Understanding the Mirai botnet

Aluno: Marcio A. C. Sczepanski

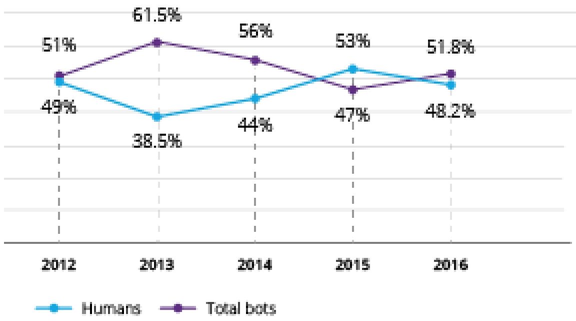
- BOT
-

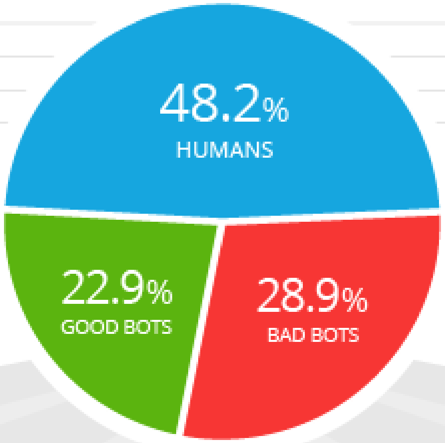
BOT TRAFFIC REPORT 2016

BOTS ONCE AGAIN COMPRISE THE MAJORITY OF ONLINE TRAFFIC AMID AN INCREASE IN GOOD BOT ACTIVITY.

BOT ACTIVITY IS IN AN UPTREND,

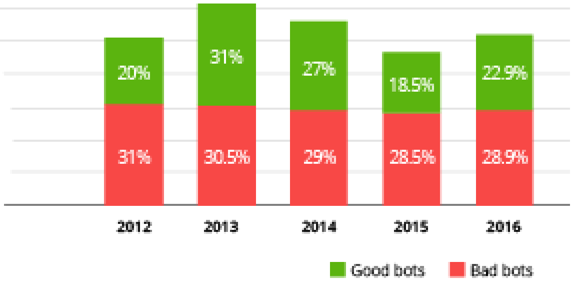
after a three year decline.





INCREASE IN GOOD BOT ACTIVITY,

which went up by 4.4 percent.



1.2%
MONITORING BOTS
Health checkers that monitor website availability and the proper functioning of various online features.

2.9%
COMMERCIAL CRAWLERS
Spiders used for authorized data extractions, usually on behalf of digital marketing tools.

6.6%
SEARCH ENGINE BOTS
Bots that collect information for search engine algorithms, which they use to make ranking decisions.

12.2%
FEED FETCHERS
Bots that ferry website content to mobile and web applications, which they then display to their users.

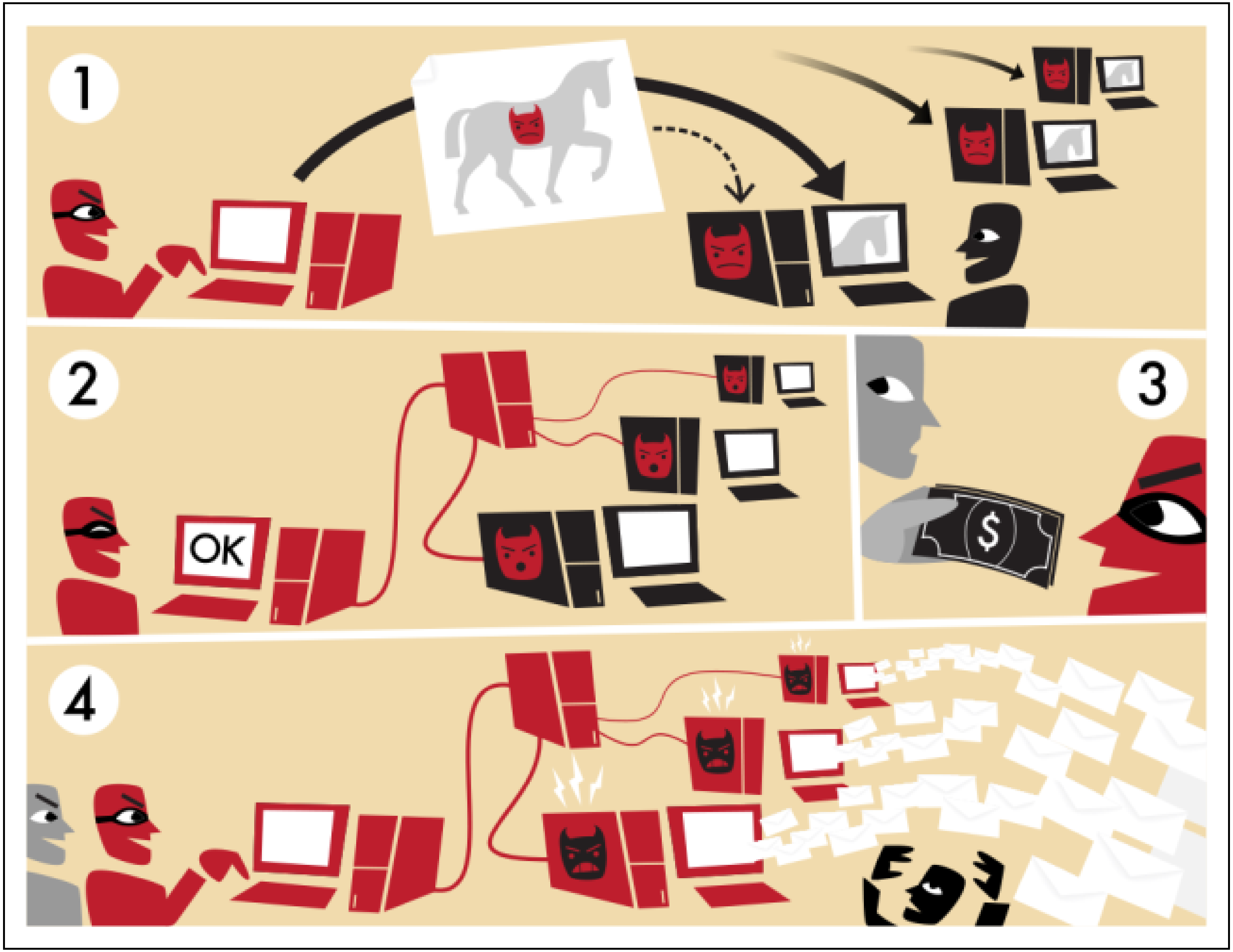
24.3%
IMPERSONATORS
Bots that assume false identities to bypass security solutions. They are commonly used for DDoS assaults.

1.7%
SCRAPERS
Bots used for unauthorized data extraction and the reverse engineering of pricing models.

0.3%
SPAMMERS
Polluters that inject spam links into forums, discussions and comment sections.

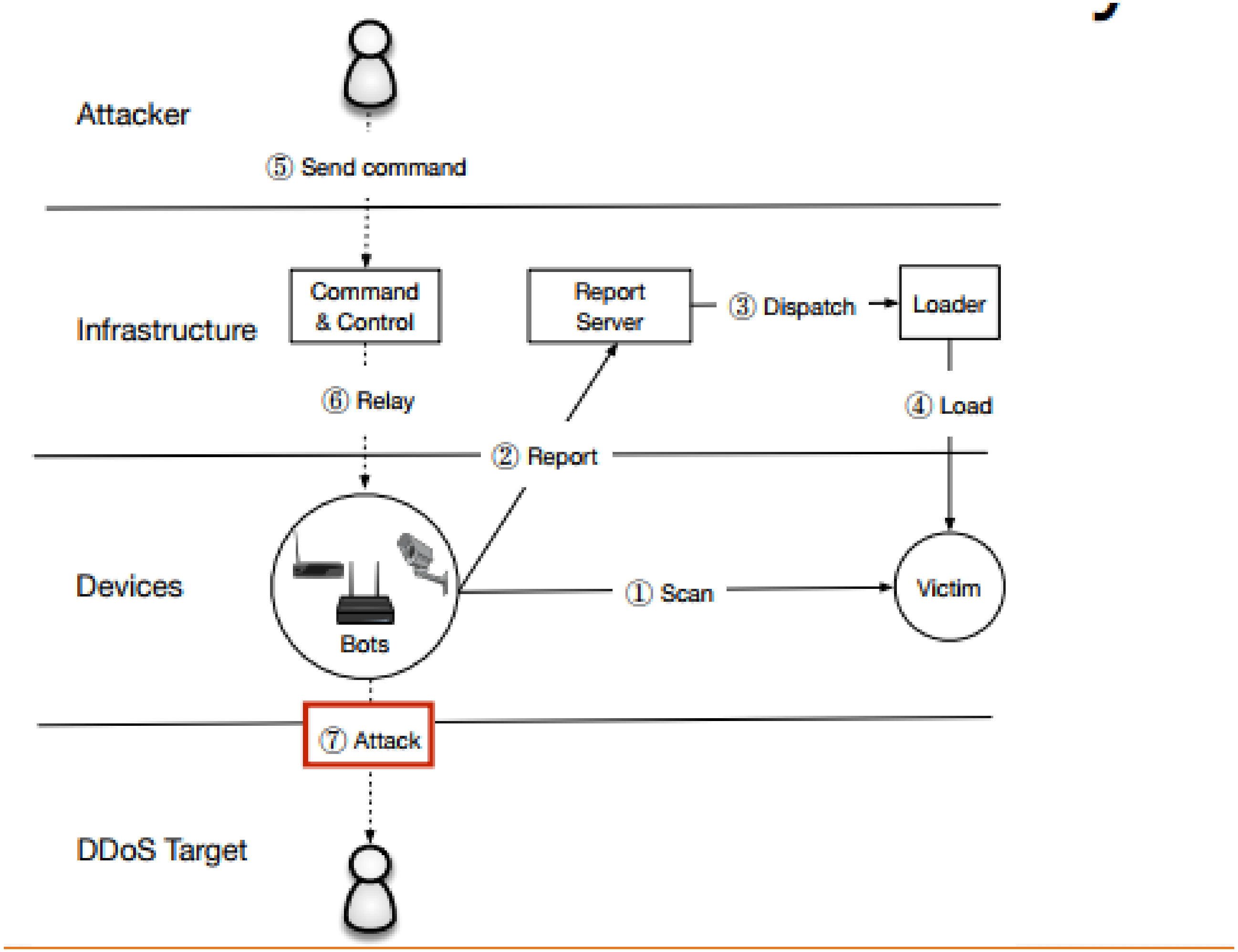
2.6%
HACKER TOOLS
Scavengers that look for sites with vulnerabilities to exploit for data theft, malware injection, etc.

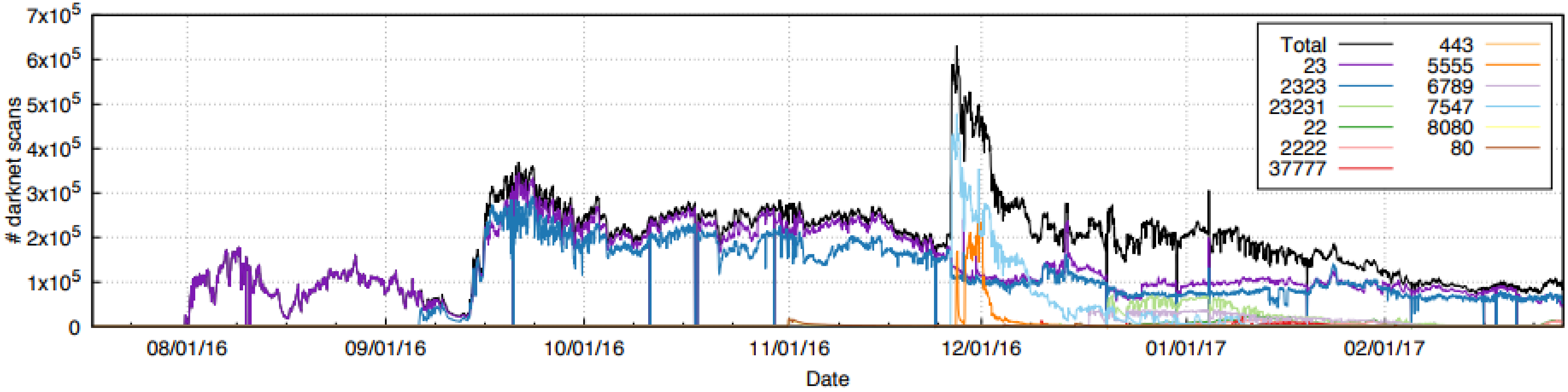
- BOT
- BotNet


1
2
OK
3
$
4

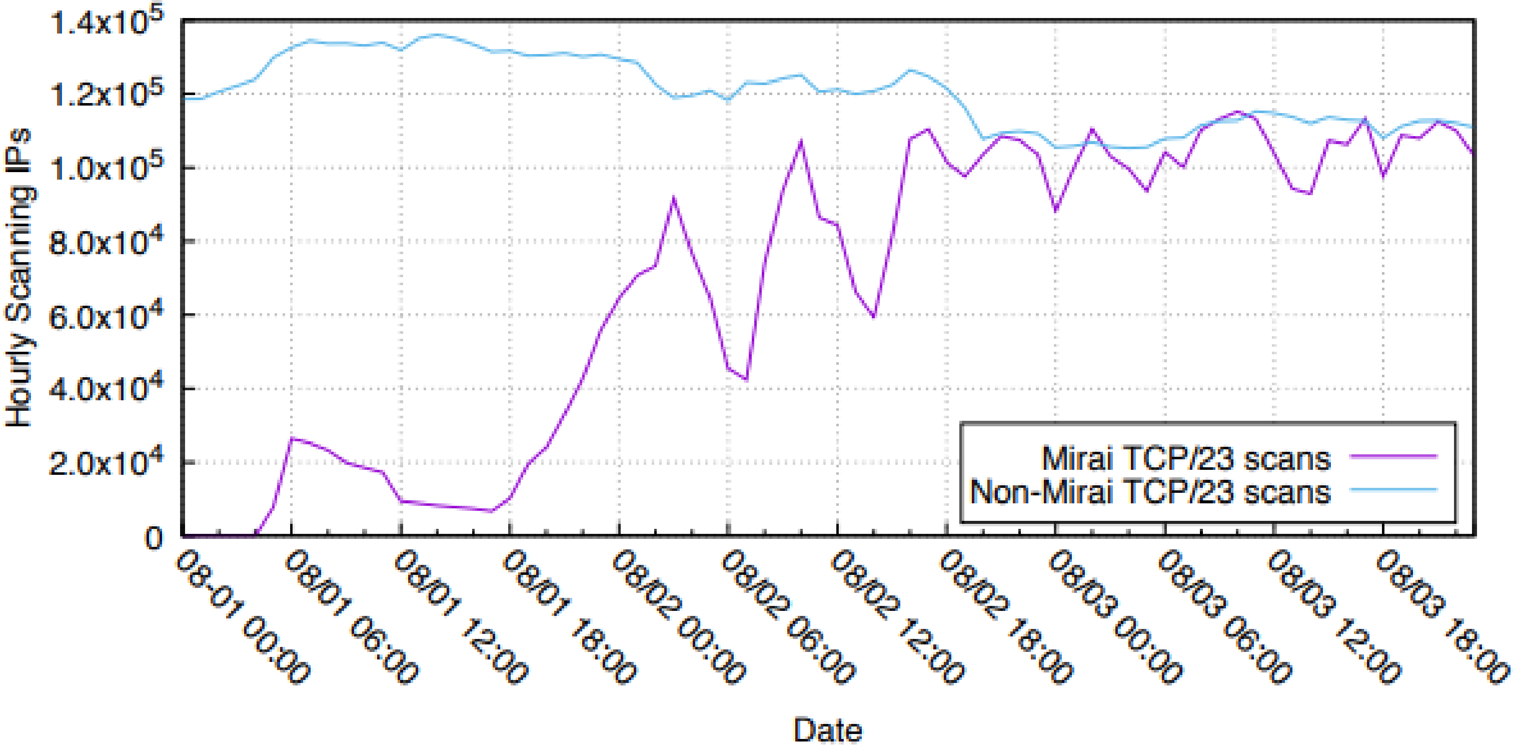
- BOT
- BotNet
- Mirai BotNet

Como funciona?





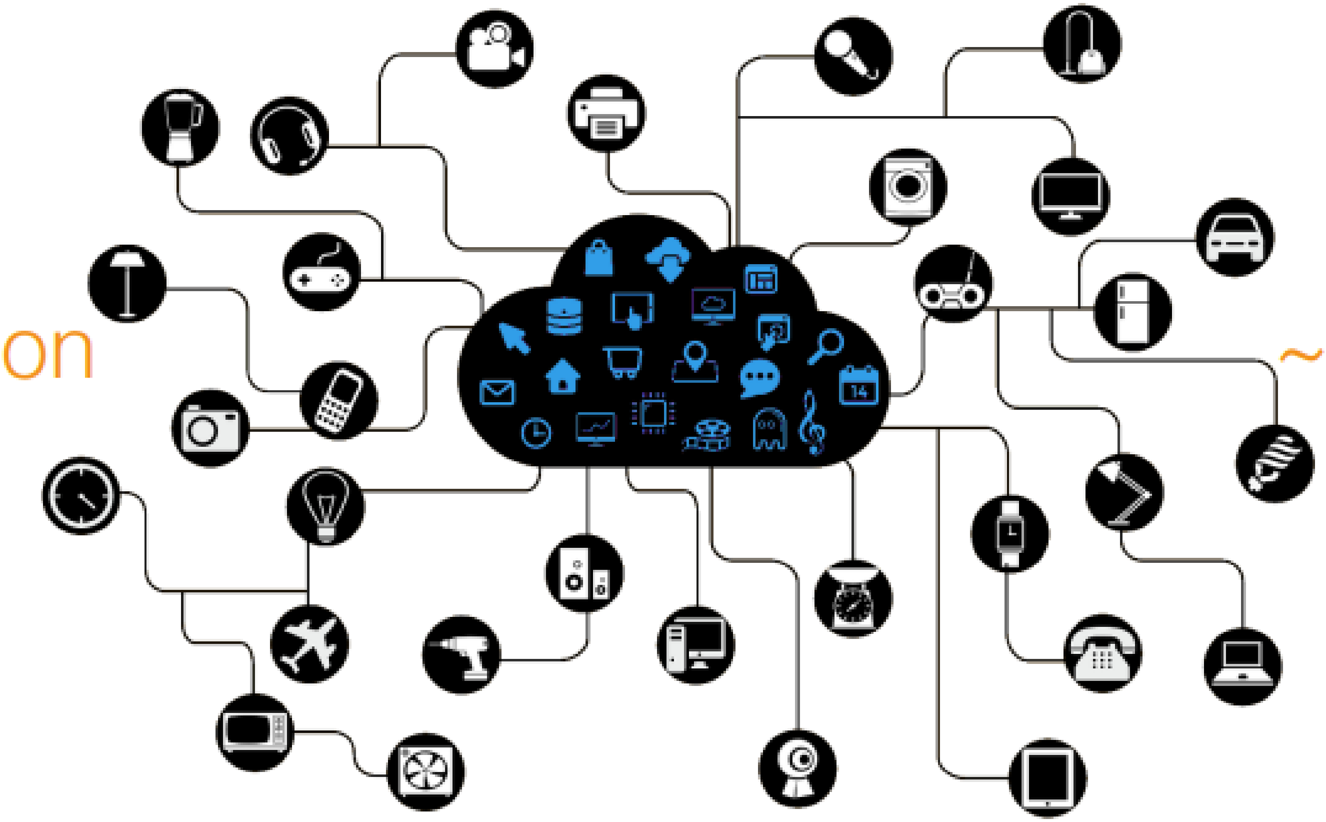
Mirai começou fazendo scan em Telnet, variantes evoluiram mirando 11 protocolos adicionais



No primeiro minuto ,após uma fase aonde apenas 1 Mirai scan foi feito, a BotNet emergiu, aonde 834 aparelhos começaram a fazer scan,nos primeiros 10 minutos já haviam 11mil hospedeiros infectados.
Dentro de 20 horas Mirai já havia infectado 64500 aparelhos.

2016

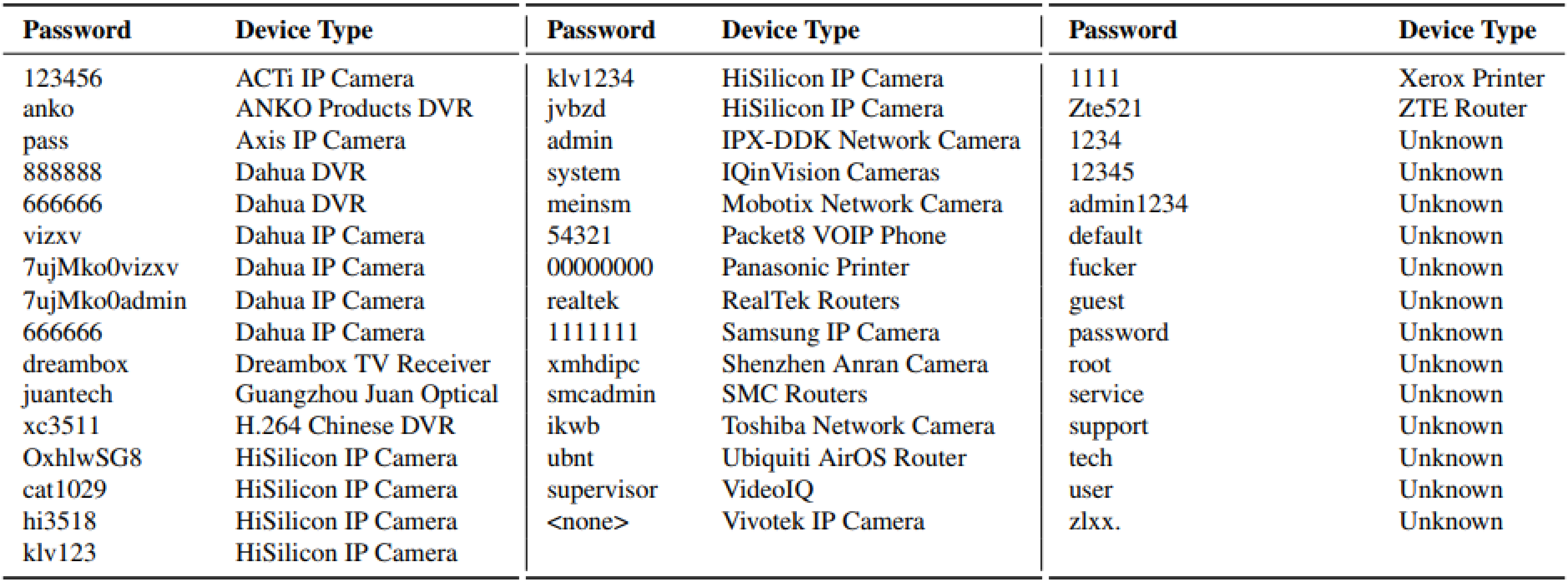
6 - 9 Billion



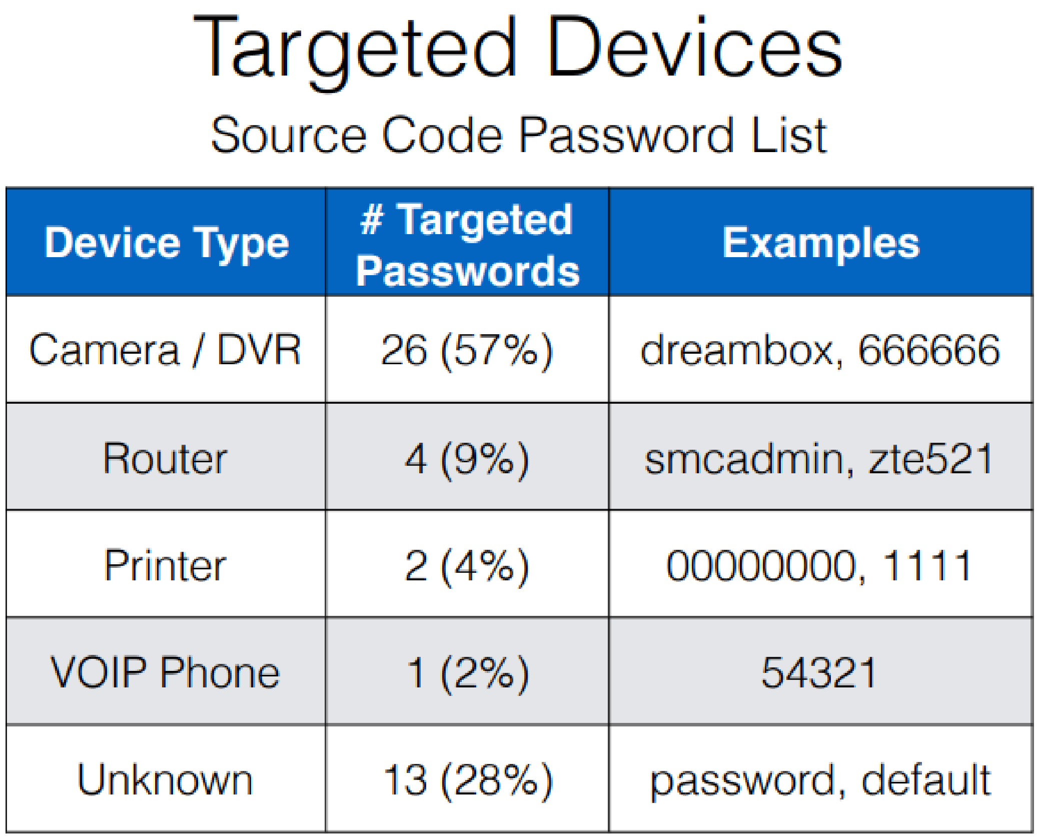
2020

~30 Billion

Mirai se utilizava de uma lista de logins e passwords dentro do seu código fonte, que foi disponibilizado em 30/09/2016



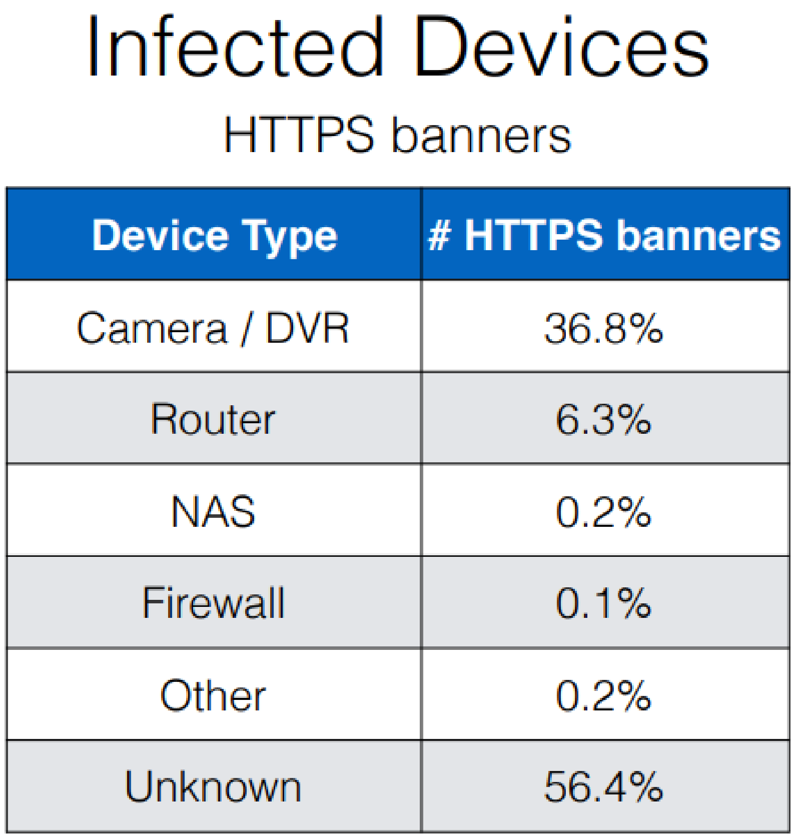
Password	Device Type	Password	Device Type	Password	Device Type
123456	ACTi IP Camera	klv1234	HiSilicon IP Camera	1111	Xerox Printer
anko	ANKO Products DVR	jvbzd	HiSilicon IP Camera	Zte521	ZTE Router
pass	Axis IP Camera	admin	IPX-DDK Network Camera	1234	Unknown
888888	Dahua DVR	system	IQinVision Cameras	12345	Unknown
666666	Dahua DVR	meinsm	Mobotix Network Camera	admin1234	Unknown
vizxv	Dahua IP Camera	54321	Packet8 VOIP Phone	default	Unknown
7ujMko0vizxv	Dahua IP Camera	00000000	Panasonic Printer	fucker	Unknown
7ujMko0admin	Dahua IP Camera	realtek	RealTek Routers	guest	Unknown
666666	Dahua IP Camera	1111111	Samsung IP Camera	password	Unknown
dreambox	Dreambox TV Receiver	xmhdipc	Shenzhen Anran Camera	root	Unknown
juantech	Guangzhou Juan Optical	smcadmin	SMC Routers	service	Unknown
xc3511	H.264 Chinese DVR	ikwb	Toshiba Network Camera	support	Unknown
OxhlwSG8	HiSilicon IP Camera	ubnt	Ubiquiti AirOS Router	tech	Unknown
cat1029	HiSilicon IP Camera	supervisor	VideoIQ	user	Unknown
hi3518	HiSilicon IP Camera	<none>	Vivotek IP Camera	zlxx.	Unknown
klv123	HiSilicon IP Camera				



Targeted Devices

Source Code Password List

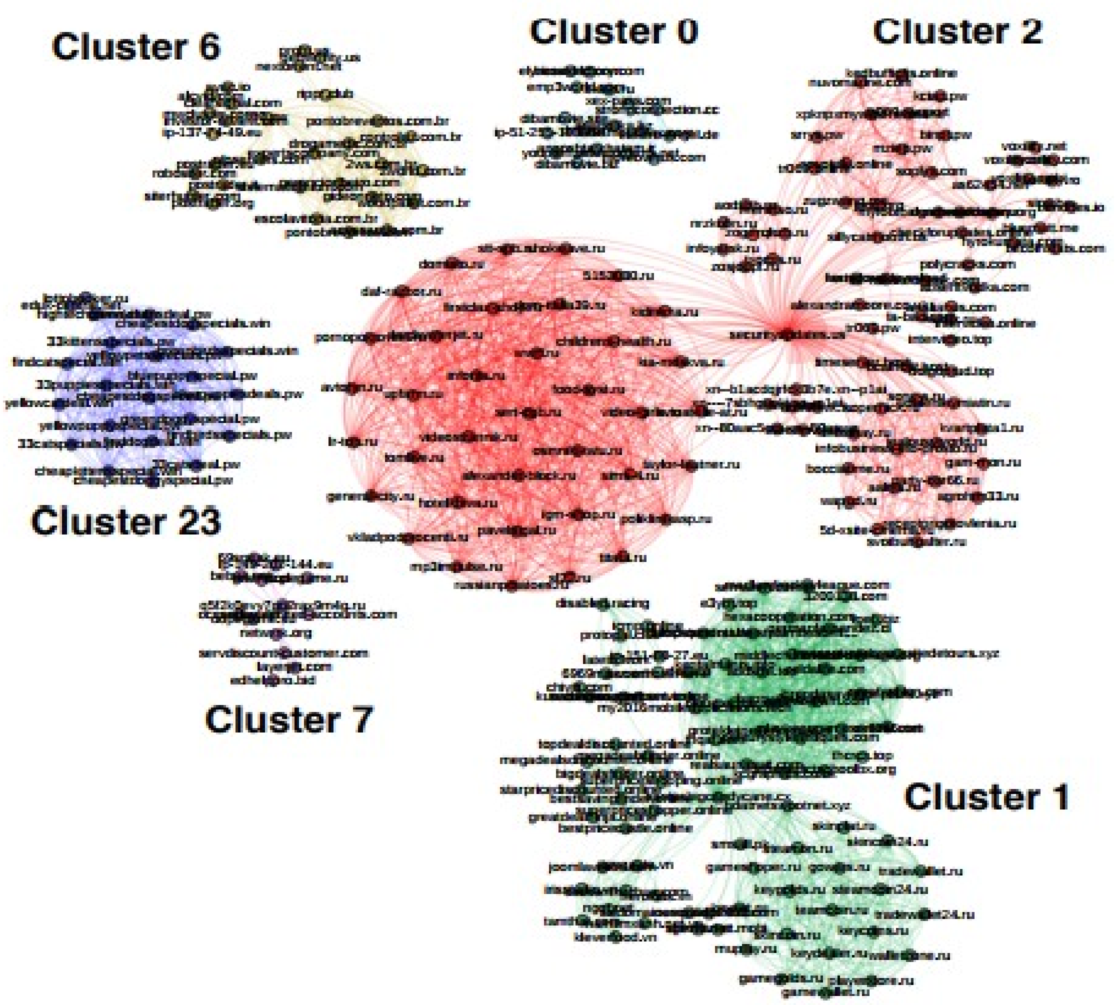
Device Type	# Targeted Passwords	Examples
Camera / DVR	26 (57%)	dreambox, 666666
Router	4 (9%)	smcadmin, zte521
Printer	2 (4%)	00000000, 1111
VOIP Phone	1 (2%)	54321
Unknown	13 (28%)	password, default



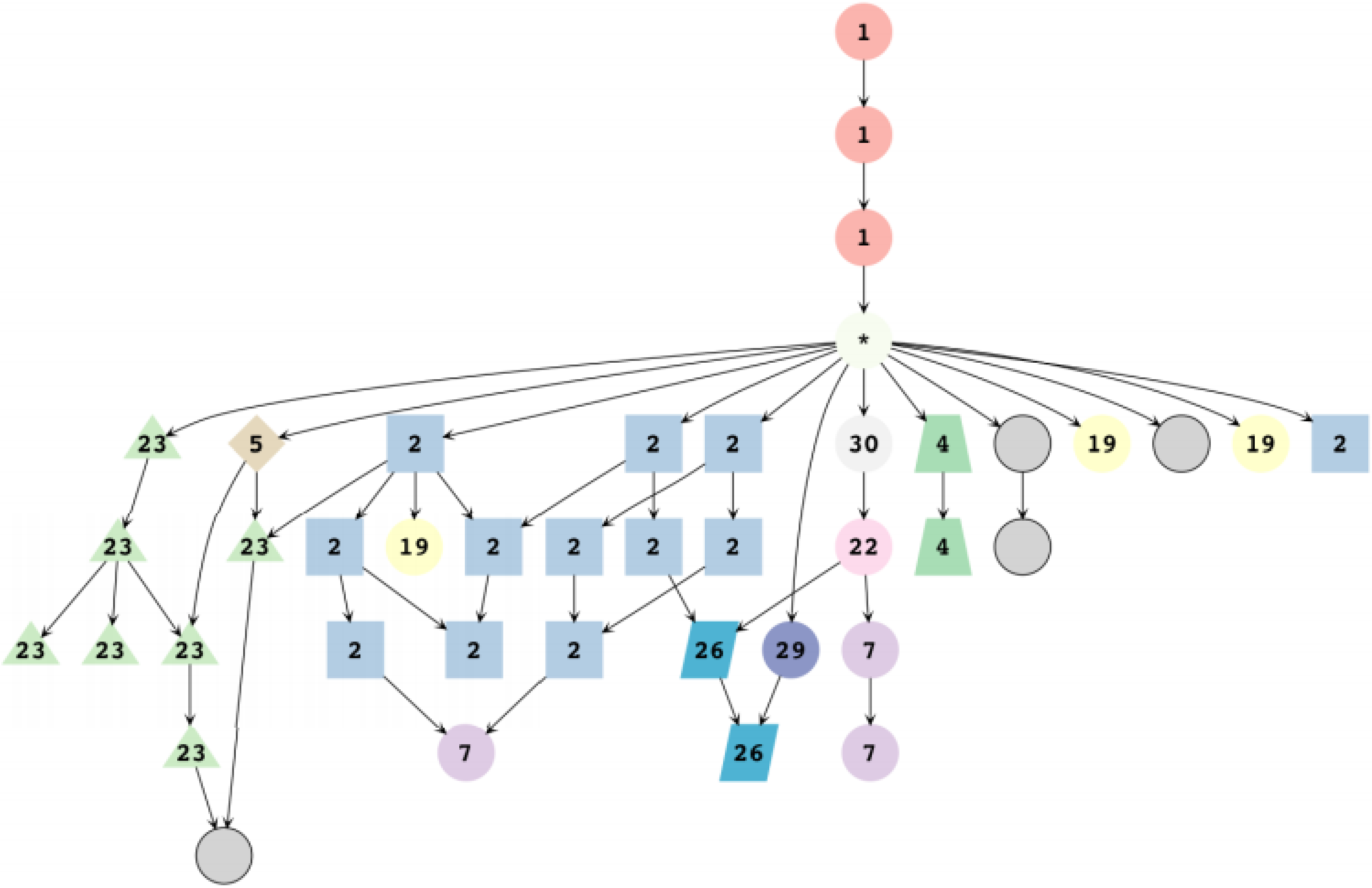
Infected Devices

HTTPS banners

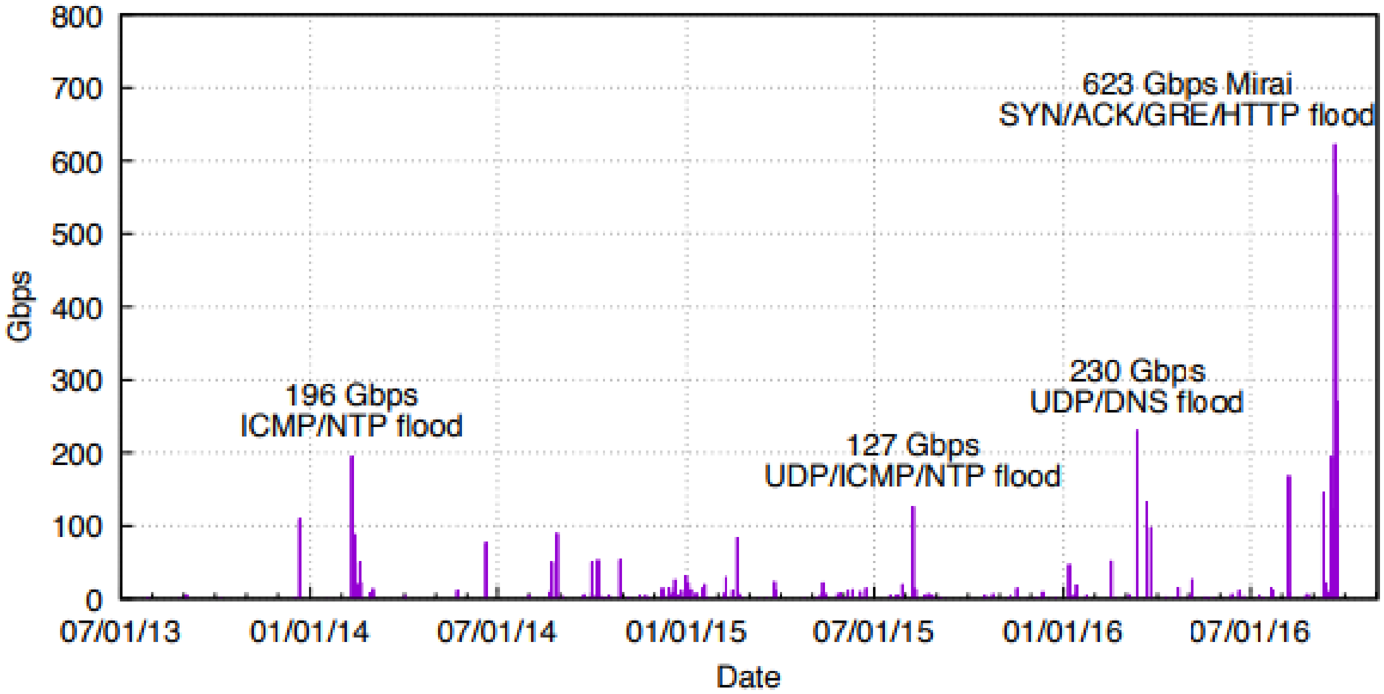
Device Type	# HTTPS banners
Camera / DVR	36.8%
Router	6.3%
NAS	0.2%
Firewall	0.1%
Other	0.2%
Unknown	56.4%



Identificados 33 clusters, acima estão demostrados o Top 6 levando em consideração a quantidade de centros de comando.
Centros de comando são os nós e as arestão são os IP‘s compartilhados

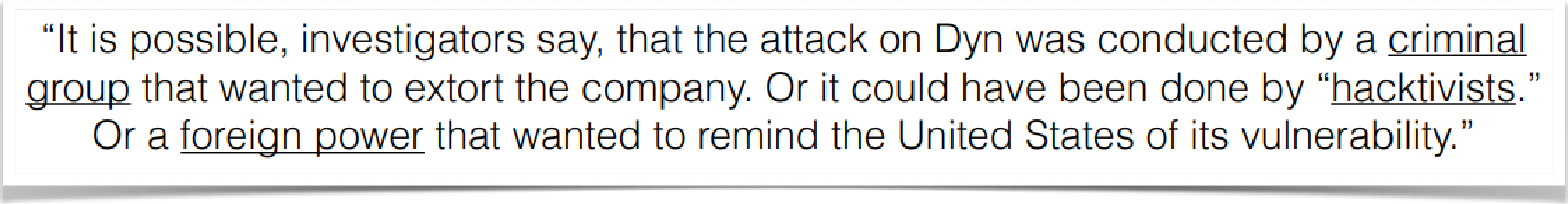


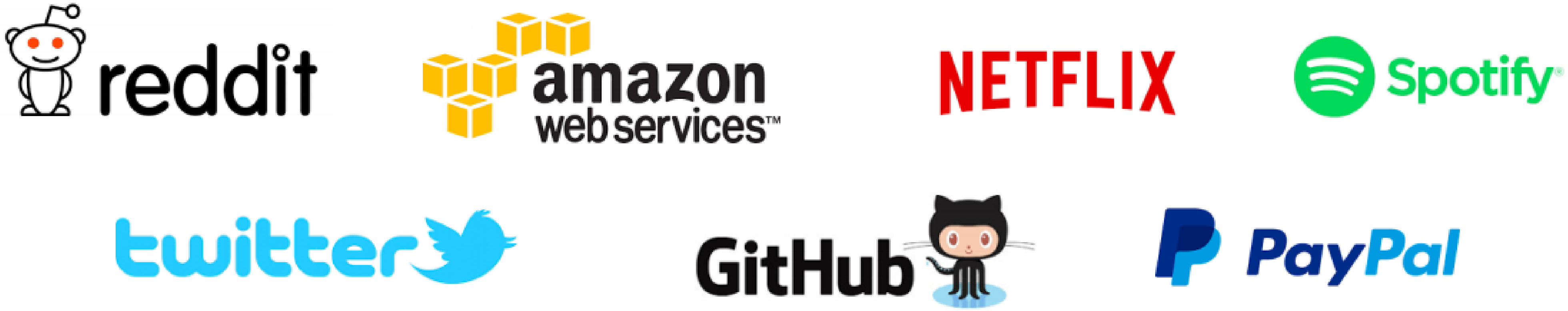
Linhagem de diferentes conjuntos de credenciais relacionadas com seus respectivos clusters.
O nó * representa a publicação do código fonte, que serviu de fundação para as variações.



O Blog de Brain Krebs Krebs on Security já foi vitima de mais de 269 ataques DdoS de 24/07/2012-22/09/2016. O ataque feito pelo Mirai BotNet foi 35 vezes maior que a media dos ataques e é considerado o maior ataque DdoS registrado publicamente.

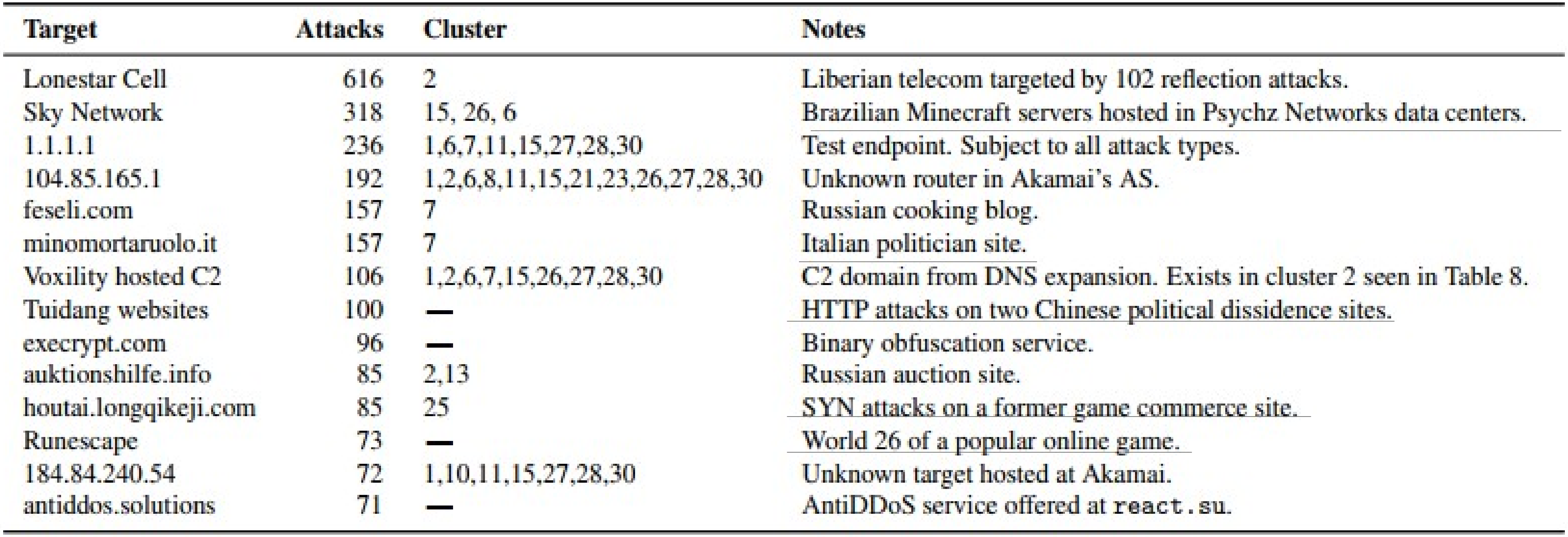
The New York Times


“It is possible, investigators say, that the attack on Dyn was conducted by a criminal group that wanted to extort the company. Or it could have been done by “hacktivists.” Or a foreign power that wanted to remind the United States of its vulnerability.”

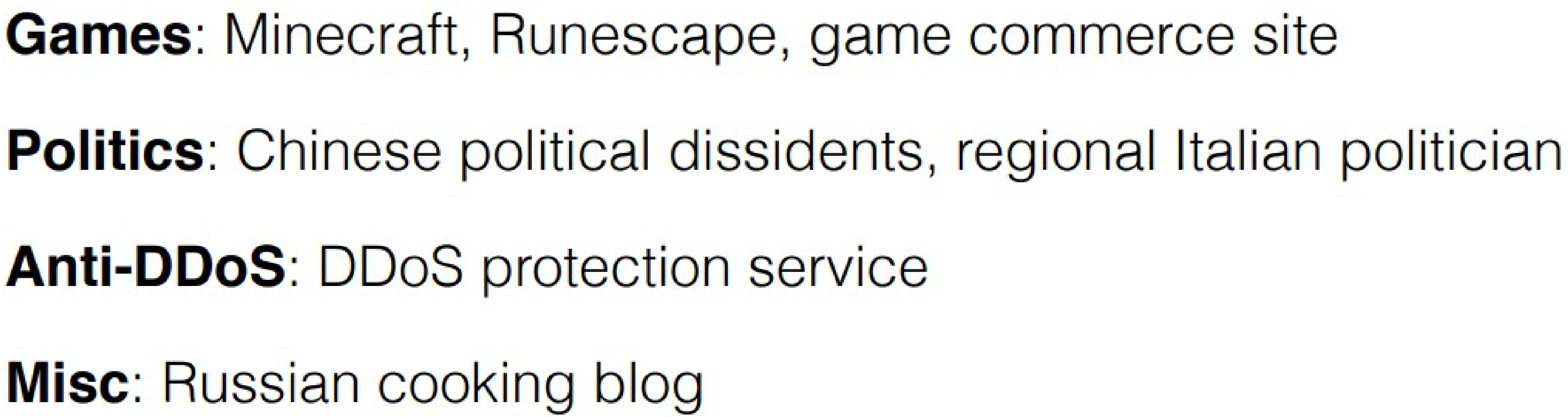


Em 21/10/2016 um grande provedor de DNS sofre uma série de ataques DdoS, derrubando grandes sites.

Uma análise mais profunda mostra que os ataques estavam mirando infraestrutura Dyn e Playstation



Target	Attacks	Cluster	Notes
Lonestar Cell	616	2	Liberian telecom targeted by 102 reflection attacks.
Sky Network	318	15, 26, 6	Brazilian Minecraft servers hosted in Psychz Networks data centers.
1.1.1.1	236	1,6,7,11,15,27,28,30	Test endpoint. Subject to all attack types.
104.85.165.1	192	1,2,6,8,11,15,21,23,26,27,28,30	Unknown router in Akamai's AS.
feseli.com	157	7	Russian cooking blog.
minomortaruolo.it	157	7	Italian politician site.
Voxility hosted C2	106	1,2,6,7,15,26,27,28,30	C2 domain from DNS expansion. Exists in cluster 2 seen in Table 8.
Tuidang websites	100	—	HTTP attacks on two Chinese political dissidence sites.
execrypt.com	96	—	Binary obfuscation service.
auktionshilfe.info	85	2,13	Russian auction site.
houtai.longqikeji.com	85	25	SYN attacks on a former game commerce site.
Runescape	73	—	World 26 of a popular online game.
184.84.240.54	72	1,10,11,15,27,28,30	Unknown target hosted at Akamai.
antiddos.solutions	71	—	AntiDDoS service offered at `react.su`.



Games: Minecraft, Runescape, game commerce site

Politics: Chinese political dissidents, regional Italian politician

Anti-DDoS: DDoS protection service

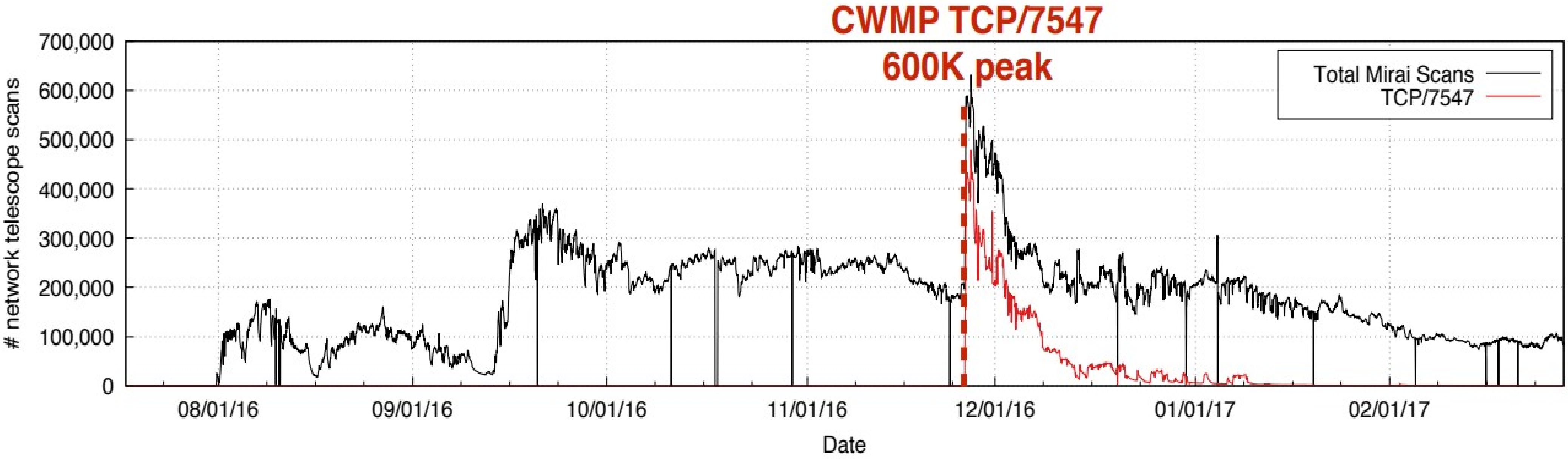
Misc: Russian cooking blog

Suspeitas confirmadas quando jogos viraram um dos alvos principais (~15%).

Jogos, Política, Serviço de proteção a DdoS e ...blog de cozinha RUSSO?

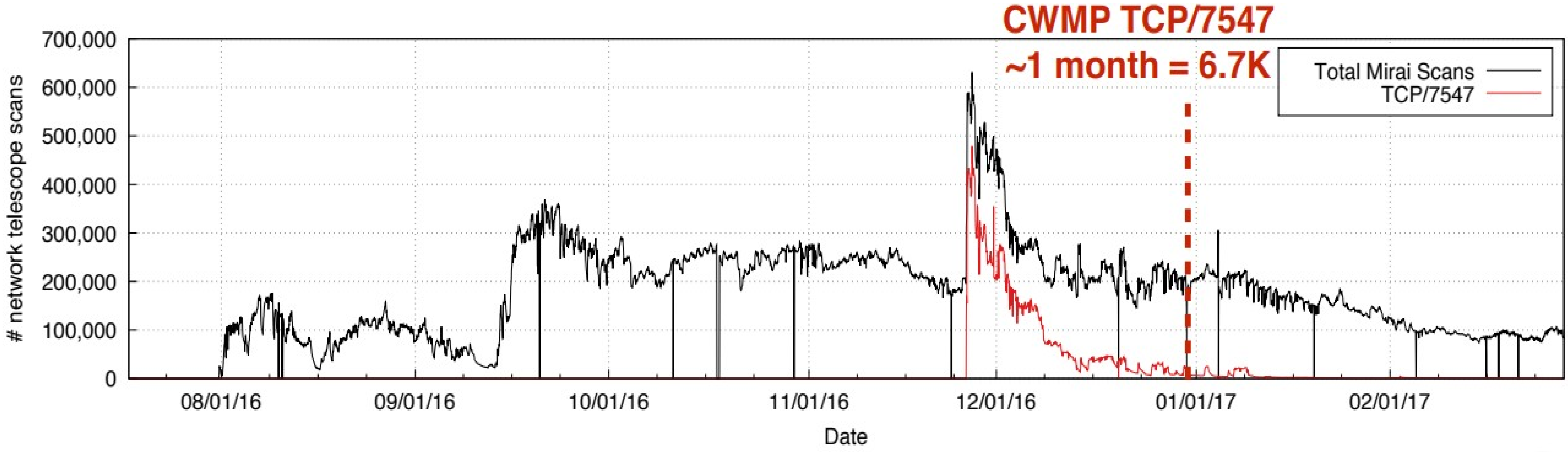
- BotNet relativamente simples.
- Abusa da negligência com relação a segurança na IoT.
- Soluções?

- Reforço na segurança – senhas geradas aleatóriamente, IoT parar de usar portas abertas por padrão.
- Updates automáticos- exemplo Deutshe Telekon



CWMP TCP/7547

600K peak



CWMP TCP/7547

~1 month = 6.7K

- Reforço na segurança – senhas geradas aleatóriamente, IoT parar de usar portas abertas por padrão.
- Updates automáticos- exemplo Deutshe Telekon
- Facilitar a detecção dos dispositovos – saber aonde está o problema.
- End-Of-Life – dispositivos sem suporte e atualizações deixam uma brecha para problemas.

- Mirai – japônes para “O futuro“.
- Gerou muitas variações.
- IoT – Ambiente sem boas práticas de segurança.

QUE TE SIRVA DE LIÇÃO!

Understanding the Mirai botnet

Aluno: Marcio A. C. Sczepanski