RedShift Networks

Unified Communications Threat Management

(RSN UCTM)

3 Ways SIP Botnets impact profitability and Tips for blocking VOIP DDOS

Presented to

SIPNOC 2018

REDSHIFT NETWORKS

Secure Cloud Communication and Collaboration.

RedShift Networks Overview

Headquarters: Silicon Valley - San Ramon CA

Product offering: VoIP Cyber Security, Threat Intelligence Analytics, Fraud Detection & Global SIP Threat Intelligence Network

Market Focus: Service Providers and Large Enterprises

Product Status: Deployed in 40 carrier networks since 2012

Customers: Service Providers

Value Proposition: Patented Proactive Synchronous (Voice) Flow Security Technology

Partners:

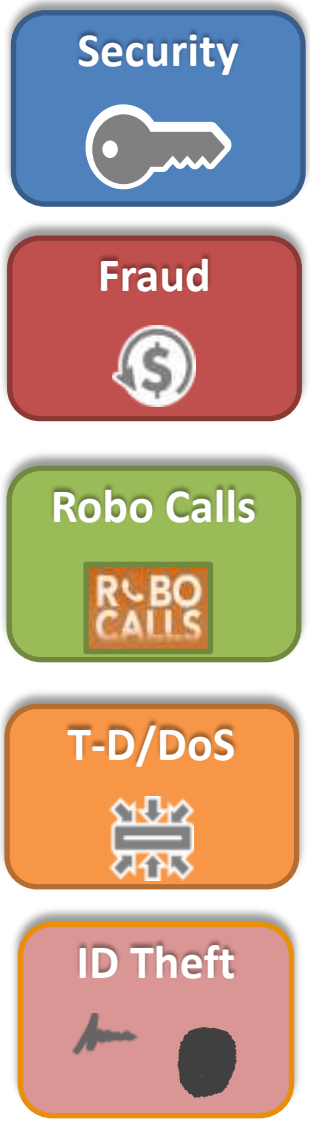
Tier 1 Carriers:

Tier 2 Carriers:

Tier 3 Carriers:

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

RedShift Proven ability to Protect Networks

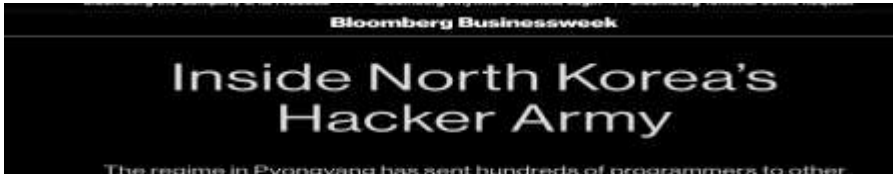


- **40** International and Domestic Carrier Deployments
  - Across US, LATAM, Asia and Europe
- Additional Average **10** to **12** Carrier Trials / Proof of Concept (POC)
- 2016 – processed **2M Active sessions** supporting **21.4M Users**
- End of 2017 - **5.7M Active sessions** supporting **44M Users**
  - By End of 2018 approximately 200M users/end points.
- **27M** VoIP Security threat **"alerts"** across installed base
- **13K** Fraud **"incidents" per year** - approximately 250 per week
- Over **5K SIP BotNets** targeting each UCTM on a continuous basis

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Cyber Attacks are everywhere – US$2T in global losses

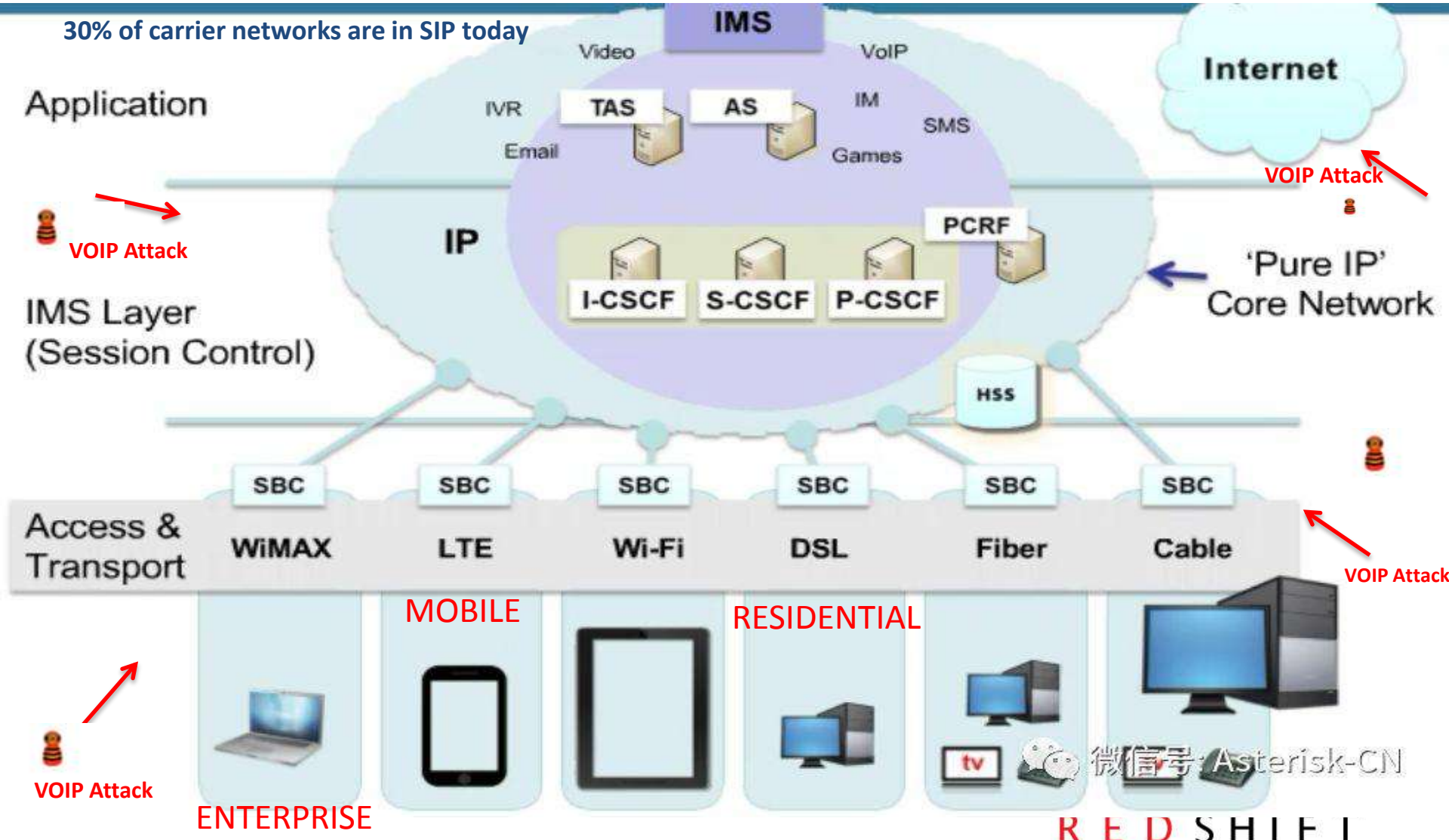
($220B Cyber Security Industry)



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

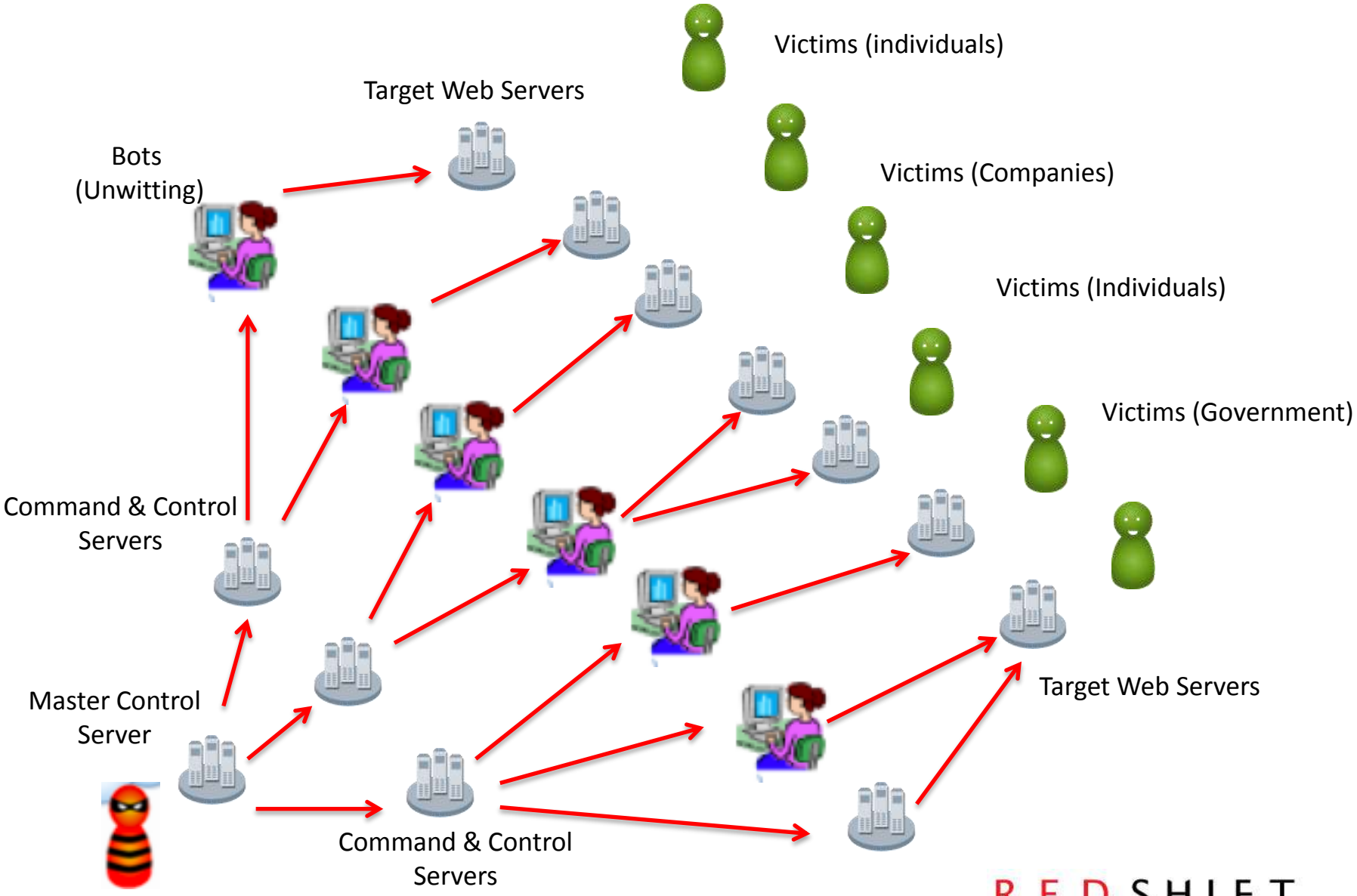
Entire Communications industry moving SIP/VOIP technologies (Enterprise & Carriers)

Carriers to spend $500B on 5G technology and Security is very important



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

What are BotNets?



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

The most dangerous global botnets

- Mariposa
  - 1M systems compromised via Malware to get credit card information, personal data etc thru DOS and Email Spam, 800K personal information compromised. Continued for 5 years
- Mirai (2016)
  - Teen hackers compromised IOT devices and left much of internet inaccessible in East Coast – Via Default passwords and attacked DNS service for major website (DYN)
- Conficker
  - Infected 15M computers in 190 countries via weak passwords and windows vulnerabilities (Updated AV would fix this).
- Necurs (2012) –
  - Generates 60% of the global SPAM (email that missed VOIP Call)
- Zeus (2007) –
  - Trojan Malware affecting Windows computers to steal passwords – DOT, BofA, Oracle, Cisco..
- Starwars (2013) –
  - 350K fake twitter accounts created by this botnet
- WireX Android Botnet (2017) -
  - Compromises Android Smartphones - runs malicious apps and creates DDOS attacks

Financial loss cause by Global Botnets

Suspected gang behind the $850 million Butterfly botnet arrested

13 DEC 2012 1

MIRAI BOTNET ATTACK COSTS COMPANIES HUNDREDS OF MILLIONS

October 26, 2016 Rich Umbach

Over the weekend, you may have noticed that popular sites like Twitter, Spotify, Reddit, The New York Times, Pinterest, PayPal and other major websites were inaccessible. This downtime across the internet can be attributed to a malware known as "Mirai."

Conficker's estimated economic cost? $9.1 billion

In a recent blog post, the Cyber Secure Institute claims that based on their previous studies into the average cost of such malware attacks, the economic loss due to the Conficker worm could be as high as $9.1 billion.

By Dancho Danchev for Zero Day | April 23, 2009 -- 11:41 GMT (04:41 PDT) | Topic: Security

Crackdown on Mariposa: Botnet Infected 13 Million PCs

APPS: SECURITY

Necurs Botnet: Halloween's Nightmare of Malicious Spam

Main Site → Blog → Apps: Security → Necurs Botnet: Halloween's Nightmare of Malicious Spam

Where are the attacks coming from?

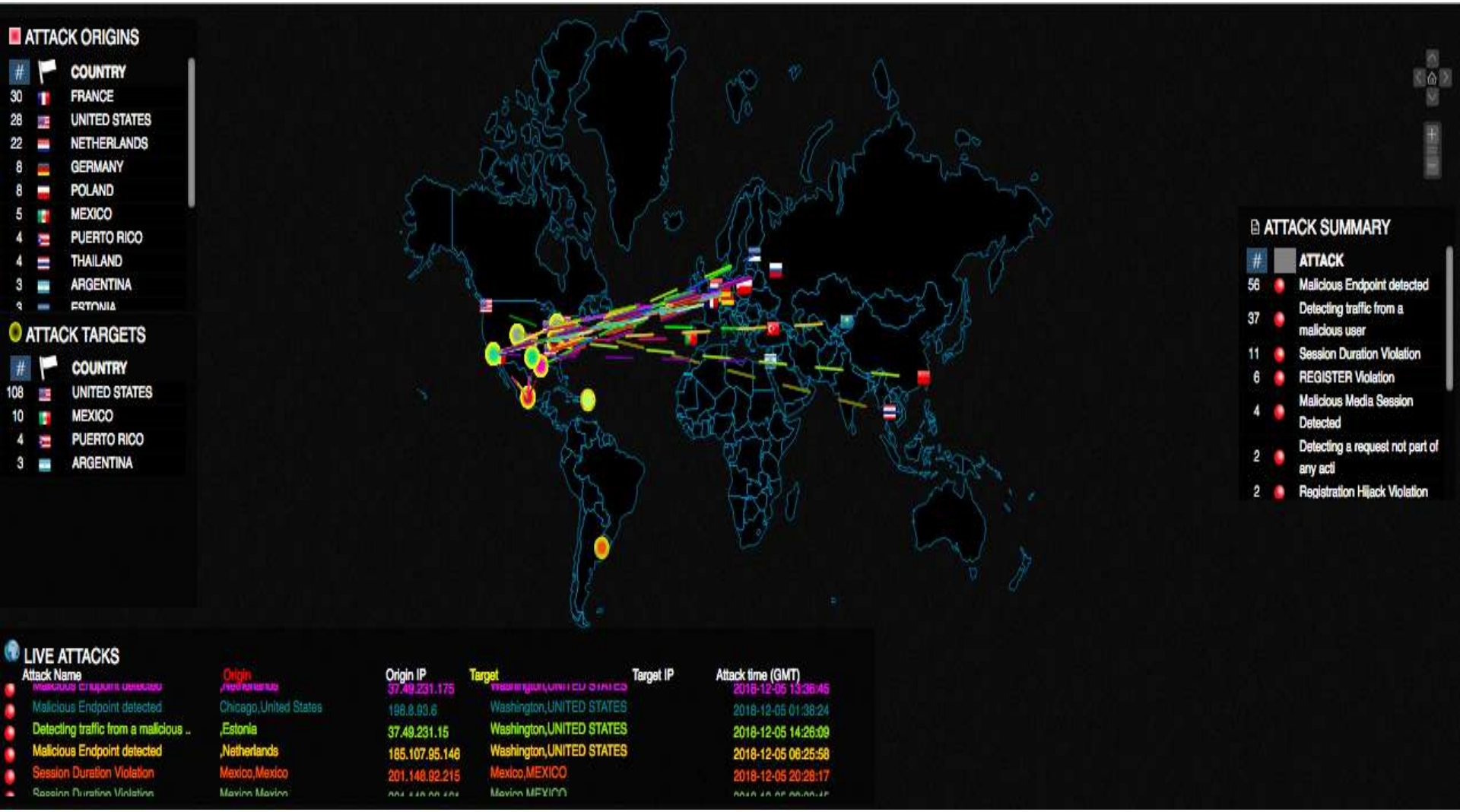
SIP Botnet Threat Intelligence 2012 to 2018

2015/2018
Much of the attack activity has now moved into Western Europe and USA

2013/2014
Most of the attack activity moved into Eastern Europe and Middle East

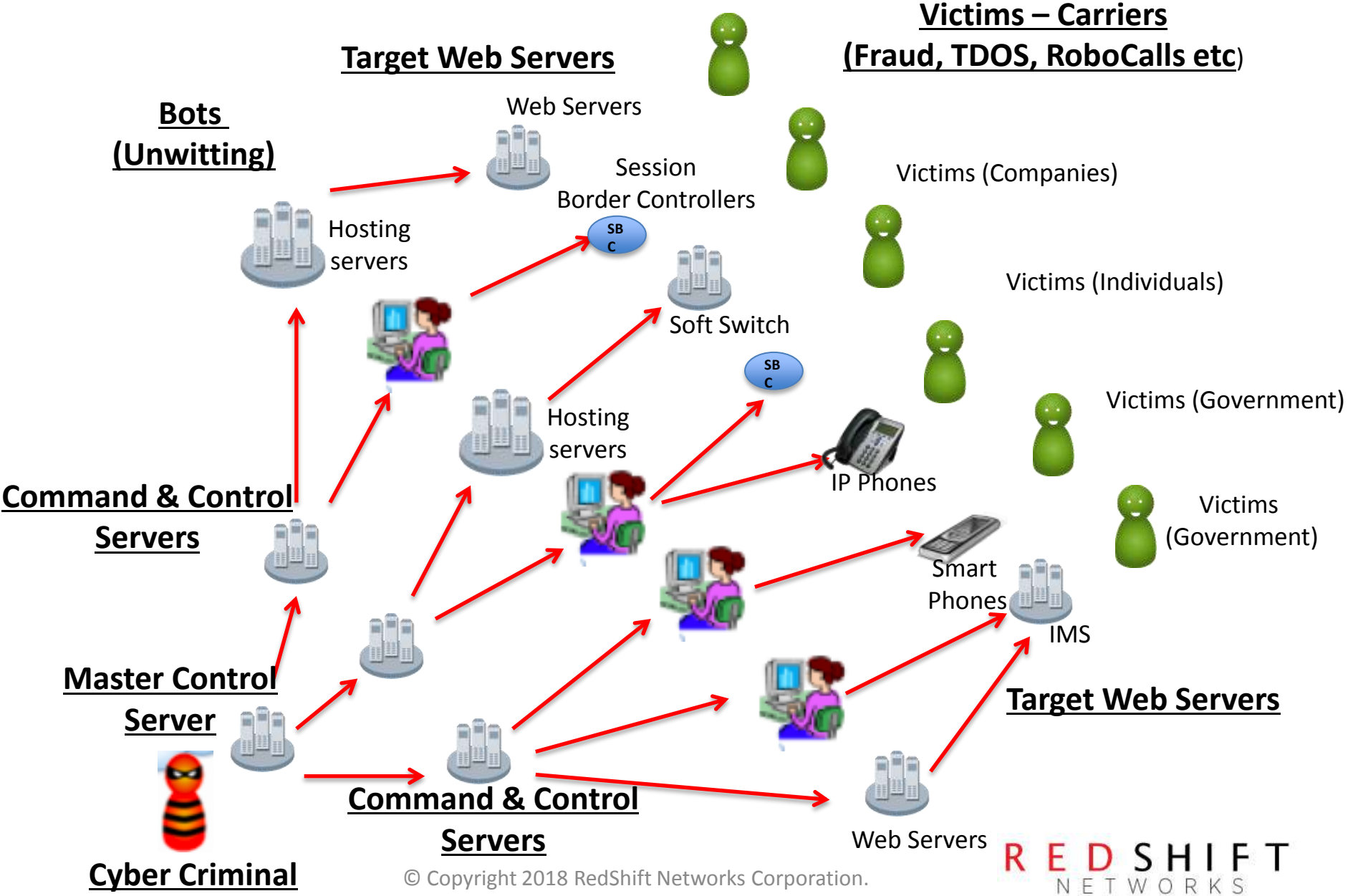
2012
Most attack activity From China, Hong Kong and Taiwan

RedShift Honeypots & customers around the world



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

SIP Botnets



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

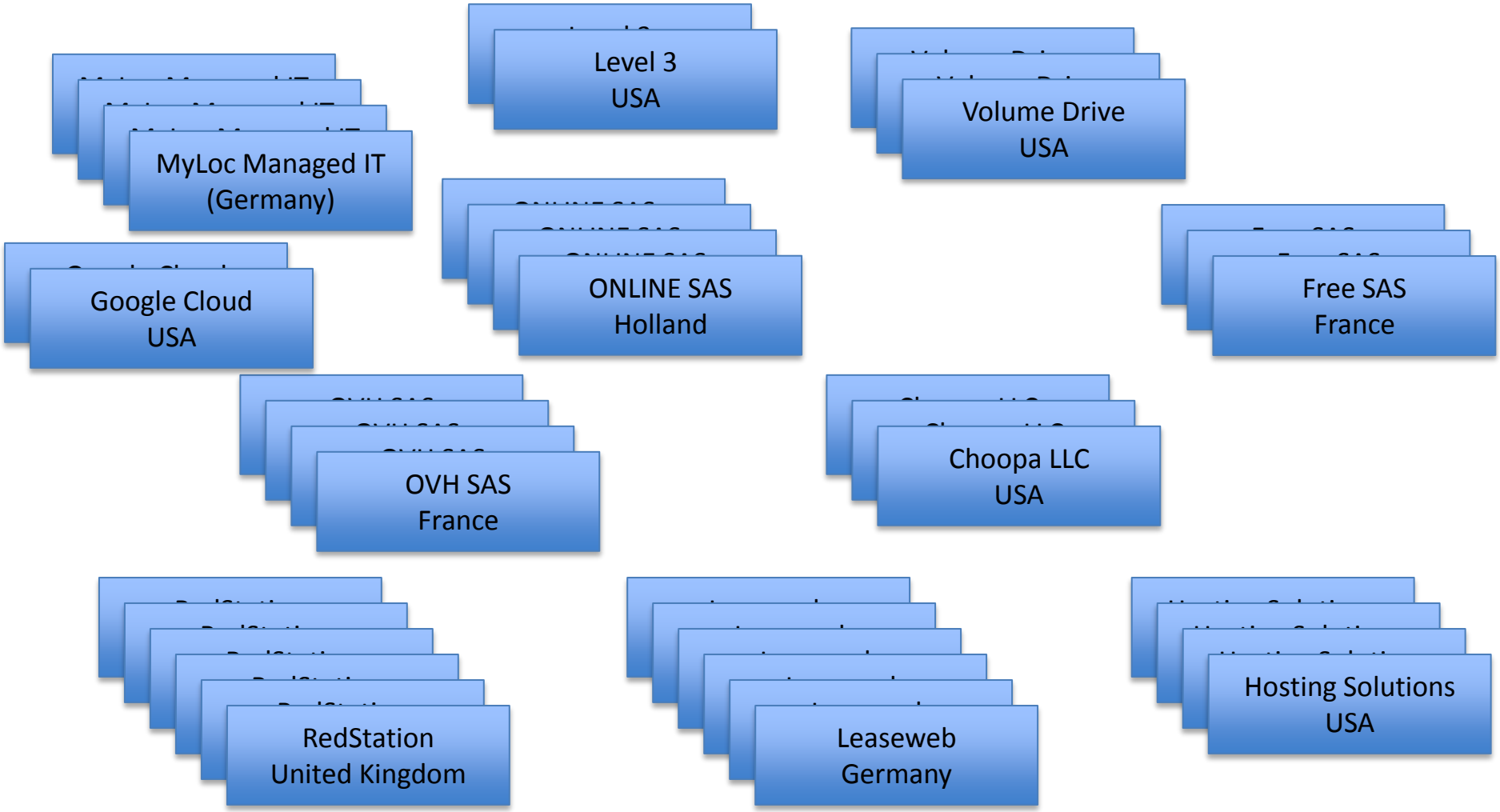
Why are SIP Botnets are so dangerous?

- Fraud Attackers - $29B problem (CFCA 2017 report)
  - IP PBX Hacking - IRSF Fraud
  - Wangiri Fraud - Subscription Fraud
  - Other attacks:
    - International Call Forwarding - Traffic Pumping
    - SIP Traffic By Pass - Illegal User Agents
- Robocalls – Causes $9.5 Billion in losses
  - FCC regulatory framework
- TDOS attacks – Average of $2.5M lost in each attack
- Other attacks – 40,000 attacks detected
  - Fuzzing attacks - Data Loss via voice channel (RTP)
  - Fake Call Teardown attack - Voice Phishing attack
  - Voicemail attacks - Eavesdropping attacks

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Where are the SIP Botnet's coming from –

Hosting, Peering and Cloud Services all over the world
(Mostly Unwitting)



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

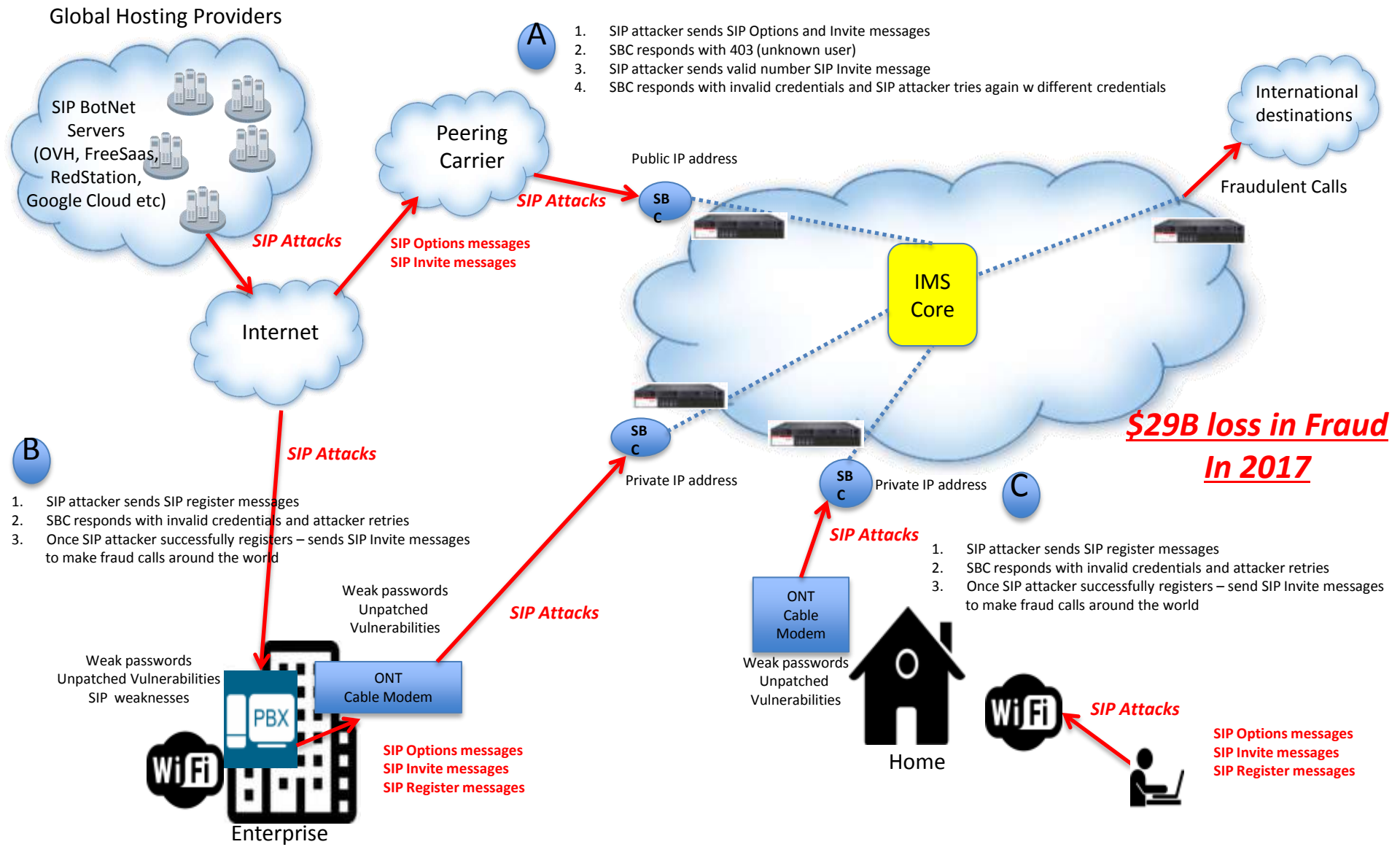
Review of SIP BotNets from around the world

(real world SIP BotNets targeting our carrier customers – 31M attacks)

	Bad_IP	Organization	Country	City	Number of targets	Alert_Types
2	212.83.148.70	ONLINE SAS	France		23	Detecting traffic from a malicious user
3	222.255.100.25	Vietnam Posts and Telecommunicatio	Viet Nam	Hanoi	23	Detecting traffic from a malicious user
4	96.4.166.79	Education Networks of America	United States	Martin	22	Detecting traffic from a malicious user
5	194.44.216.57	Uarnet	Ukraine	Lviv	22	Detecting traffic from a malicious user
6	95.213.164.2	OOO Network of data-centers Selecte	Russian Federation	Moscow	20	Detecting traffic from a malicious user
7	212.129.20.175	ONLINE SAS	France		20	Detecting traffic from a malicious user
8	212.129.36.27	ONLINE SAS	France		19	Detecting traffic from a malicious user
9	46.17.46.71	LLC Baxet	Russian Federation		18	Detecting traffic from a malicious user
10	46.29.161.74	LLC Baxet	Russian Federation	Moscow	18	Malicious Endpoint detected,Detectin
11	62.4.15.172	ONLINE SAS	France		18	OPTIONS SIP scan,Detecting traffic fro
12	82.99.219.36	Pars Online PJS	Iran		18	Detecting traffic from a malicious user
13	82.103.129.48	EASYSPEEDY	Denmark		18	Detecting traffic from a malicious user
14	163.172.126.8	ONLINE SAS	France		18	Detecting traffic from a malicious user
15	192.3.8.212	ColoCrossing	United States	Buffalo	18	Detecting traffic from a malicious user
16	199.48.225.70	Mexico Internet Exchange	United States	San Ysidro	18	Malicious Endpoint detected,Detectin
17	37.49.231.14	Estro Web Services Private Limited	Netherlands		17	Detecting traffic from a malicious user
18	38.121.232.9	Cogent Communications	United States	New York	17	Detecting traffic from a malicious user
19	66.206.35.98	Turnkey Internet	United States	Latham	17	Detecting traffic from a malicious user
20	158.69.108.225	OVH Hosting	Canada	MontrÃ©al	17	Detecting traffic from a malicious user
21	176.32.32.79	BX-NETWORK	Russian Federation	Moscow	17	Malicious Endpoint detected,Detectin
22	207.244.157.26	Wowrack.com	United States	Seattle	17	Detecting traffic from a malicious user

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Use Case – Fraud - SIP attacks targeting SBCs



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Real World Examples of SIP Botnets in Carrier Networks

- SIP Botnet sends INVITE Messages

Suspicious IP Address and Hosting Service

Alert Name	Category	Src Ph	Dest Ph	Time	Severity	Source IP	Src Country
Malicious Endpoint detected	External	admin	0315312207899	Wed Dec 05 10:22:31 EST 2018	High	185.107.94.54	NETHERLANDS
Malicious Endpoint detected	External	+1-800-900-1000	918282292201	Sun Dec 02 22:15:34 EST 2018	High	185.107.94.54	NETHERLANDS

Alert Report Reason:

A message received with Malicious User Agent Header.Malicious User Agent -->sipcli/v2.2

User Action:

Check services at at the server if required

Packet Info:

```
INVITE sip:0315312207899@[redacted]SIP/2.0
via: SIP/2.0/UDP 185.107.94.54:5076;branch=z9hG4bK-4335e91a28dfe920f1021824f592b898;rport
max-forwards: 70
from: "admin" <sip:admin@[redacted];tag=d61ef957
to: "0315312207899" <sip:0315312207899@[redacted]>
call-id: 4335e91a28dfe920f1021824f592b898
cseq: 1 INVITE
contact: <sip:admin@185.107.94.54:5076>
allow: INVITE, MESSAGE, ACK, CANCEL, BYE
content-length: 270
content-type: application/sdp
reason: null
user-agent: sipcli/v2.2
```


REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Real World Examples in Carrier Networks

- SIP Botnet tries to REGISTER

Suspicious IP Address and Hosting Service

☐	REGISTER Violation	62.210.246.172	FRANCE	Paris	Free SAS	Medium	61	Wed Dec 05 2018
☐	REGISTER Violation	212.83.178.209	FRANCE	Paris	Free SAS	Medium	10	Wed Dec 05 2018

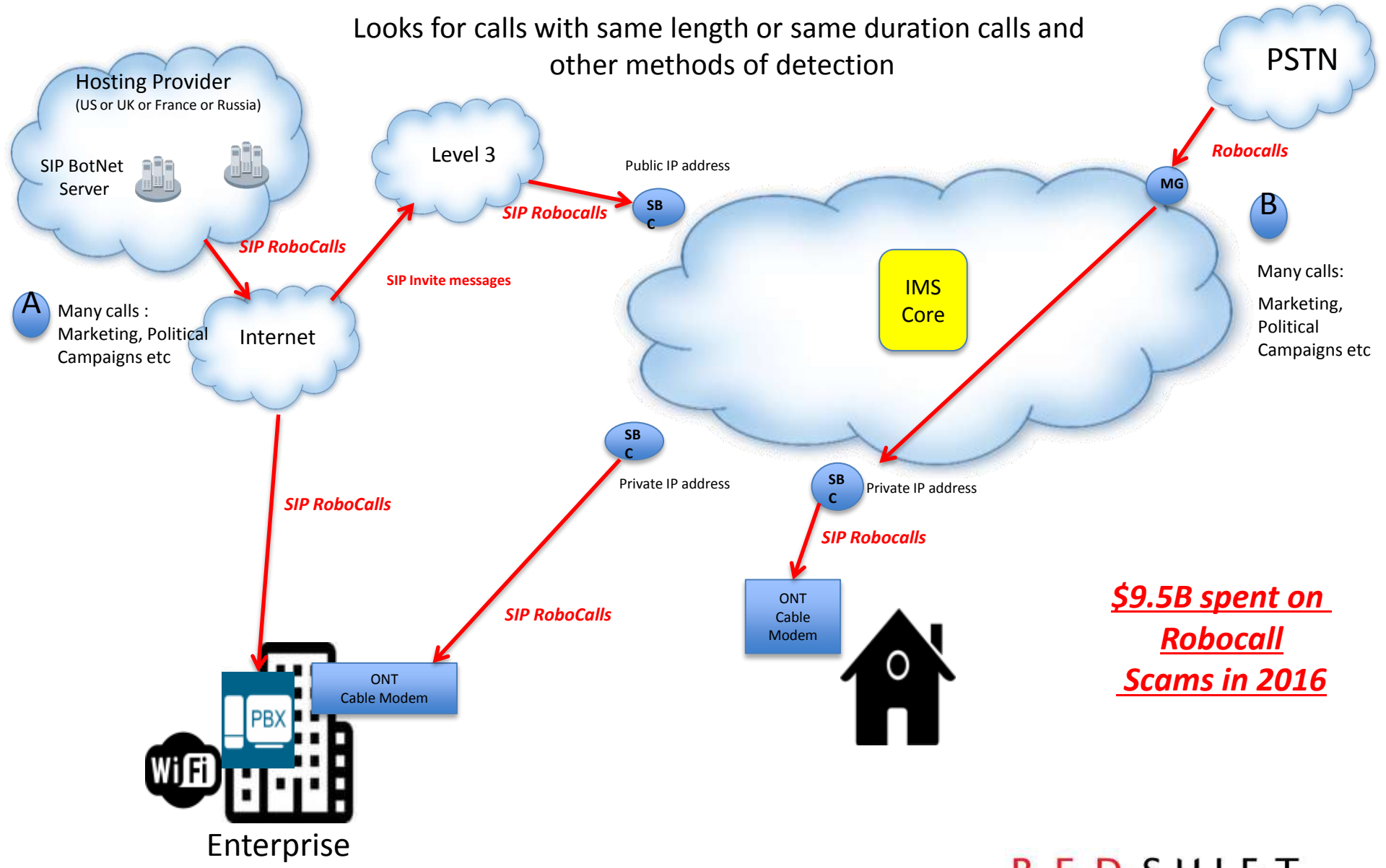
- SIP Botnet tries variation of numbers

Alert Name	Category	Src Ph	Dest Ph	Time	Severity	Source IP	Src Cou
REGISTER Violation	External	1013	011441594800002	Wed Dec 05 14:17:27 EST 2018	Medium	62.210.246.172	FRANCE
REGISTER Violation	External	1013	900114417853300	Wed Dec 05 13:53:24 EST 2018	Medium	62.210.246.172	FRANCE
REGISTER Violation	External	1013	701144178533001	Wed Dec 05 13:33:02 EST 2018	Medium	62.210.246.172	FRANCE
REGISTER Violation	External	1012	09441594800002	Wed Dec 05 13:10:43 EST 2018	Medium	62.210.246.172	FRANCE

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Use Case – SIP Robocalls attacks targeting SBCs

Looks for calls with same length or same duration calls and other methods of detection

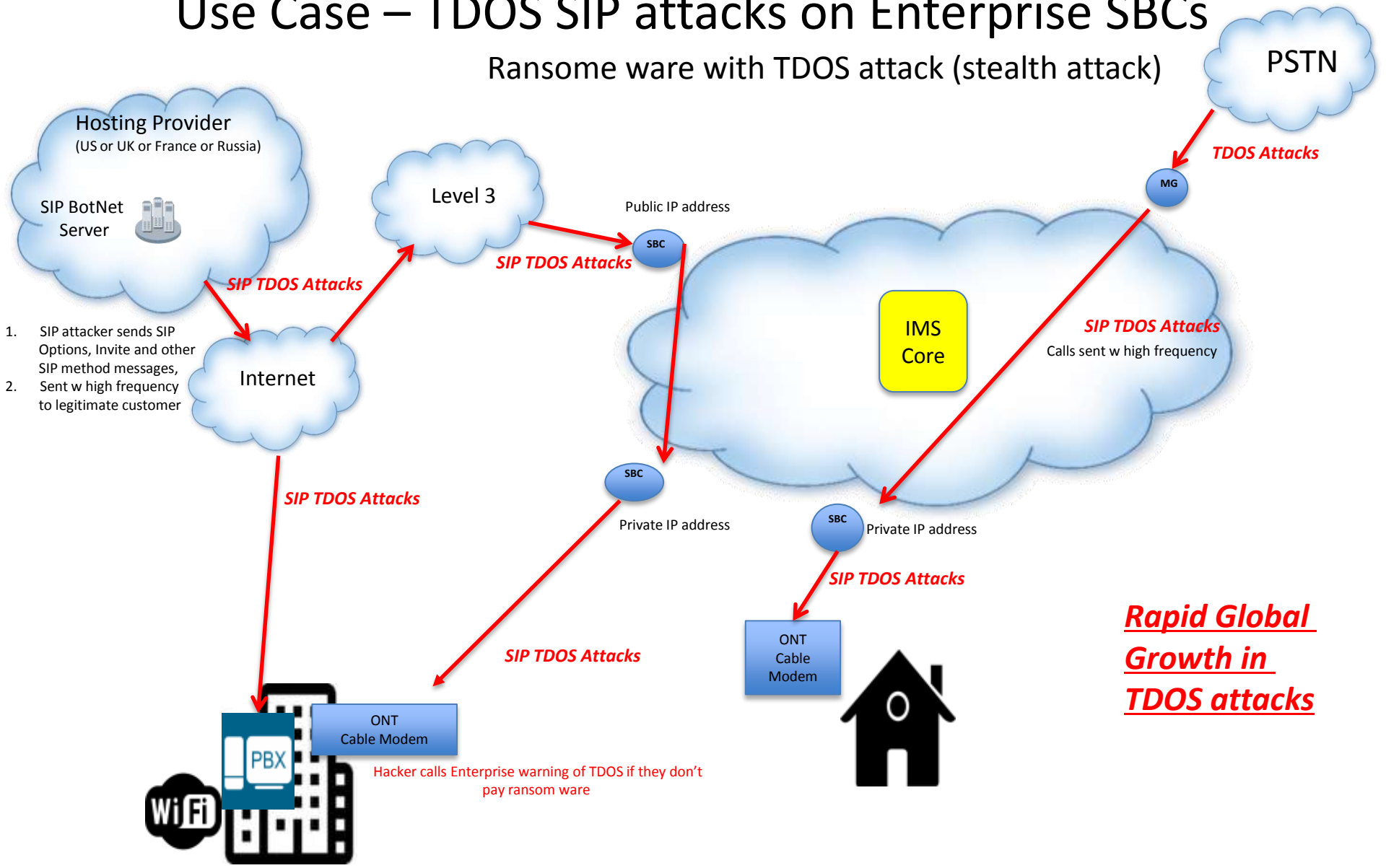


$9.5B spent on Robocall Scams in 2016

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Use Case – TDOS SIP attacks on Enterprise SBCs

Ransome ware with TDOS attack (stealth attack)



Rapid Global Growth in TDOS attacks

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Real world Attack Examples –Other Use Cases

- Fraud and theft of Service
  - Illegal User Agents
  - VoIP BotNets, etc.
  - Can lead to coordinated DoS attack on Voice Network
- Call Short Stopping
  - Calls Forwarded to International Destinations
- SIP Traffic By-Pass
- SIP Stealth based DoS/DDoS
- TDoS on Fax, IVR, Voicemail, Softswitch (TAS)

- Register Storm on SBC
  - Lose of processing resources
- Traffic Pumping
- RoboCall attacks
  - Shake & Stir (FCC)
  - Data Centers
  - Emergency Centers (911, etc.)
- Error Code Alerts – Stress in VoIP elements
- FCC Rural Call Completion Rate reports

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Financial Losses due to VOIP attacks

- Direct Loss due to Fraud
  - $1M loss within 1 hour
  - $6M loss due to illegal user agents
  - $1M loss in 6 months of Call short stopping (Calls forwarded to Intl Dest)
- Ransom ware & TDOS attack caused $50,000 to medium sized enterprise
- Customer dissatisfaction due to
  - network issues and poor telephone service

Loss of Revenue due to Misconfigurations

- Large Enterprise loss of $500k as International traffic mistakenly directed to wrong network

- **SLA penalties w customers**
  - Credits issued up to 25% of revenue due to voice issues
- **Loss of Revenue due to 70% rejection of legitimate calls**
  - $1M in revenue per quarter

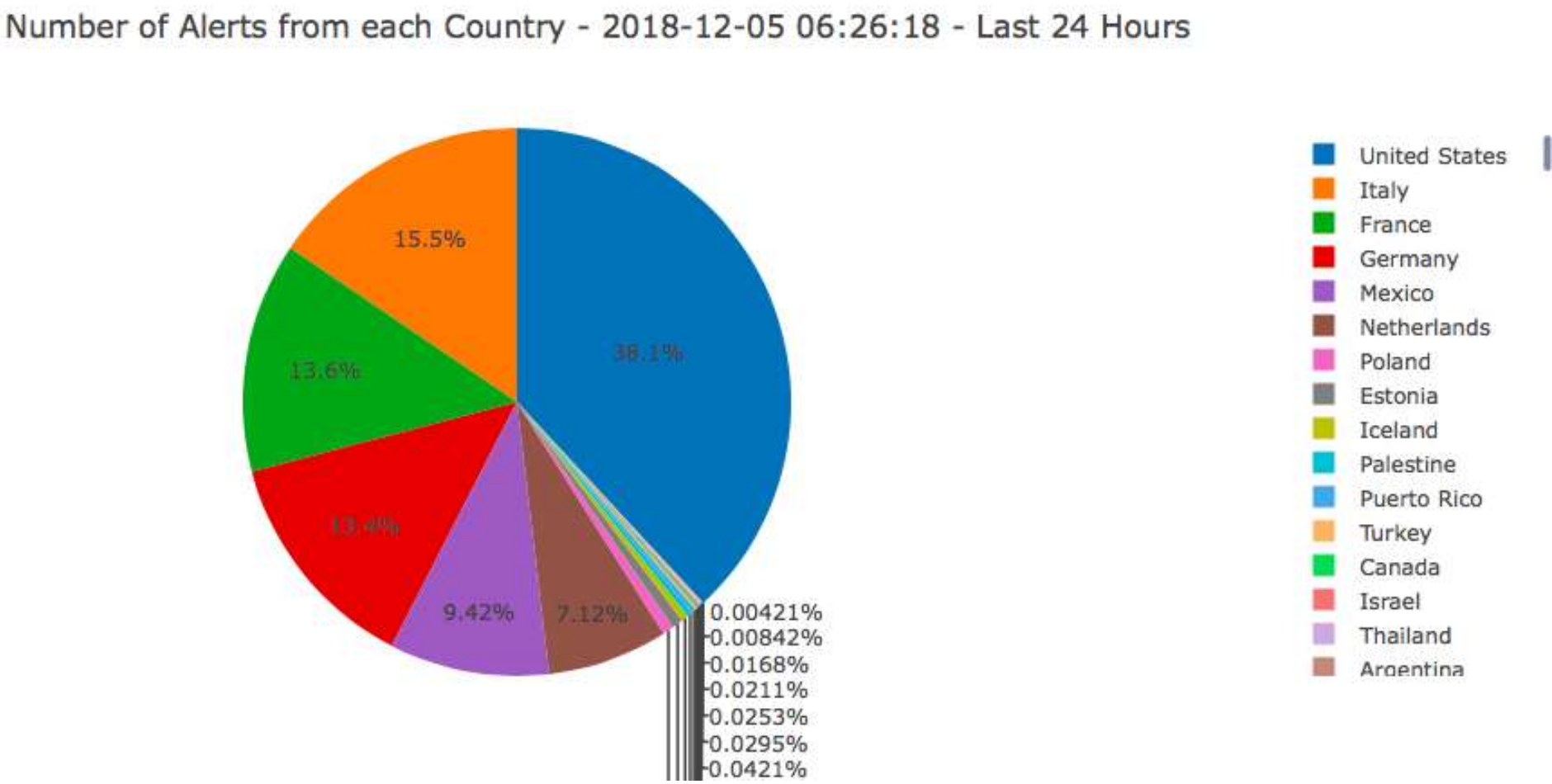
REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

What we saw in last 12 months of these SIP BotNet attacks

(across 40 carriers in Americas)

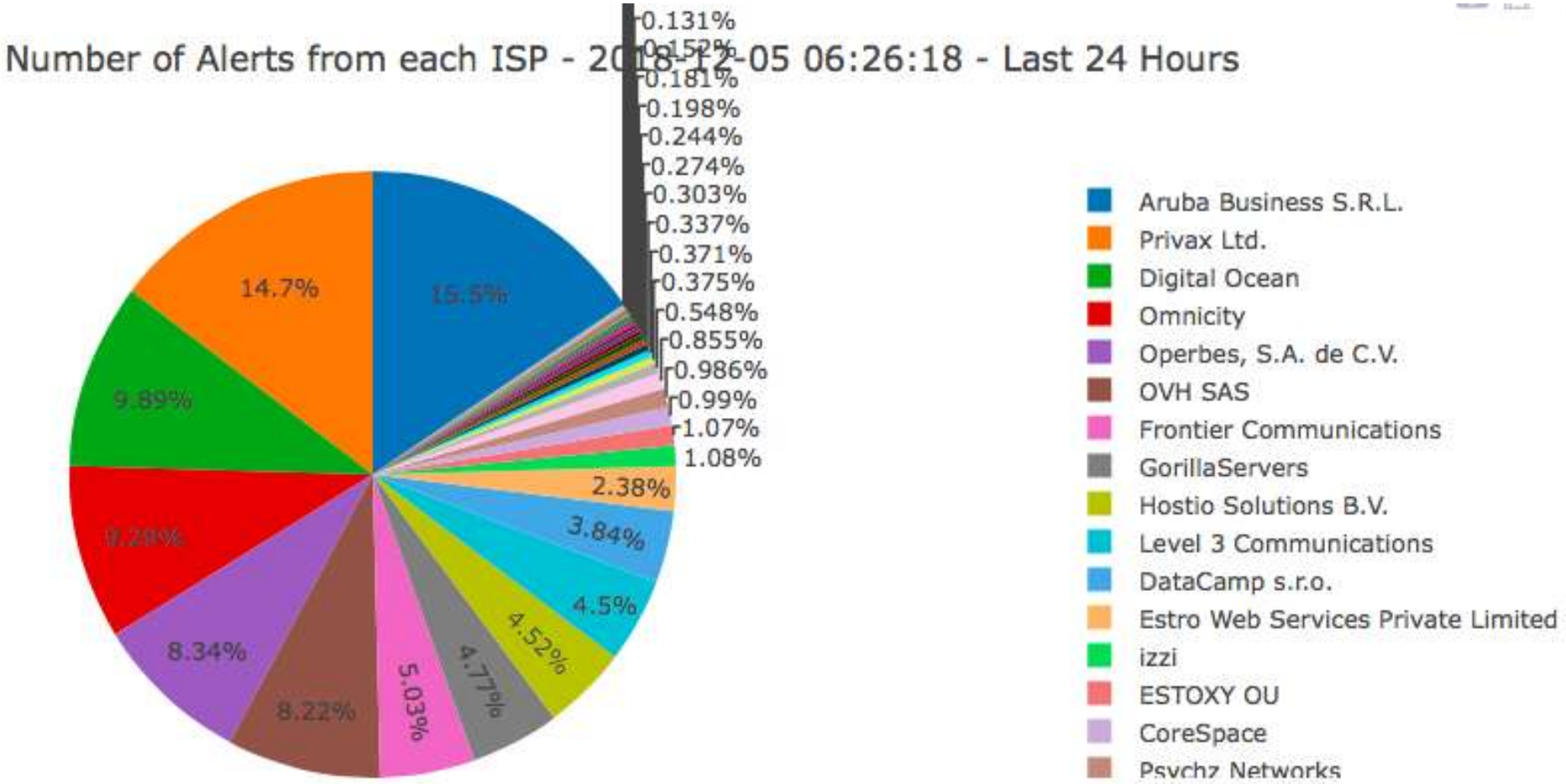
- 31M SIP attacks around world (mostly North America) in 2018
- Around 4000 new unique SIP Botnet IP addresses
- Average of 300 plus new unique SIP Botnet IP addresses per month
  - SIP Botnets are continuously changing
- Mix of attacks from known and unknown Carriers/ISP/Hosting Services:
  - Russia, France, Canada, UK, USA, Holland, Germany etc
- We're researching the different types of Botnets and who they are:
  - Stay tuned!!

Trending data about these SIP Botnets in 2018



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

Sources of SIP Botnets by Carrier



REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

VOIP and UC&C Threat Categories

- **Device and OS Vulnerabilities**
- **Device Configuration Weakness**
- **IP/TCP Network Infrastructure Weakness**
- **VOIP & UC Protocols Implementation Vulnerabilities**
- **VOIP & UC Network Eavesdropping**
- **VOIP & UC Network Interception and Modification**
- **Fuzzing Attacks**
- **Voice & UC Denial of Service (VDOS/UCDOS) Attacks**
- **Signaling Manipulation Attacks**
- **Media Manipulation Attacks**
- **SPAM over Internet Telephony (SPIT)**
- **UC Infrastructure Threats (Voice, Media, IM, Web, UC & Collaboration)**
- **UC Application Layer Threats**
- **Data ➔ Voice Threats**
- **Voice Phishing**

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

What carriers should do about these SIP Botnets (free monthly list of bad SIP botnets)

- Ensure SBC doesn't respond to those Bad IP addresses from SIP Botnets (not even with error messages)
- Update phone, SBC, Soft switch and all VOIP elements firmware/software
- Change all passwords away from Default passwords
- Lock down only allowed User Agents w firmware version
- Use encryption if possible.
- Monthly update of SIP botnet (Bad IP addresses) to any carrier that subscribes.
  - Send email to amitava@redshiftnetworks.com

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

VOIP Security Check list – recommended steps

- Internal controls for VOIP/UC systems ensure strong password strength protection
- Employ strong encryption
- VOIP/UC systems be tested against standard penetration & vulnerability testing tools – patched regularly
- Provide detailed Call Logs, Billing logs, Alerts & Events log, Audit & Admin Logs
- Employ strong 2-factor authentication to prevent unauthorized use
- Ensure security and confidentiality of consumer information gathered by VOIP/UC systems
- Protect against any MITM based threats – illegal tampering, routing or modification of user or call records – e.g. Call-ID spoofing, Toll Fraud, SQL Injection
- Protect against unauthorized access to VOIP/UC records
- Provide security of health data stored in Voice Messaging systems
- Prevent sabotage of UC/VOIP services – Identity stealing, escalation – minimize use of soft phones – botnets that can steal data
- Present clean separation of UC VLANs with Data VLANs – Proper Authentication, Authorization, Auditing controls
- Protect eavesdropping of WiFi IP Phone's
- All payment card information using VOIP/UC needs to be encrypted with 2-factor authentication using a Virtual Private Network (VPN)
- Prevent against any voicemail hacking attacks
- Protect against any illegal redirecting or tampering of VOIP traffic
- Prevent illegitimate eavesdropping (or recording) of media traffic

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.

With its' patented advanced correlation engine technology, RedShift Networks is able to holistically combine **SIP Security, Fraud Detection and Network, Application and User layer Analytics** for visibility into anomalous activities, enabling real-time threat mitigation and troubleshooting!

Thank you / Questions

REDSHIFT NETWORKS
Secure Cloud Communication and Collaboration.