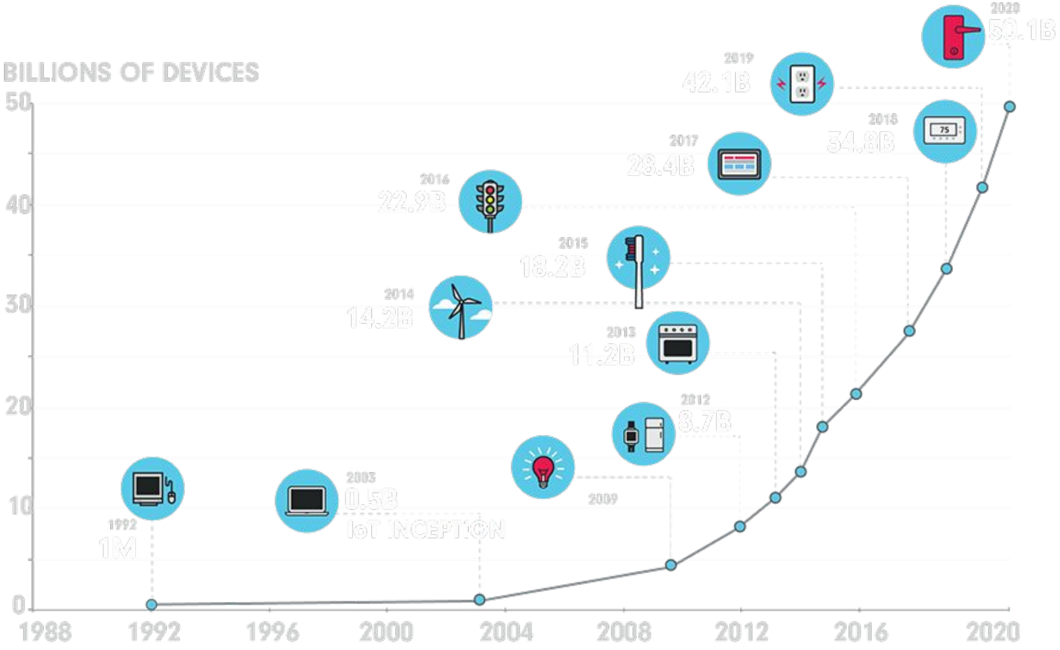
Examining Mirai’s Battle over the Internet of Things

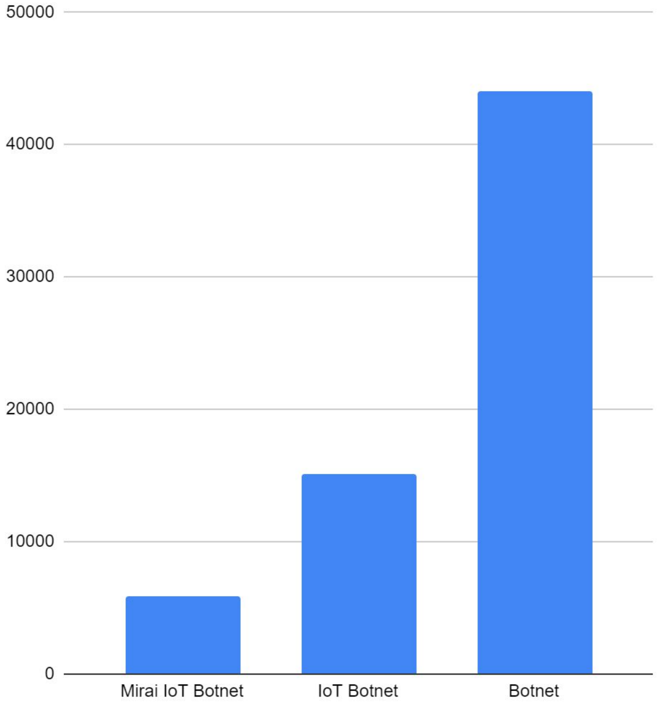
COMPSCI 726 Seminar
presented: Nicholas Berg
date: 2021-10-04
original work: Griffioen and Doerr (2020)

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                    // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                          // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                          // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                      // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                      // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);                  // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);                  // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);              // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                      // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                          // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);      // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                              // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);          // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                              // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                          // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                              // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                          // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                              // root     pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);      // admin    admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                              // root     1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);          // admin    smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                          // admin    1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                      // root     666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);              // root     password
```

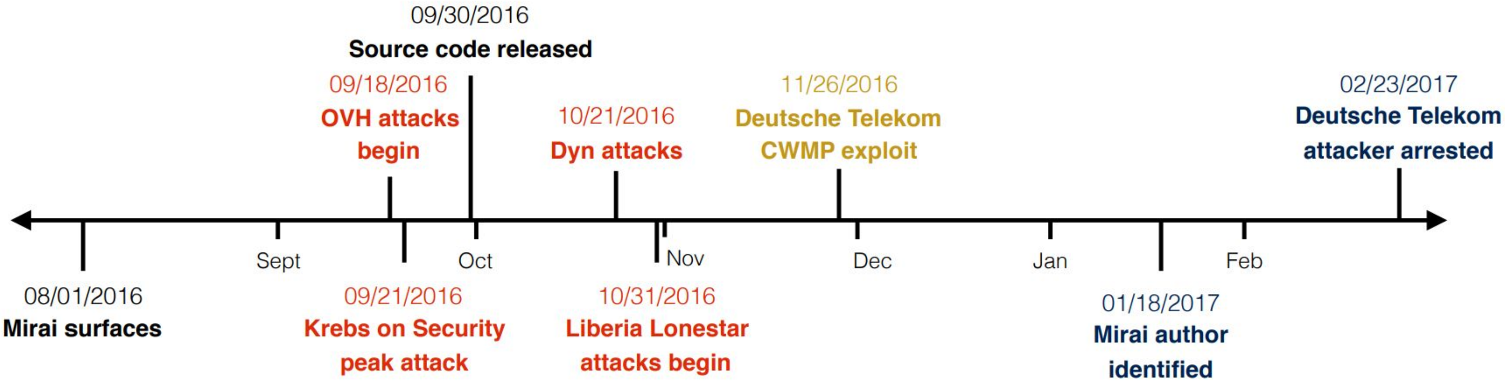
Motivation: Mirai - A model Organism for IoT Botnets



Source: Cisco



Background: A brief history of Mirai


08/01/2016
Mirai surfaces

09/18/2016
OVH attacks begin

09/21/2016
Krebs on Security peak attack

09/30/2016
Source code released

10/21/2016
Dyn attacks

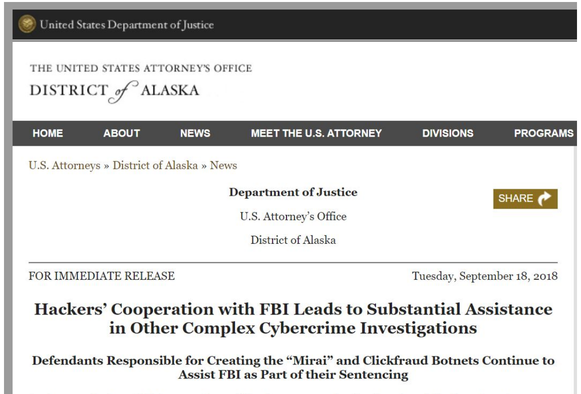
10/31/2016
Liberia Lonestar attacks begin

11/26/2016
Deutsche Telekom CWMP exploit

01/18/2017
Mirai author identified

02/23/2017
Deutsche Telekom attacker arrested

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In *26th {USENIX} security symposium ({USENIX} Security 17)* (pp. 1093-1110).


United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT *of* ALASKA

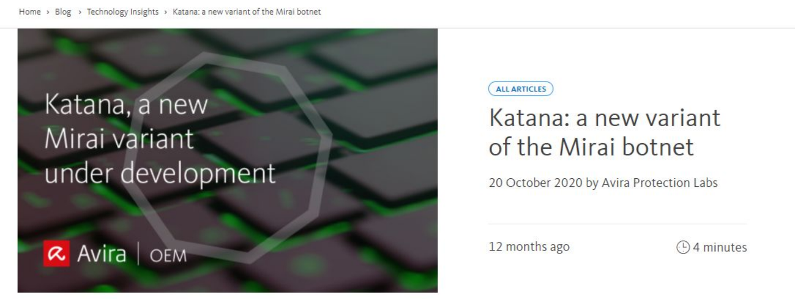
U.S. Attorneys » District of Alaska » News

Department of Justice
U.S. Attorney's Office
District of Alaska

FOR IMMEDIATE RELEASE Tuesday, September 18, 2018

Hackers' Cooperation with FBI Leads to Substantial Assistance in Other Complex Cybercrime Investigations

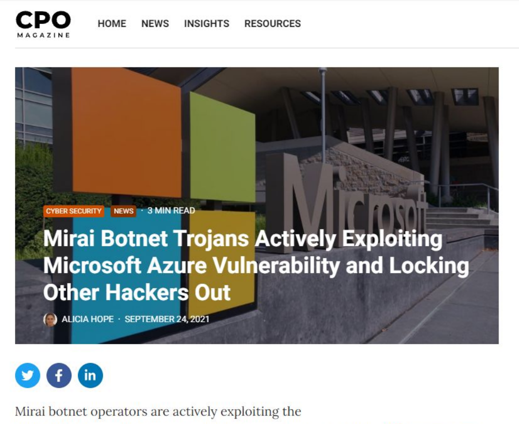
Defendants Responsible for Creating the "Mirai" and Clickfraud Botnets Continue to Assist FBI as Part of their Sentencing


Home › Blog › Technology Insights › Katana: a new variant of the Mirai botnet

Katana: a new variant of the Mirai botnet

20 October 2020 by Avira Protection Labs

12 months ago 4 minutes



Mirai Botnet Trojans Actively Exploiting Microsoft Azure Vulnerability and Locking Other Hackers Out

ALICIA HOPE · SEPTEMBER 24, 2021

Mirai botnet operators are actively exploiting the

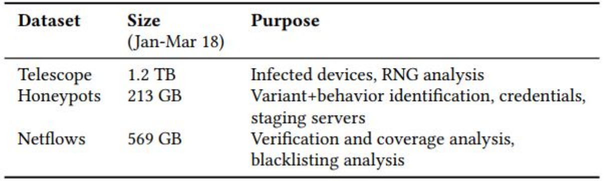
Problem: **Understanding Mirai**

“How do adversaries adapt their strategies to take over and keep a large enough market share of devices?” - Griffioen 2020

- **Empirical Paper:**
  What does the Mirai-like IoT Malware system look like?
- **Breaking Mirai’s PRNG:**
  Can we use the Mirai source code to learn more about Mirai’s deployment?
- **Understanding the Mirai Backend:**
  How do the 39 variants interact, evolve, and specialise. Is Mirai self sustaining?

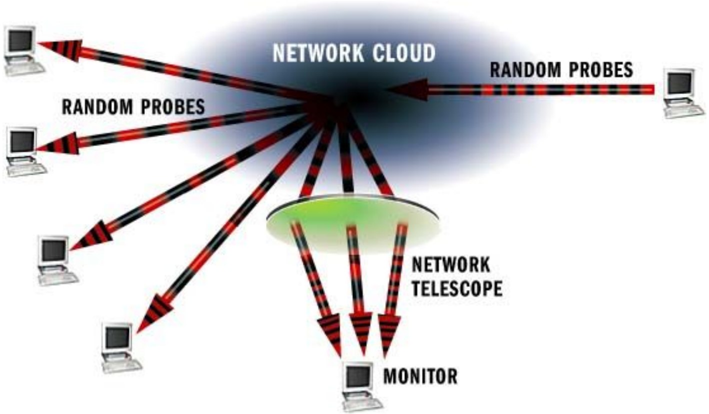
Solution 1: **Idea**

Idea: Go out and look



Dataset	Size (Jan-Mar 18)	Purpose
Telescope	1.2 TB	Infected devices, RNG analysis
Honeypots	213 GB	Variant+behavior identification, credentials, staging servers
Netflows	569 GB	Verification and coverage analysis, blacklisting analysis

Table 1: Datasets used in this study.



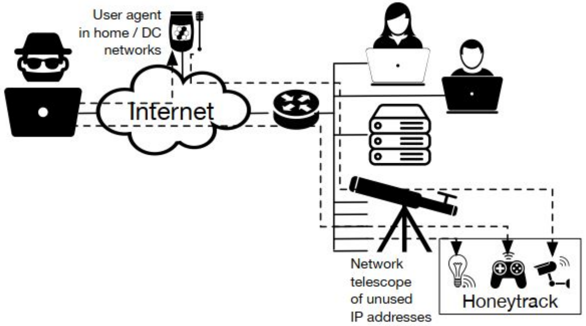

User agent in home / DC networks
Internet
Network telescope of unused IP addresses
Honeytrack

Figure 4: The Honeytrack system routes compromization requests into a separate, virtualized environment.

Details: Breaking Mirai’s PRNG

time(NULL)
    Reduced 32 to 16 (or less)

clock()
    Reduced 32 to 1 bit

getpid() ⊕ getppid()
    entropy(15 ⊕ 15) = 15

Total Entropy Reduction
    94 to 32 bits

Seed produced in 100 ms
(from source port and window size)

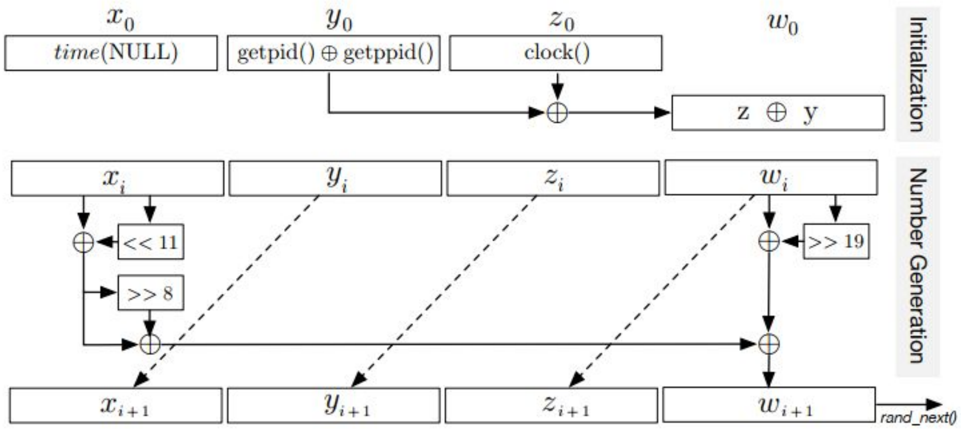
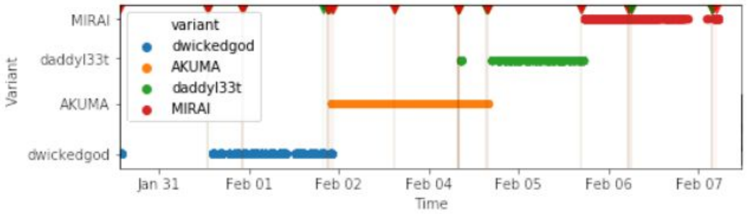
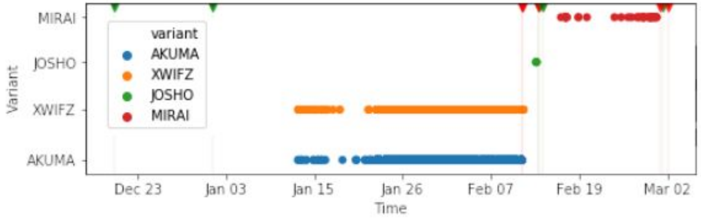


Figure 3: RNG initialization and generation.

Results: The world according to Mirai



(a) Devices get cleaned up and get reinfected by the same malware variant, until another variant takes over on the restart of a device.



(b) Concurrent infections on 1 IP. The first started 10 days before the second, in mid Jan our setup launched and registered both variants.

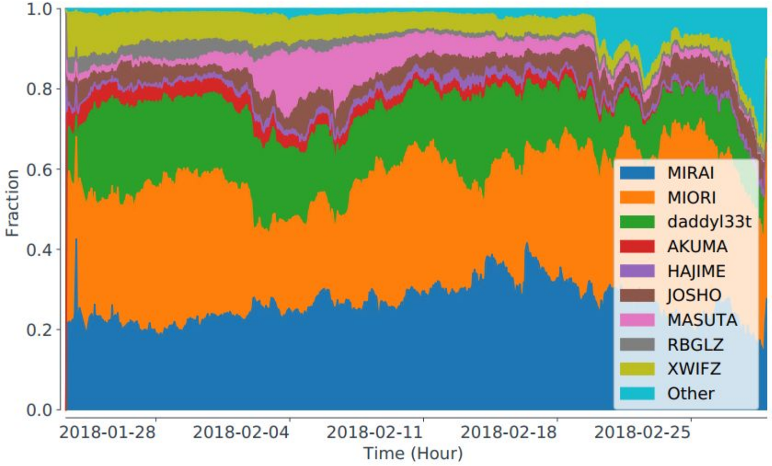
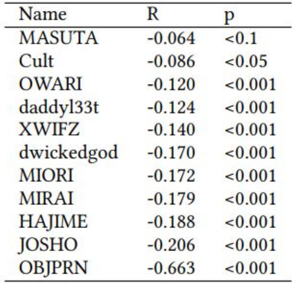


Figure 5: Marketshare of advertised variants.

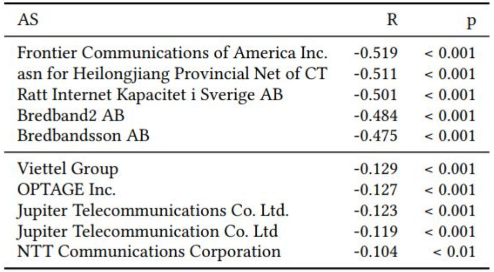
Criticism 1: Statistical Analysis

Criticism: Statistical Analysis



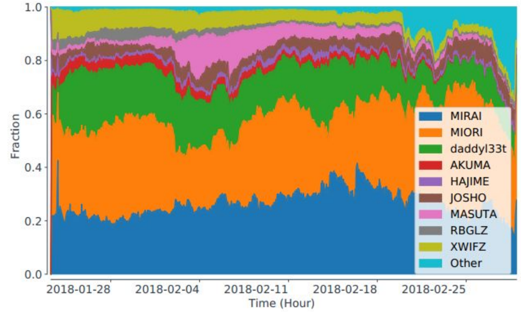
Name	R	p
MASUTA	-0.064	<0.1
Cult	-0.086	<0.05
OWARI	-0.120	<0.001
daddyl33t	-0.124	<0.001
XWIFZ	-0.140	<0.001
dwickedgod	-0.170	<0.001
MIORI	-0.172	<0.001
MIRAI	-0.179	<0.001
HAJIME	-0.188	<0.001
JOSHO	-0.206	<0.001
OBJPRN	-0.663	<0.001

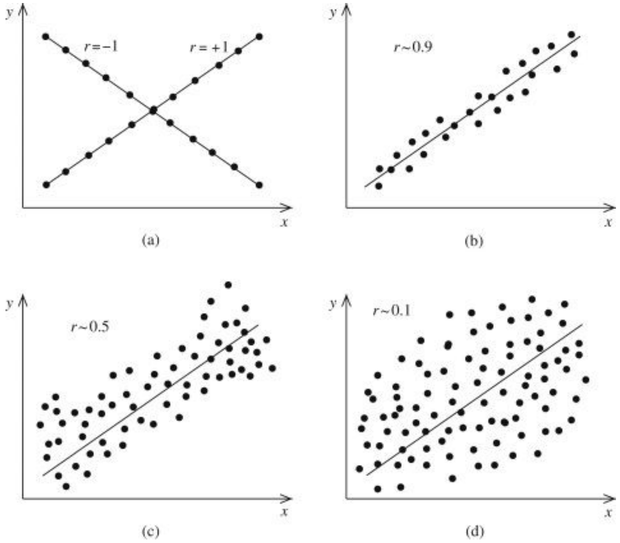
Table 3: Correlation between botnet size and its growth.



AS	R	p
Frontier Communications of America Inc.	-0.519	< 0.001
asn for Heilongjiang Provincial Net of CT	-0.511	< 0.001
Ratt Internet Kapacitet i Sverige AB	-0.501	< 0.001
Bredband2 AB	-0.484	< 0.001
Bredbandsson AB	-0.475	< 0.001
Viettel Group	-0.129	< 0.001
OPTAGE Inc.	-0.127	< 0.001
Jupiter Telecommunications Co. Ltd.	-0.123	< 0.001
Jupiter Telecommunication Co. Ltd	-0.119	< 0.001
NTT Communications Corporation	-0.104	< 0.01

Table 4: Correlation between the size of an AS and its growth, ordered by coefficient for the top and bottom 5 ASes.





Criticism: Causation and Explanation of Observations

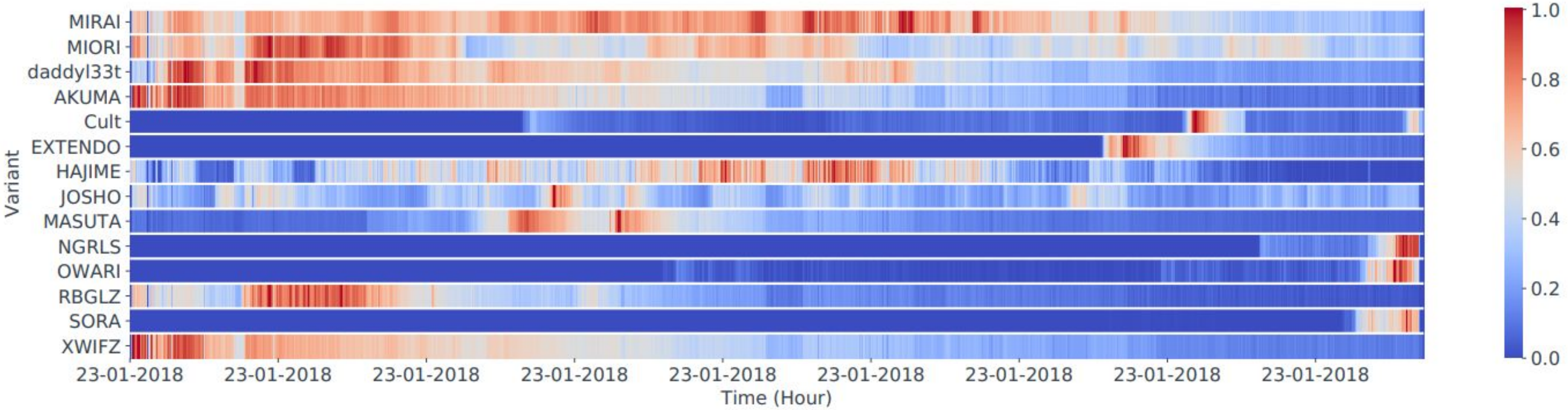
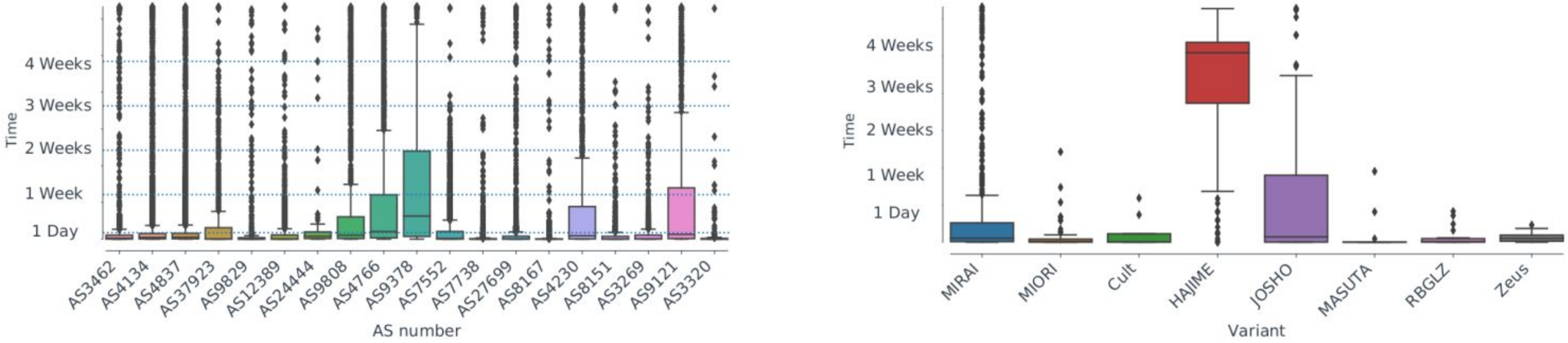


Figure 6: Lifetime distribution of variants over time, normalized per variant. Red shows peak per hour, blue shows little hosts being infected by the variant.

Criticism: Causation and Explanation of Observations



(a) Infection times per AS with more than 1,000 infections, showing large differences between the infection times of different ASes.

(b) Infection times of different variants on AS9121, showing large differences of variants within ASes.

Figure 10: Infection times of different ASes and variants.

Criticism 3: Helps Black Hats more than White Hats

Criticism 3: A great resource… for hackers?

Advice for Mirai Black Hats:

- Use better PRNG
- Select IP ranges more carefully
  - Especially Developing countries
- Harvest Passwords from other variants
  - Even better find your own vulnerabilities
- Spread loading servers across the bot net

Advice for Cyber Security:

- *Generally Absent from paper*

Alternative Suggestions

- Improve Security of IoT Devices
- Block Telnet (e.g. Firewall)
- Sift and Block junk Packets
- Attack Loading Servers (or their hosts)

Thank you for listening.
Questions?

Key Sources:
Conference Presentation https://dl.acm.org/doi/10.1145/3372297.3417277
Original Paper https://dl.acm.org/doi/pdf/10.1145/3372297.3417277

Other resources:

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In 26th {USENIX} security symposium ({USENIX} Security 17) (pp. 1093-1110).
Elie Bursztein Inside Mirai the infamous IoT Botnet: A Retrospective Analysis
Mirai Source Code (github)
Attack on KrebsOnSecurity Cost IoT Device Owners $323K
OMIGOD Mirai Exploit September 2021