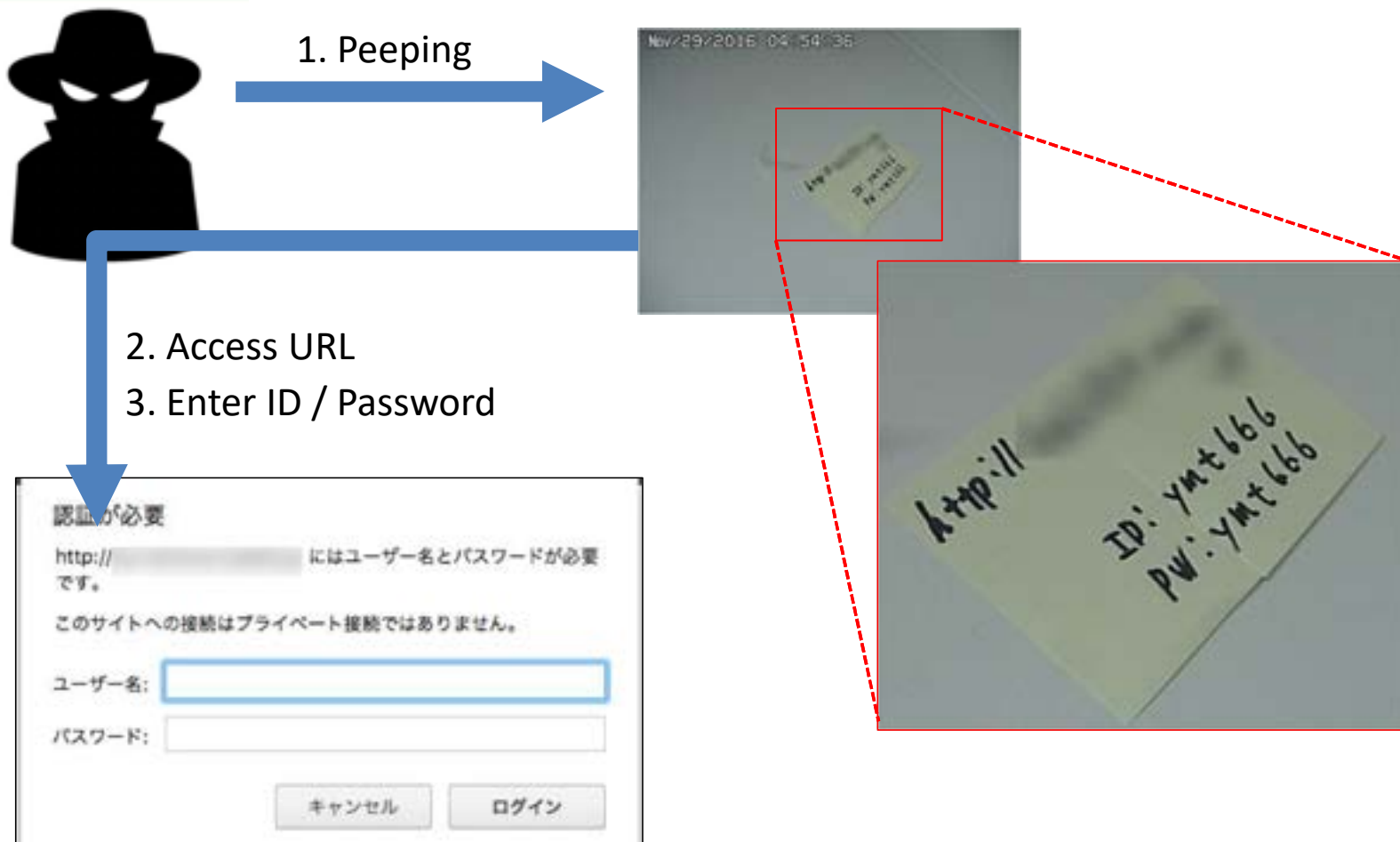
```
GET /xxxxxxx/xxxxx?resolution=640&amp;quality=1&amp;  
Language=0&amp;COUNTER HTTP/1.1  
Referer: http://www.insecam.org/en/bycountry/JP/?page=4
```

- We confirmed that honey camera was indeed registered to insecam

Peeps jumped to more than 20,000 times per day after the inclusion in Insecam page



Observing the misuses of credentials



Access to the URL with bait credentials

Host that sent the request	Access host using domain of URL	Login challenge host	Host that entered ID/password displayed on camera A
583	422	235	217

- Observed access to the bait URL from 422 IP addresses
 - ➔ Humans are watching images of cameras
- 217 IP address entered ID / password displayed on camera A
 - ➔ Some peepers go “beyond peeping” (login challenge)

Kazuki Tamiya, Aamir H. Bokhari, Yuta Ezawa, Sou Nakayama, Ying Tie, Rui Tanabe, Akira Fujita, Katsunari Yoshioka, Tsutomu Matsumoto, "Dangers of IP Camera . An Observational Study on Peeping," Journal of Information Processing, 2020

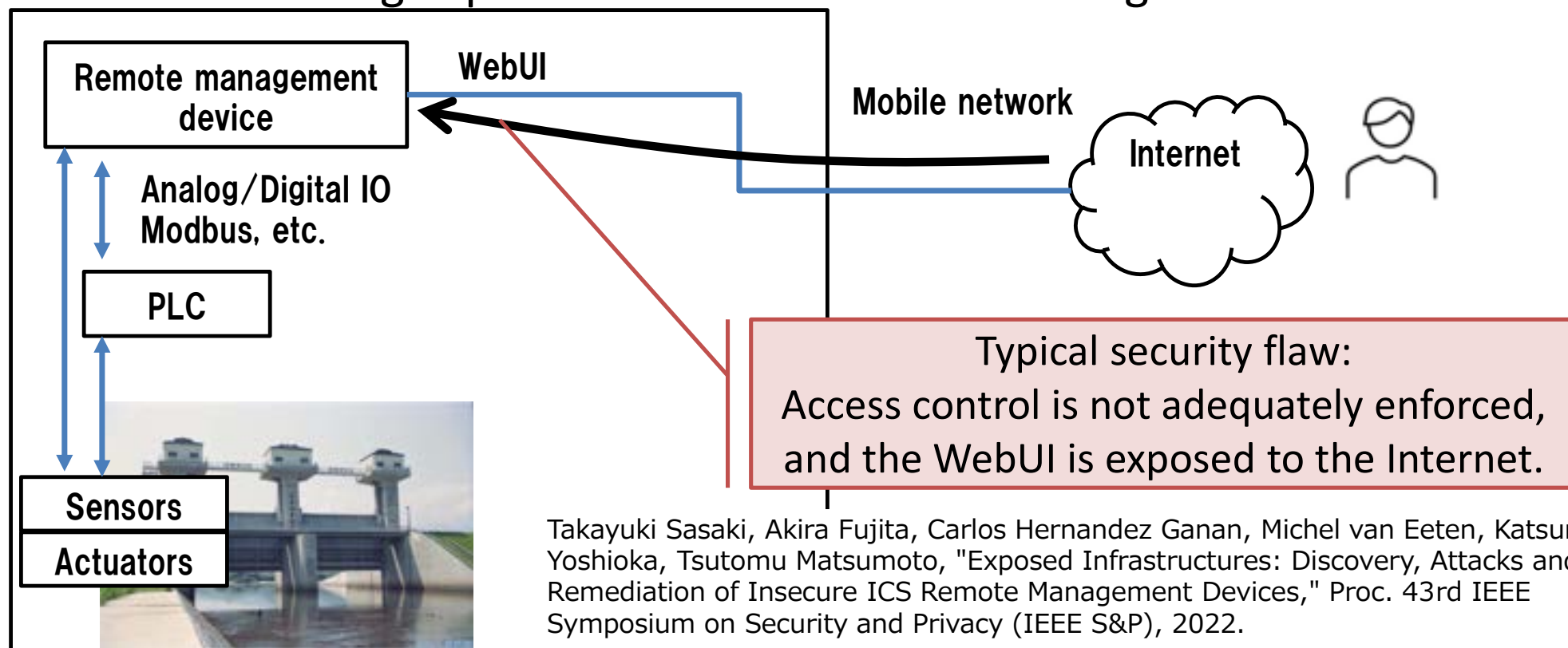
Camera operated by attackers



Critical Systems!

Remote management devices are used for infrastructures such as water facilities, power plants, and factories.

We focus on detecting exposed WebUIs of remote management devices.



A dimly lit control room with multiple computer workstations and a large wall of monitors. The room features several desks with blue chairs, each equipped with a computer monitor. In the background, a long wall is covered with numerous smaller monitors displaying various data and maps. The overall atmosphere is professional and technical.

Example Case:
Waterworks Monitoring System



Example Case:
River Gate

A photograph of a railway track with a train in the distance, overlaid with the text "Example Case: Railway Signaling". The image shows a complex railway infrastructure with multiple tracks, overhead power lines, and signal masts. A white train is visible in the distance on the left track. The text is centered over the image in a white serif font.

Example Case:
Railway Signaling



Case:

Power Substation

Are these insecure facilities
actually targeted?


Honey Facilities!



Image of Data logger
Model number of Data logger



Critical infra system does attract attackers!

	#visitors per IP per Day	Average # commands	Average duration of visit [s]
 <p>NHK NEWS WEB</p> <p>河川カメラに不正アクセス 別のサイバー攻撃に悪用か</p> <p>ただいま調整中です。</p> <p>複数の専門家 “機器のセキュリティのぜい弱性つかれ ウイルスに感染など「乗っ取り」の被害の可能性。”</p>		6.01	400
		2.08	134
		3.04	178
<p>NHK news on 2023/3/4 reporting IP cameras for river monitoring system being compromised</p>			5.4



Post on hacking forum attracts attackers (and security experts)

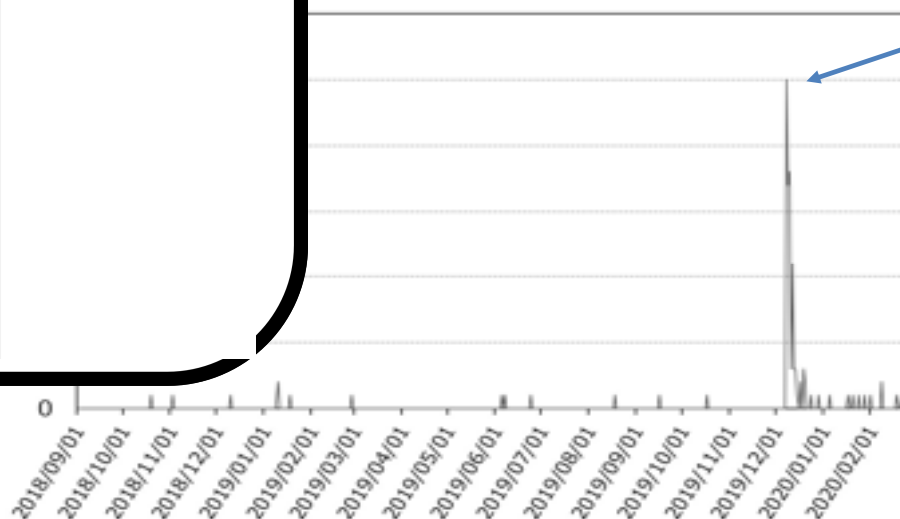
Yokohama Air Control Tower
by L0gg1n - December 08, 2019 at 02:16 AM

L0gg1n



December 08, 2019

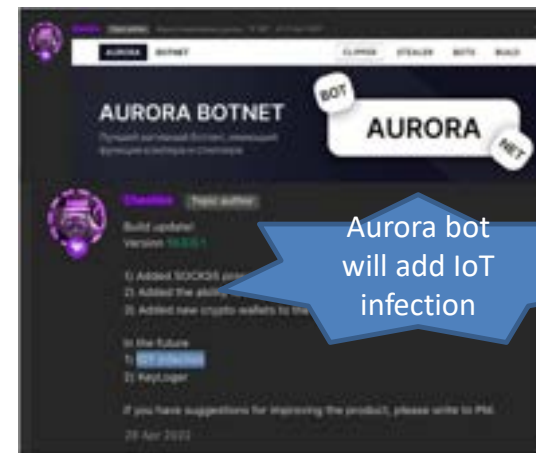
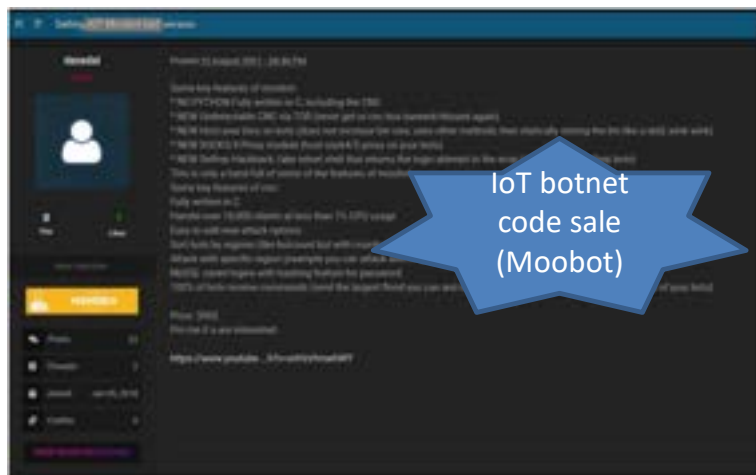
Event
Launch of honeypot
New thread on the honeypot facility in hacking forum
Attacks jump up (login challenges increased)
Notification from security vendor
Notification from anonymous expert
Notification from JPCERT/CC



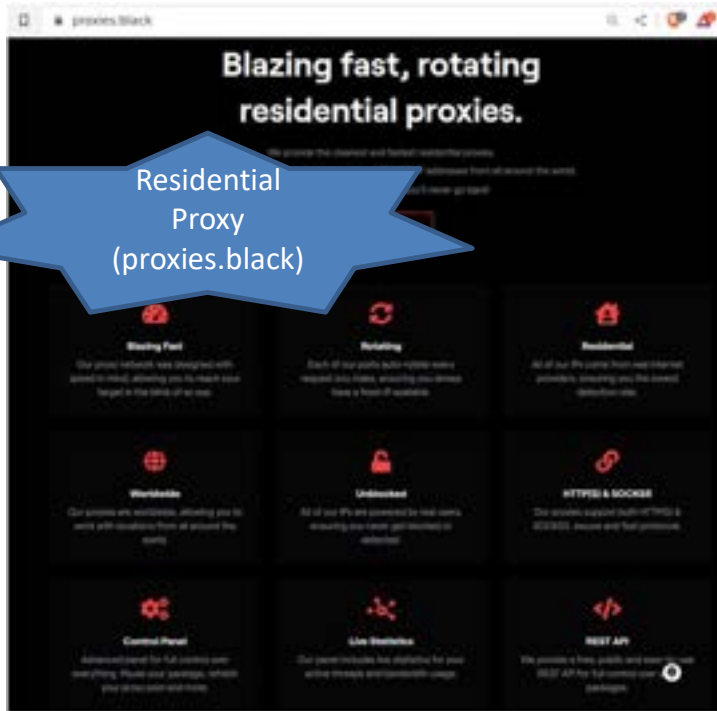
Attacks jump up after a new thread on a honeypot facility started

Cybercrime as a service

IoT Botnet (DDoS, etc)

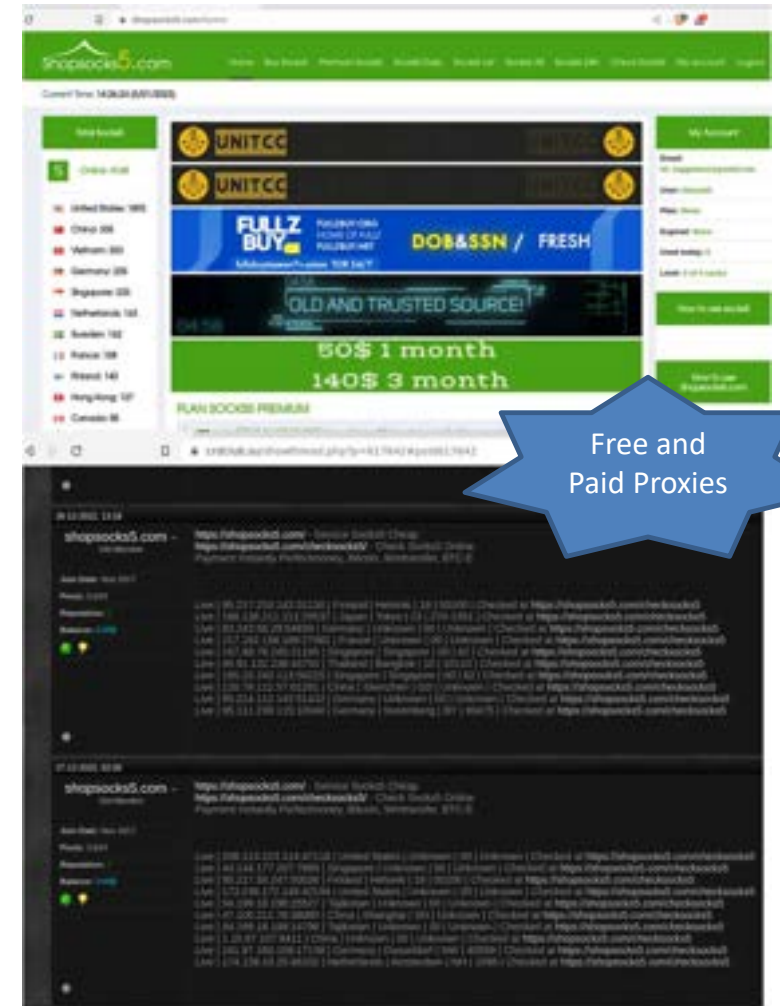


IoT Proxy (selling hacked devices as proxies)



Residential Proxy (proxies.black)

- Proxies.black
 - Popular among intruders
 - Forum says IoT devices
 - I did experiment
- Shopsocks5.com
 - So many free proxies are shared in the hacker forums
 - We can check it too



Free and Paid Proxies

Summary

- Insecurity of IoT devices has been already exploited for years. The trends likely continue as attackers are aware of this fundamental insecurity coming from diversity and complex supply chains in the IoT industries.
- Cyber attacks on IoT devices are (and will be) a part of cyber crime business.
- In warfare, cyber attacks are conducted as weapons (e.g., sweeper in Ukraine). We observe massive continuous reconnaissance over the network, which would increase their impact.

Thank you!

Katsunari Yoshioka, Ph.D
Yokohama National University

yoshioka@ynu.ac.jp
<http://yoshioka.ynu.ac.jp/>

For more, please visit:

IoT POT: Honeypot for Revealing IoT Cyber Threats
<https://sec.ynu.codes/iot>

References:

Takayuki Sasaki, Akira Fujita, Carlos Hernandez Ganan, Michel van Eeten, Katsunari Yoshioka, Tsutomu Matsumoto, "Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices," 43rd IEEE Symposium on Security and Privacy, 2022.

Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022.

Seiya Kato, Rui Tanabe, Katsunari Yoshioka, Tsutomu Matsumoto, "Adaptive Observation of Emerging Cyber Attacks targeting Various IoT Devices," IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021.

Rui Tanabe, Tatsuya Tamai, Akira Fujita, Ryoichi Isawa, Katsunari Yoshioka, Tsutomu Matsumoto, Carlos Ganan and Michel Van Eeten, "Disposable Botnets: Examining the Anatomy of IoT Botnet Infrastructure," Proc. International Conference on Availability, Reliability, and Security (ARES2020), 2020.

Kazuki Tamiya, Aamir H. Bokhari, Yuta Ezawa, Sou Nakayama, Ying Tie, Rui Tanabe, Akira Fujita, Katsunari Yoshioka, Tsutomu Matsumoto, "Dangers of IP Camera . An Observational Study on Peeping," Journal of Information Processing, 2020

O. Cetin, C. Ganan, L. Altena, D. Inoue, T. Kasama, K. Tamiya, Y. Tie, K. Yoshioka, M. van Eeten, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," The Network and Distributed System Security Symposium (NDSS 2019), 2019.

Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoT POT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Vol. 57, No. 4, 2016.

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoT POT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.