Connecting and Protecting
the Networked World

What if you could stop cybercrime before it happened?

Financial crime prevention: 'the human factor'

23rd February

We are in the era of digital transformation

Level(3) COMMUNICATIONS

Connecting and Protecting
the Networked World

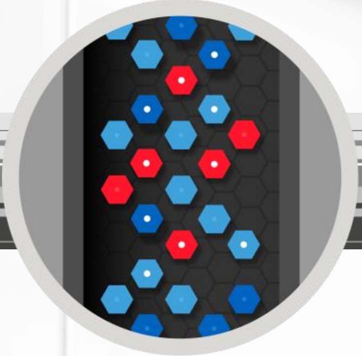
5.2 billion
people connected

More mobility

By 2017, the world will have almost **5.2 billion** people connected through mobile devices[4]

IOT

By 2016, **6.4 billion** devices will be connected to the Internet - **and 5.5 million** new 'things' will join them each day until those numbers reach **20.8 billion by 2020**[1]



More data

By 2020, over **1/3 of all data** will live in or pass through the cloud

2020

More devices

By 2020, each employee will have **seven connected devices**[3]

82%

Cloud

82% of enterprises report a **multi-cloud strategy**[2]

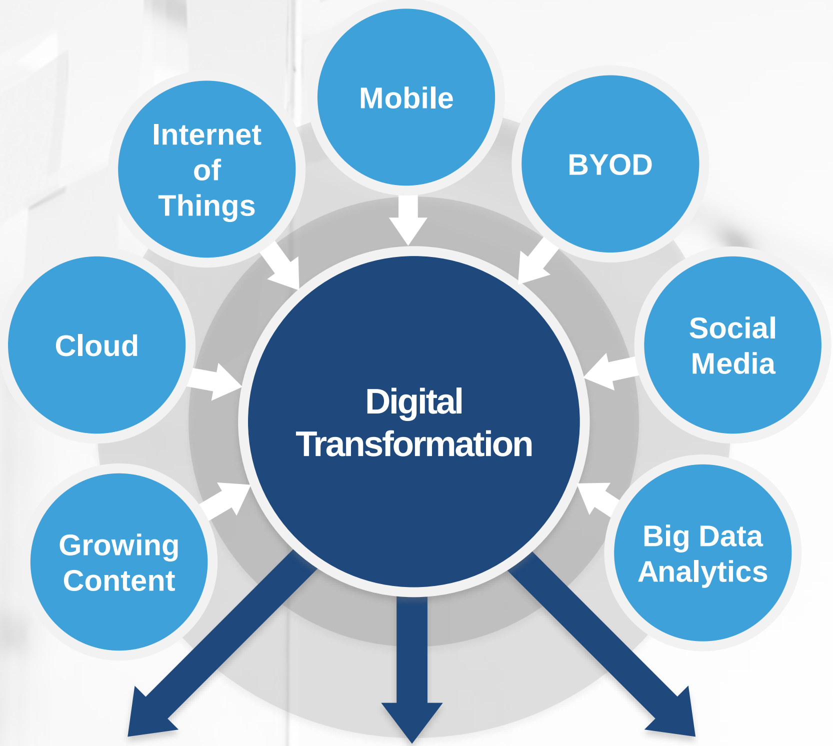
[1] Gartner, 2015
[2] RightScale 2015 “State of the Cloud Report”
[3] Gartner, 2014
[4] Cisco, 2015

The Challenge

To become more agile to keep up with the pace of change

Level(3) COMMUNICATIONS

Connecting and Protecting
the Networked World



Mobile

BYOD

Social Media

Big Data Analytics

Growing Content

Cloud

Internet of Things

Digital Transformation

Growth

Efficiency

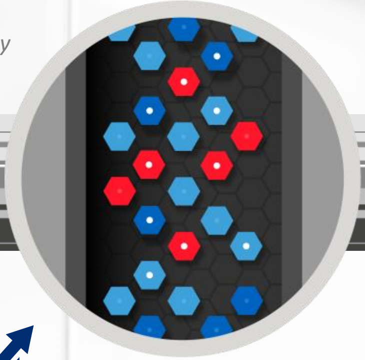
Security

Platform for a new digital architecture

Security Landscape Continues to Evolve

Attacks Are Changing In Form, Complexity, Volume

Level(3) COMMUNICATIONS
Connecting and Protecting
the Networked World



Signatures

100 percent of victims had up-to-date anti-virus signatures

Source: Fireeye 2016 infographic fireeye-advanced-threat-protection.pdf

Malware

431 million new malware variants seen in 2015, an increase of 36%

Source: Symantec Internet Security Report, April 2016

Breaches

9 breaches in 2015 with more than **10 million** identities exposed: a total of **429 million** exposed

Source: Symantec Internet Security Report, April 2016

Breach

47% of victims learn they are breached by a third party

Source: Fireeye 2016 infographic fireeye-advanced-threat-protection.pdf

Compromised Systems

46% of compromised systems had no malware on them

Source: Fireeye 2016 infographic fireeye-advanced-threat-protection.pdf

What We Face

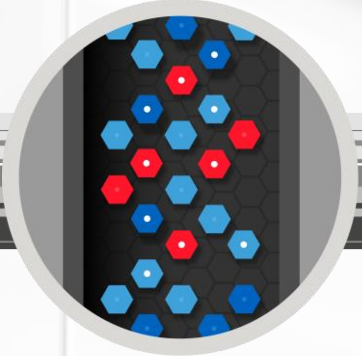
Zero Day and Half Day Attacks

The average zero day lasts 26 months

The average half day lasts 6 months

Increase in targeted attacks

Significant research prior to attacks



Growing regulatory and compliance requirements

Greater transparency

Reaching critical mass. Total IT Budget spend on security at 45% in two Years rise to 55%

Nation state actors beginning to beta test capabilities “contract out” to organized crime

Black market trading sites increasing

Dark Web now larger

Significant increase in DDoS attack volume and bandwidth

Black market trading sites increasing

Security from Our Lens

We **monitor**
~1.3 billion
Security events per day

We **respond** to and
mitigate ~100
DDoS attacks a day

We **identify** and **remove**
at least **one C2**
network a month

We **monitor** over
48 billion
NetFlow sessions per day

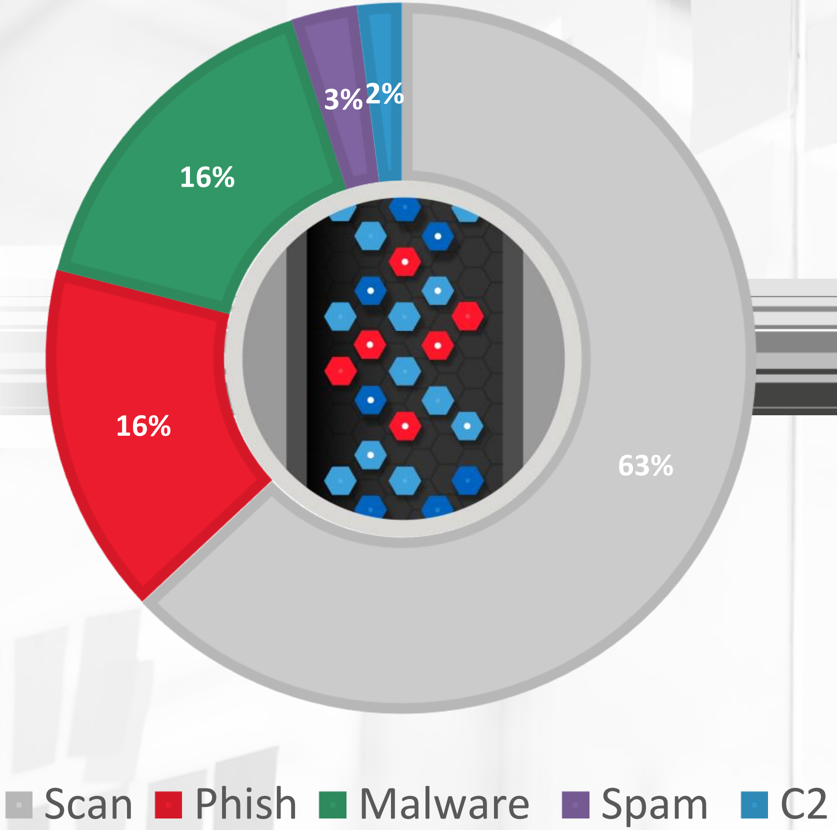
We **collect**
~87 TB
of data per day

We perform
daily audits,
protect and monitor
all our products & systems

Who Is Attacking?

Top 10 countries seen hosting C2s in Q1, 2016

Connecting and Protecting the Networked World



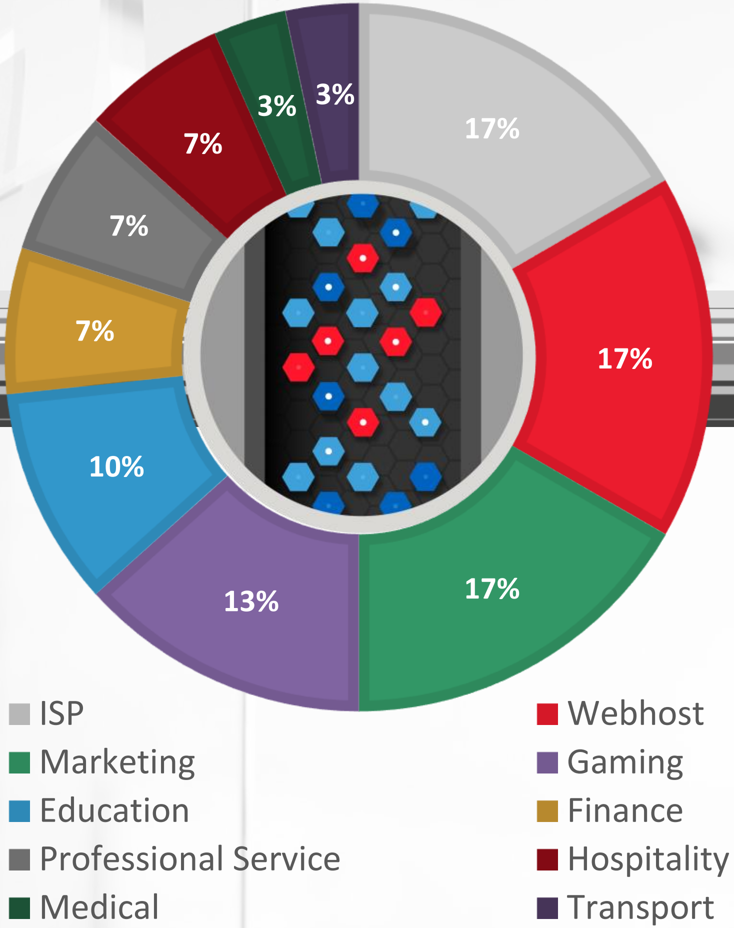
1. United States
2. Russia
3. South Korea
4. China
5. Germany
6. United Kingdom
7. France
8. Netherlands
9. Poland
10. Ukraine

What we have seen?

Connecting and Protecting
the Networked World

Attacks

Attacks are automated business, scanning all businesses across all sectors



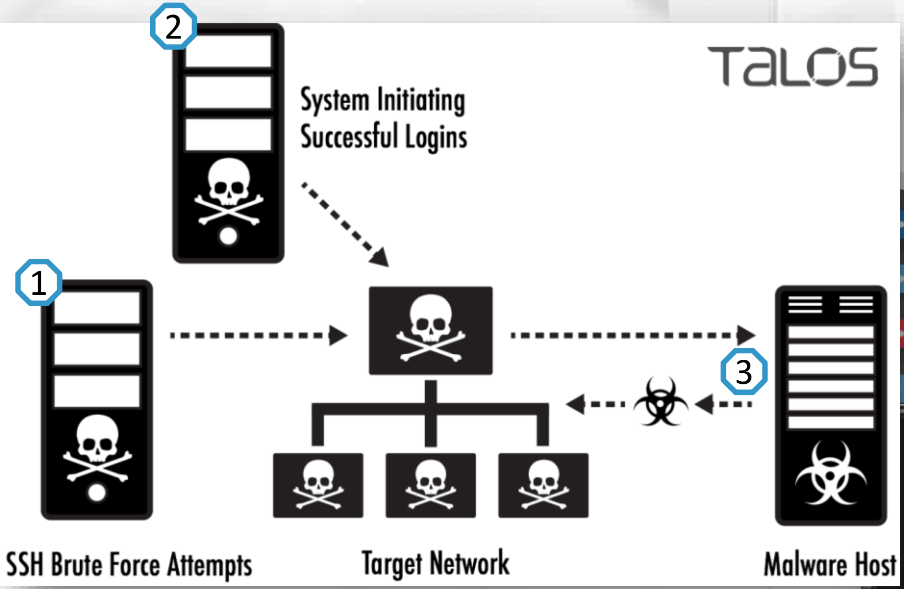
Victims

The victim profile changes each month

Source: Level 3 Communications, July 2016

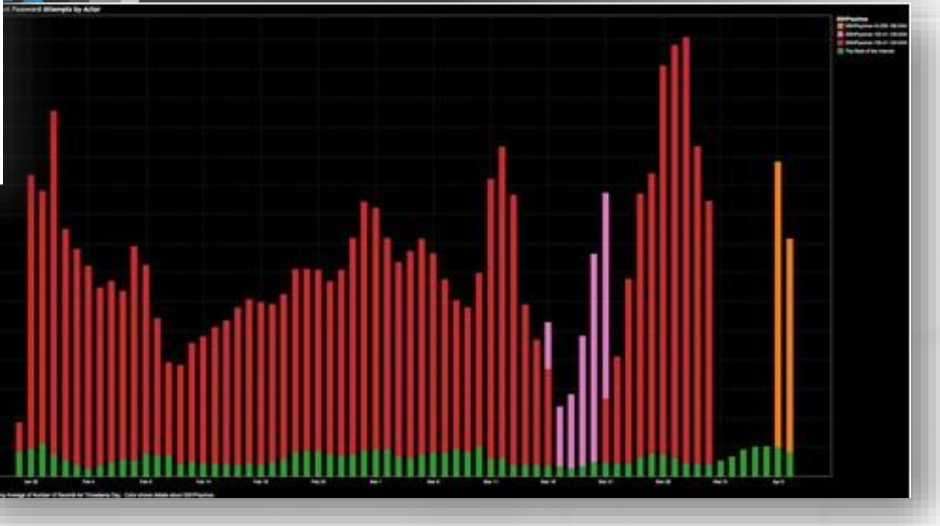
Threat Intelligence Use Case

SSH Psychos



Generated Traffic

A visual depiction of the SSHPyscho traffic verses SSH traffic of the rest of the Internet



Attack on Linux

1 Large amounts of SSH brute force login attempts from 103.41.124.0/23.Attempting to guess the password for the root user, with over 300,000 unique passwords

2 Next step involves a login from a completely different IP ranges

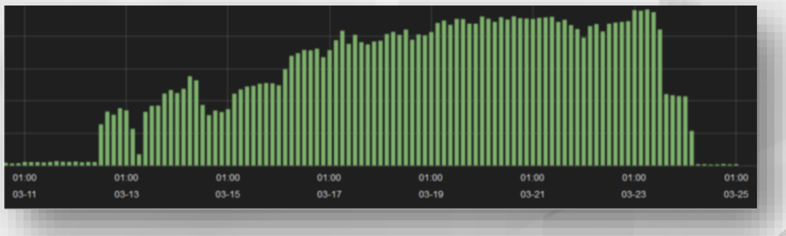
3 Login is achieved a wget request is sent outbound for a single file which has been identified as a DDoS rootkit

Threat Intelligence Use Case

Point of Sale Malware: PoSeidon

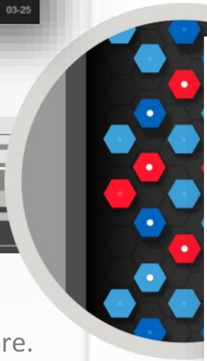
Level(3) COMMUNICATIONS

Connecting and Protecting the Networked World



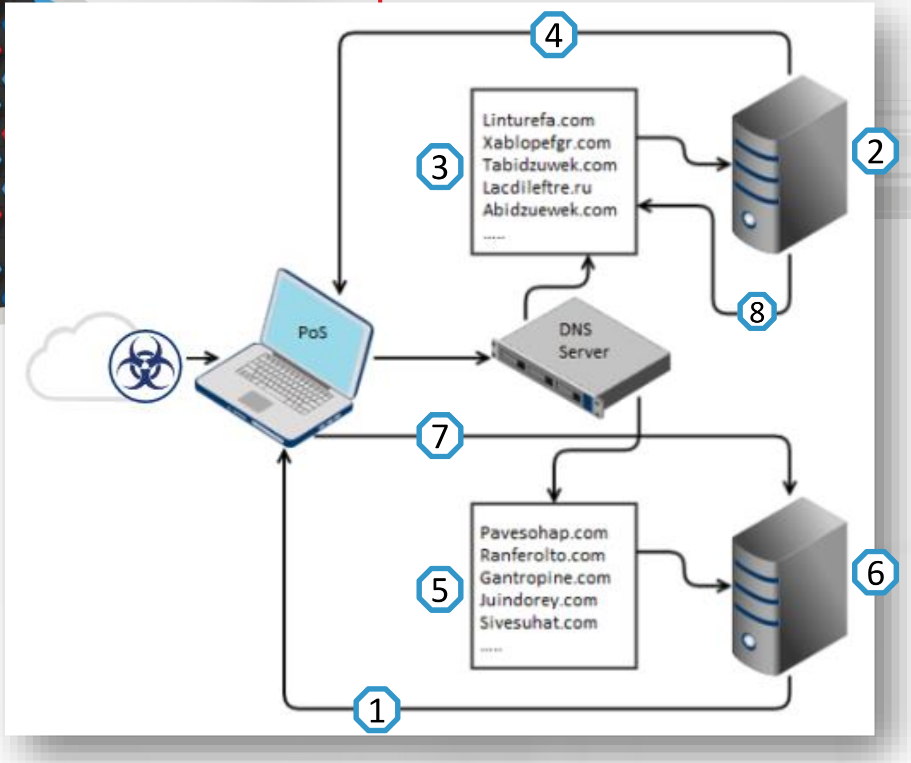
Lucrative business for malware

Attackers will continue to target PoS systems and employ various obfuscation techniques in an attempt to avoid detection.



Malware Anatomy

The PoS system is compromised by the PoSeidon malware. The malware includes a list of domains 3 for the C2 server. If a domain's DNS resolves the host is sent to the C2 2 where it Downloads 4 the exfiltration server domains 5. The compromised system then contacts the DNS server every 120 seconds looking for an exfiltration server 6. Once a exfiltration server is located – the stored credit card data is transferred 7 out. If the C2 goes offline 8 the compromised computer than attempts to resolve another C2 domain 3 - if this fails it watches the exfiltration server 6 for a new set of domains which are returned to the compromised host 1



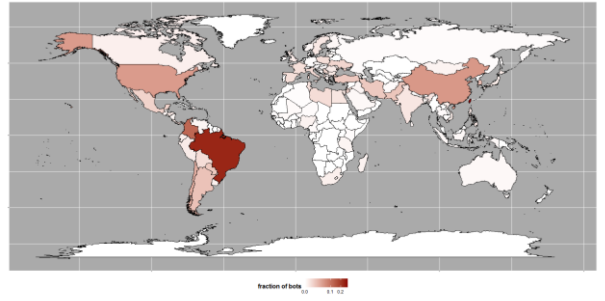
Threat Intelligence Use Case

IoT Vulnerabilities and Bashlite Botnets

Level(3) COMMUNICATIONS

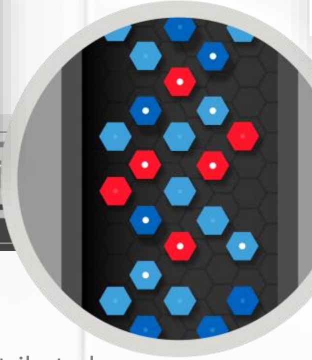
Connecting and Protecting the Networked World

Global Distribution of Gafgyt Bots



Identifiable devices

96 percent were IoT devices (of which 95 percent were cameras and DVRs), roughly 4 percent were home routers and less than 1 percent were compromised Linux servers.



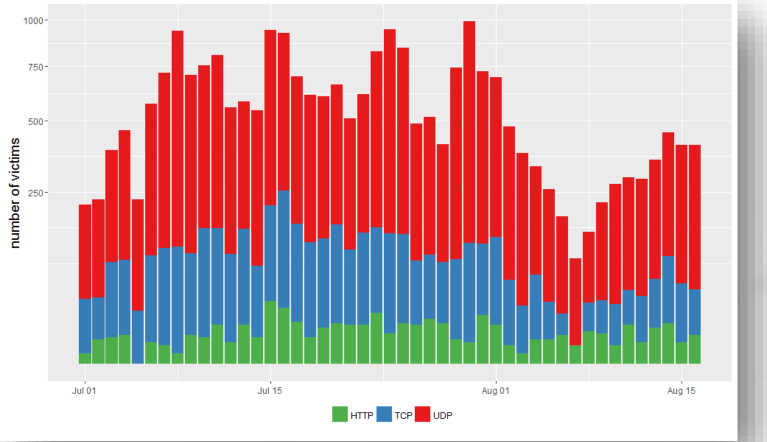
IoT

IoT devices compromised for the purpose of creating Distributed Denial of Service (DDoS) botnets

Botnets used to launch more than 100 attacks per day, 75 percent of the attacks launched using BASHLITE are shorter than 5 minutes.

The malware family is responsible for botnets that control approximately one million endpoints

Most bots located in Brazil, Colombia and Taiwan

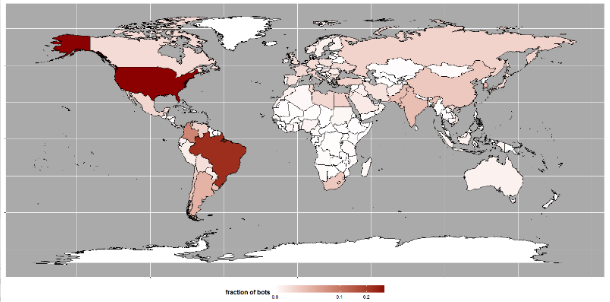


Volume of Attacks by Type

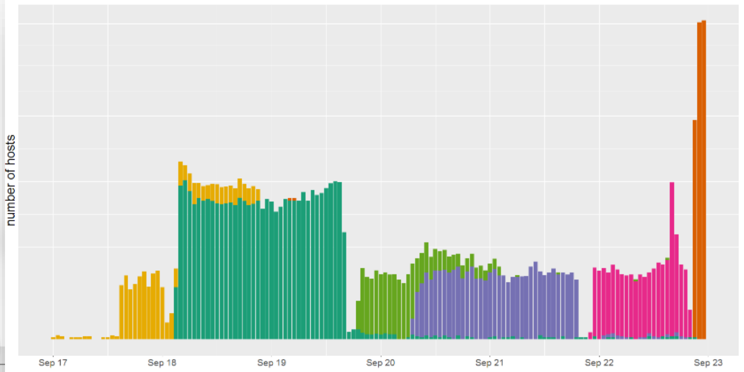
Threat Intelligence Use Case

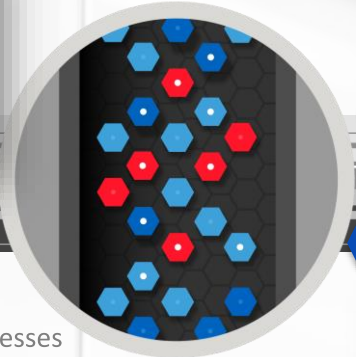
How the Grinch Stole IoT (Mirai)

Global Distribution of Mirai Bots



Mirai "network" C2 outbound traffic binned by hour. Colours represent different C2s





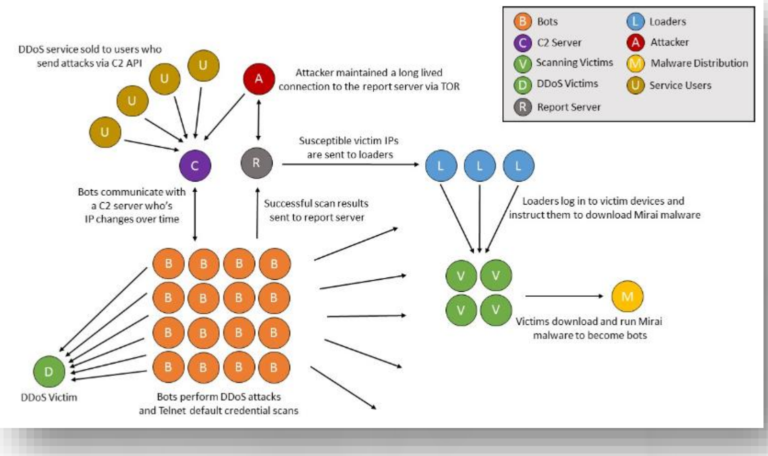
Mirai

C2s associated with this botnet. Additionally, the IP addresses identified pointed to domains containing "santasbigcandycane.cx"

Every two days, a new network C2 IP became active. This switching behaviour is roughly 3-times more rapid than we observed in the gafgyt botnet

We discovered was that the Mirai network C2s were attacked several times by a gafgyt/BASHLITE botnet.

Mirai infrastructure was much more complex than the various gafgyt variants


B Bots
L Loaders
C C2 Server
A Attacker
V Scanning Victims
M Malware Distribution
D DDoS Victims
U Service Users
R Report Server
DDoS service sold to users who send attacks via C2 API
U
U
U
U
A
Attacker maintained a long lived connection to the report server via TOR
C
R
Susceptible victim IPs are sent to loaders
L
L
L
Bots communicate with a C2 server who's IP changes over time
Successful scan results sent to report server
Loaders log in to victim devices and instruct them to download Mirai malware
B
V
M
Victims download and run Mirai malware to become bots
D
DDoS Victim
Bots perform DDoS attacks and Telnet default credential scans

Structure of a Mirai botnet