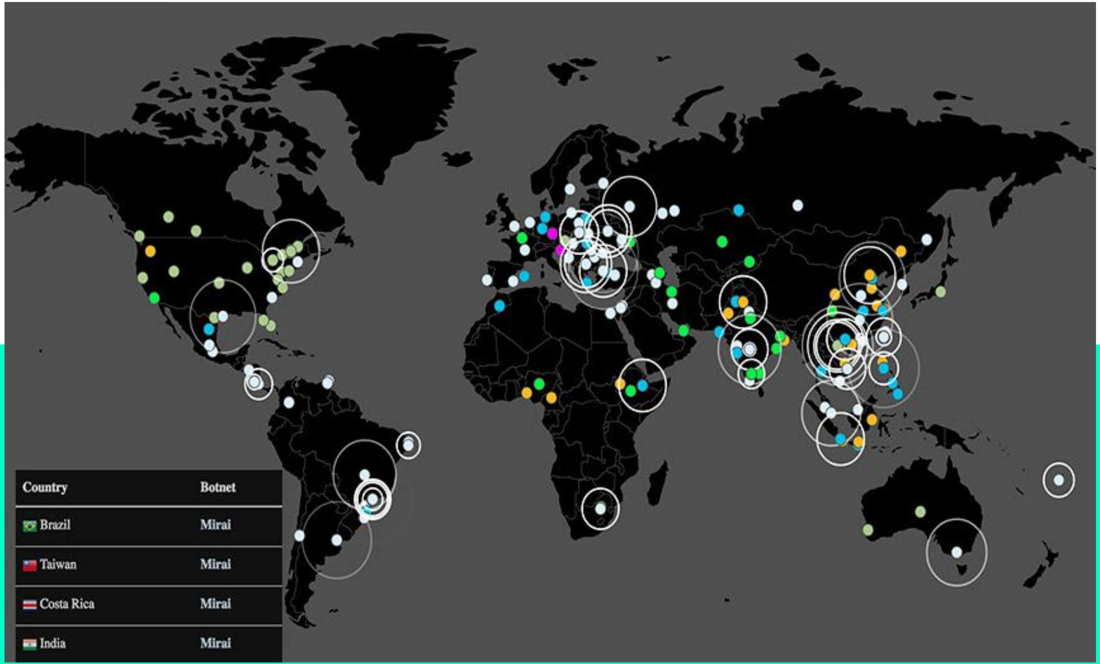
MIRAI



Country	Botnet
Brazil	Mirai
Taiwan	Mirai
Costa Rica	Mirai
India	Mirai

WHAT IS MIRAI

mirai (japanese translates as “future”) is a malware that turns network devices running Linux into remotely controlled bots that can be used as part of a botnet in a large scale network attacks.

WHAT HAPPENED

At its peak in September 2016,Mirai temporarily crippled several high profile services such as OVH (cloud service) ,Dyn (Dns server) and Krebs On Security (a cybersecurity news site) using a massive DDoS attack.

for example OVH reported that these attacks exceeded 1 Terabytes of traffic per second which at the time was the largest found on public record.

Mirai's takedown of the internet

on october 21, a Mirai attack targeted the popular DNS provider DYN.

This even prevented internet users from accessing many popular websites including AirBnB Amazon,Github,Netflix and Twitter by disrubting the DYN name resolution service

NOTE *

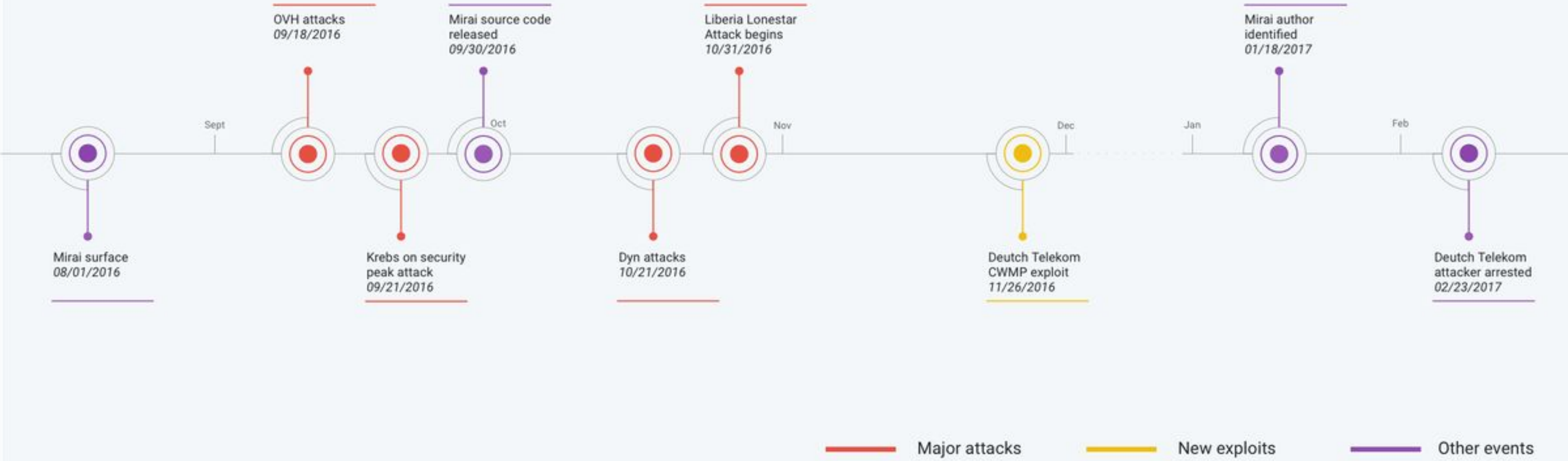
what's remarkable about these attacks is they were carried out via small ,innocuous (IoT) devices such as home routers

personal surveillance cameras and air quality monitors.

at its peak Mirai infected over 600,000 vulnerable IoT devices

Mirai major event timeline

https://elie.net/mirai



Mirai surface
08/01/2016

OVH attacks
09/18/2016

Krebs on security peak attack
09/21/2016

Mirai source code released
09/30/2016

Dyn attacks
10/21/2016

Liberia Lonestar Attack begins
10/31/2016

Deutch Telekom CWMP exploit
11/26/2016

Mirai author identified
01/18/2017

Deutch Telekom attacker arrested
02/23/2017

🟥 Major attacks
🟨 New exploits
🟪 Other events

HOW MIRAI WORKS

- At its core,Mirai is a self-propagating worm which means it replicates itself and attacks vulnerable IoT devices
- the infected devices are controlled via a central set of command and control servers which makes them a botnet
- these servers tell the devices which sites to attack
- made of 2 key components replication module and attack module

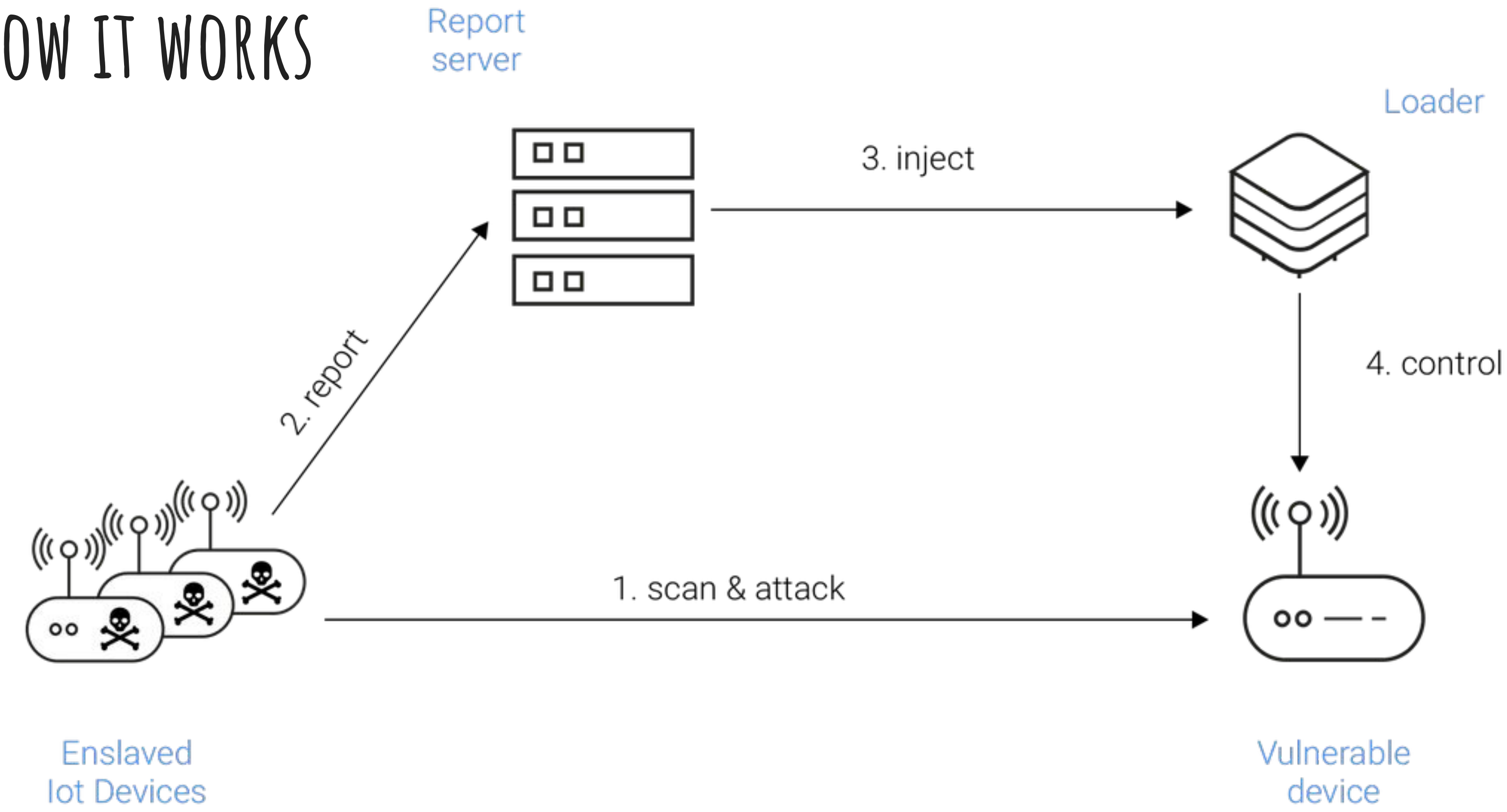
REPLICATION MODULE

the replication module is responsible for growing the botnet size by enslaving many IoT devices as possible .

it accomplishes this by randomly scanning the entire internet by viable targets .

Once the it compromises a vulnerable device the module reports it to the C&C servers so it can be infected with the latest mirai payload

HOW IT WORKS

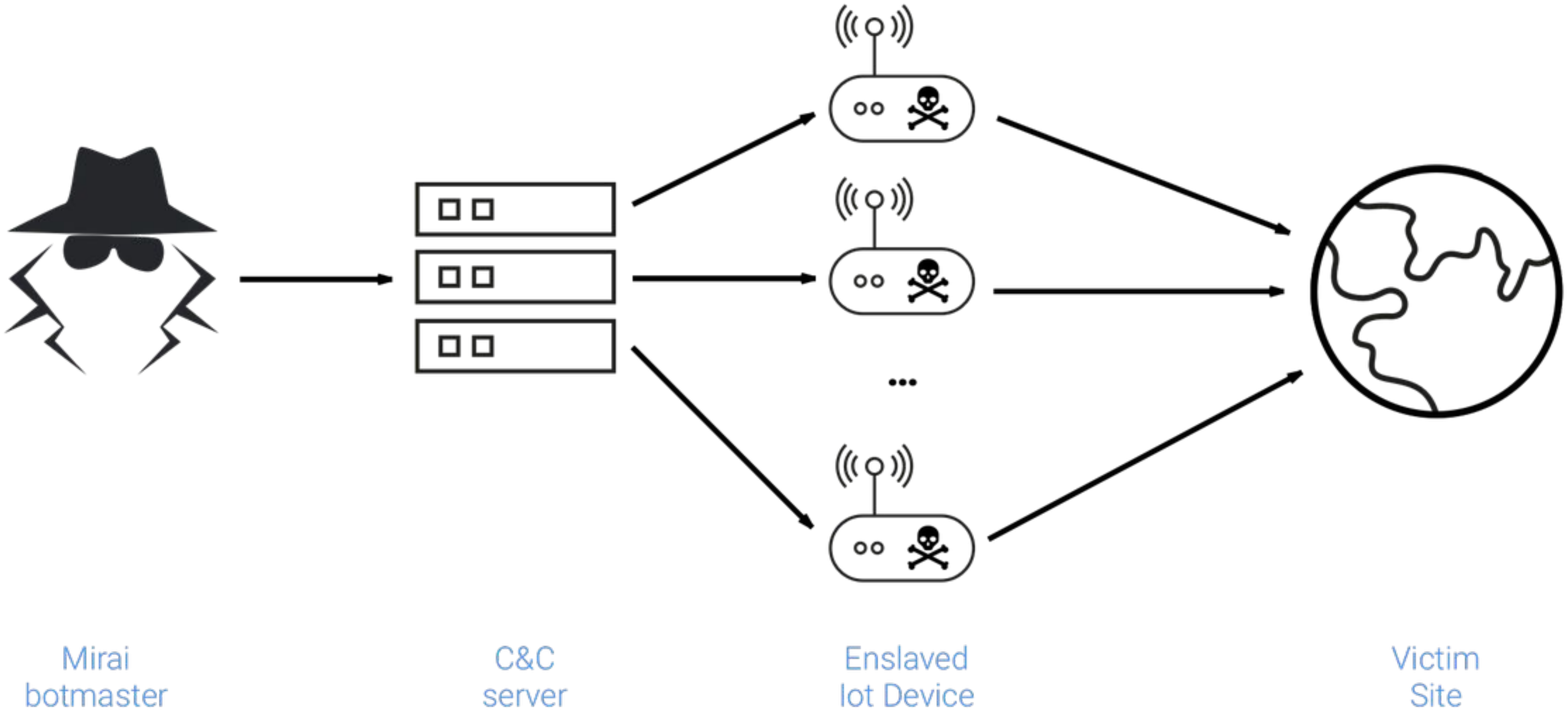

Report
server
Loader
3. inject
2. report
4. control
1. scan & attack
Enslaved
Iot Devices
Vulnerable
device

ATTACK MODULE

The attack module is responsible for carrying out DDos attacks against the targets specified by the C&C servers.

This module implements most of the code DDoS techniques such as HTTP flooding,UDP flooding and all TCP flooding options.

This wide range of methods allowed Mirai to perform volumetric attacks,application-layer attack and TCP state-exhaustion attacks.



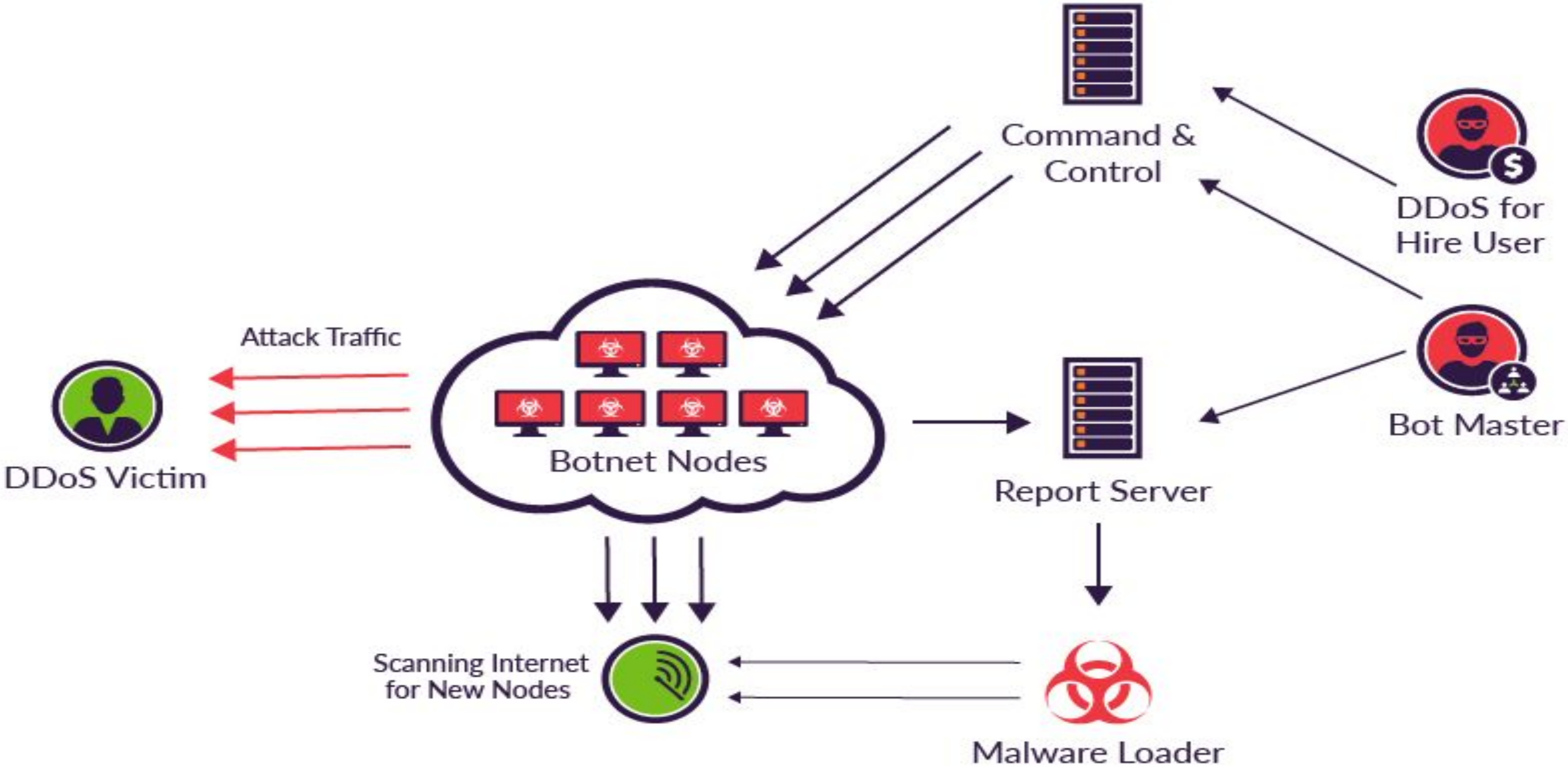
Mirai
botmaster

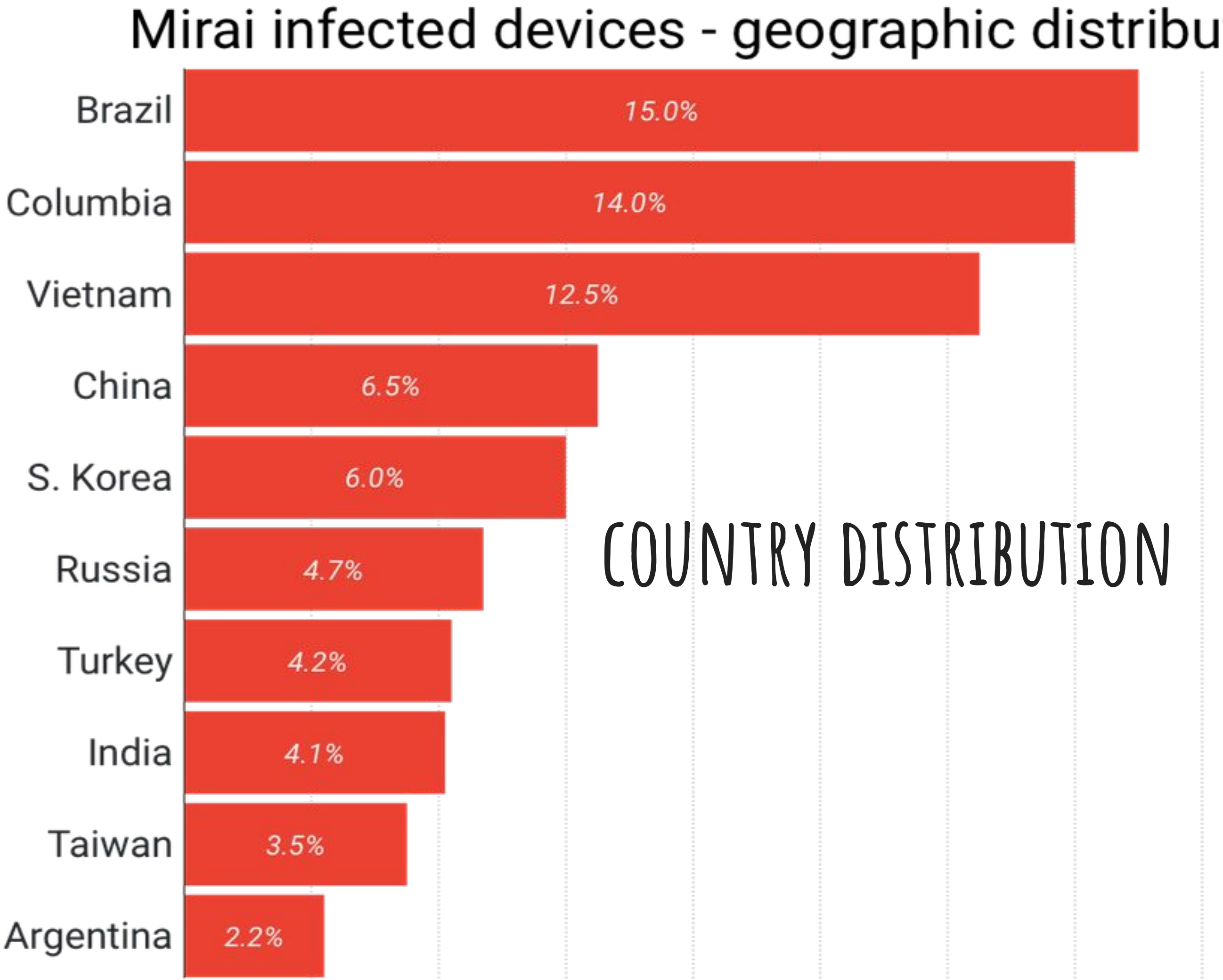
C&C
server

Enslaved
Iot Device

Victim
Site

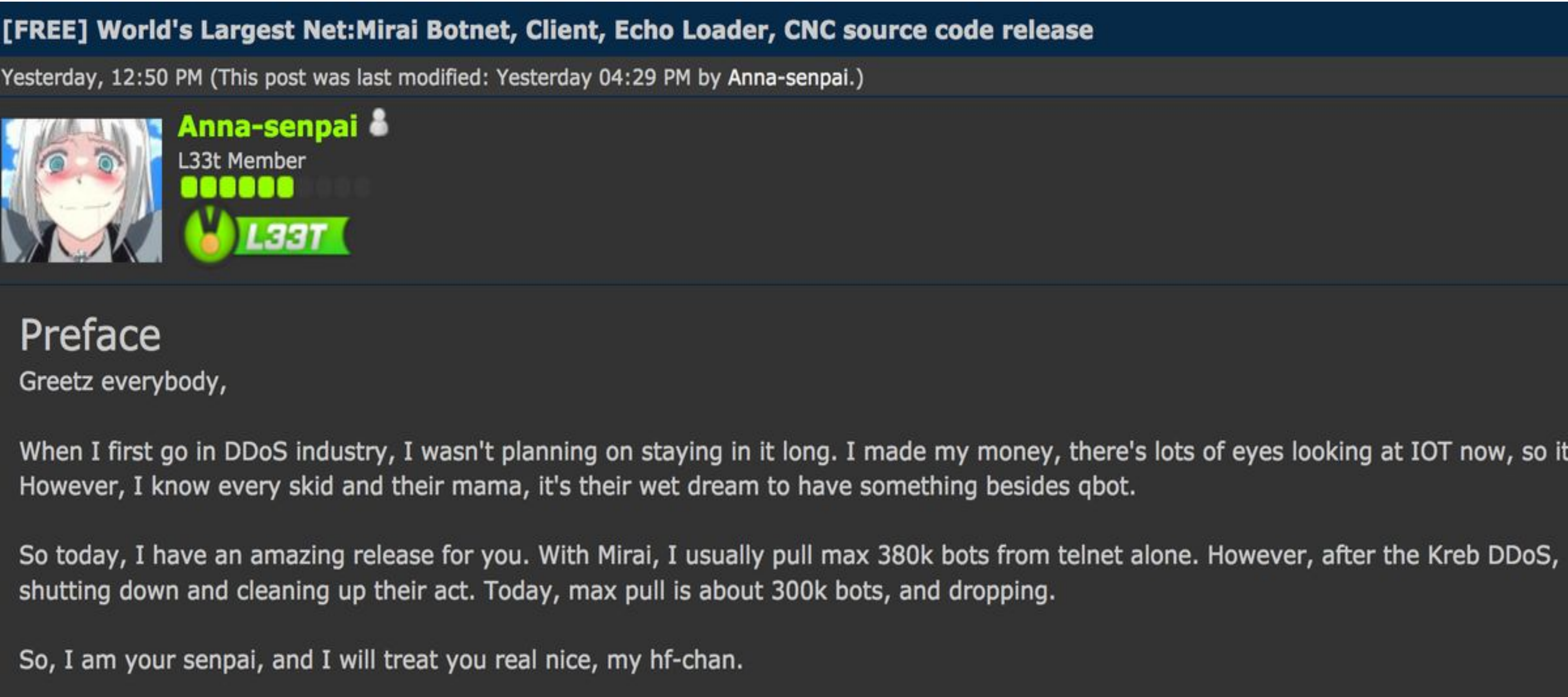
Mirai at a Glance





COUNTRY DISTRIBUTION

THE RISE OF COPYCATS AND THE END OF THE ORIGIN



[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

THE RISE OF COPYCATS

in an unexpected developments, on september 30 ,2017 , Ann-senpai,Mirai’s alleged author,released the Mirai source code via and infamous hacking forum.He also wrote a forum post announcing his retirement

the code release sparked a proliferation of copycat hackers who started to run their own Mirar botnets.

from that point forward the,Mirai attacks were not tied to a single actor or infrastructure but to multiple groups,which made attributing attributing the attacks and discerning the motive behind them significantly harder.

HOW THE MIRAI IMPOSTERS WERE TRACKED

to keep up with the Mirai variants proliferation and track the various hacking groups behind them the investigators tuned to infrastructure clustering .

Reverse engineering all the Mirai version the could find allowed them to extract the ip addresses and domains used as C&C by the various hacking groups that ran their own Mirai Verian.

in total ,they recovers two ip addresses and 66 distinct domains.

MIRAIS ORIGINAL AUTHOR OUTED

in the month following his website being taken offline,Brian Krebs Devoted hundreds of hours to investigate Anna-Senpai,The infamous Mirai author.

in early January of 2017, Announced that he believes Anna-senpai to be Paras Jha , a Rutgers student who apparently has been involved in previous game hacking related schemes.

Brian also identified Josia White as a person of interest.

After being outed,Paras Jha and Josia White and another individual were questioned by authorities and plead guilty in federal court to a variety of charges,some including their activity related to Mirai.

KEY TAKEAWAYS

the prevalence of insecure IoT devices on the internet makes it very likely for the foreseeable future, they will be the main source of DDoS attacks.

Mirai and subsequent IoT botnets can be averted if IoT vendors start to follow basic security best practices.

ELIMINATE DEFAULT CREDENTIALS

this will prevent hackers from constructing a credential main list that allows the to compromise a myriad of devices as Mirai did.

MAKE AUTO PATCHING MANDATORY

IoT devices are meant to be “set and forget”, which makes manual patching unlikely.Having them auto-patch is a good option to ensure that no widespread vulnerability can be exploited to take down large chunks of the internet.

IMPLEMENT RATE LIMITING

Enforcing login rate limiting to prevent brute force attack is a goodway to mitigate the tendency of people to use weak passwords

WHAT CAN YOU DO IN THE CYBER SECURITY SIDE OF THING

1.know your traffic

Use network and application monitoring tools to identify traffic trends and tendencies.

2.Build a recovery plan

be sure to analyze risk and prioritize DDoS mitigation and service recovery efforts in meaningful business terms like lost revenue in accordance with you company strategic information risk management models.

3.have a plan B

be in a position to rapidly restore core services in the face of a DDoS ATTACK.

4.implement zero trust security models

a zero trust framework can help protect against DDos attacks by enforcing least-privileged access and ensuring only authorized users gain access to critical applications and services.

5.incorporate DDoS Attacks into penetration testing to simulate complex attacks and identify vulnerabilities