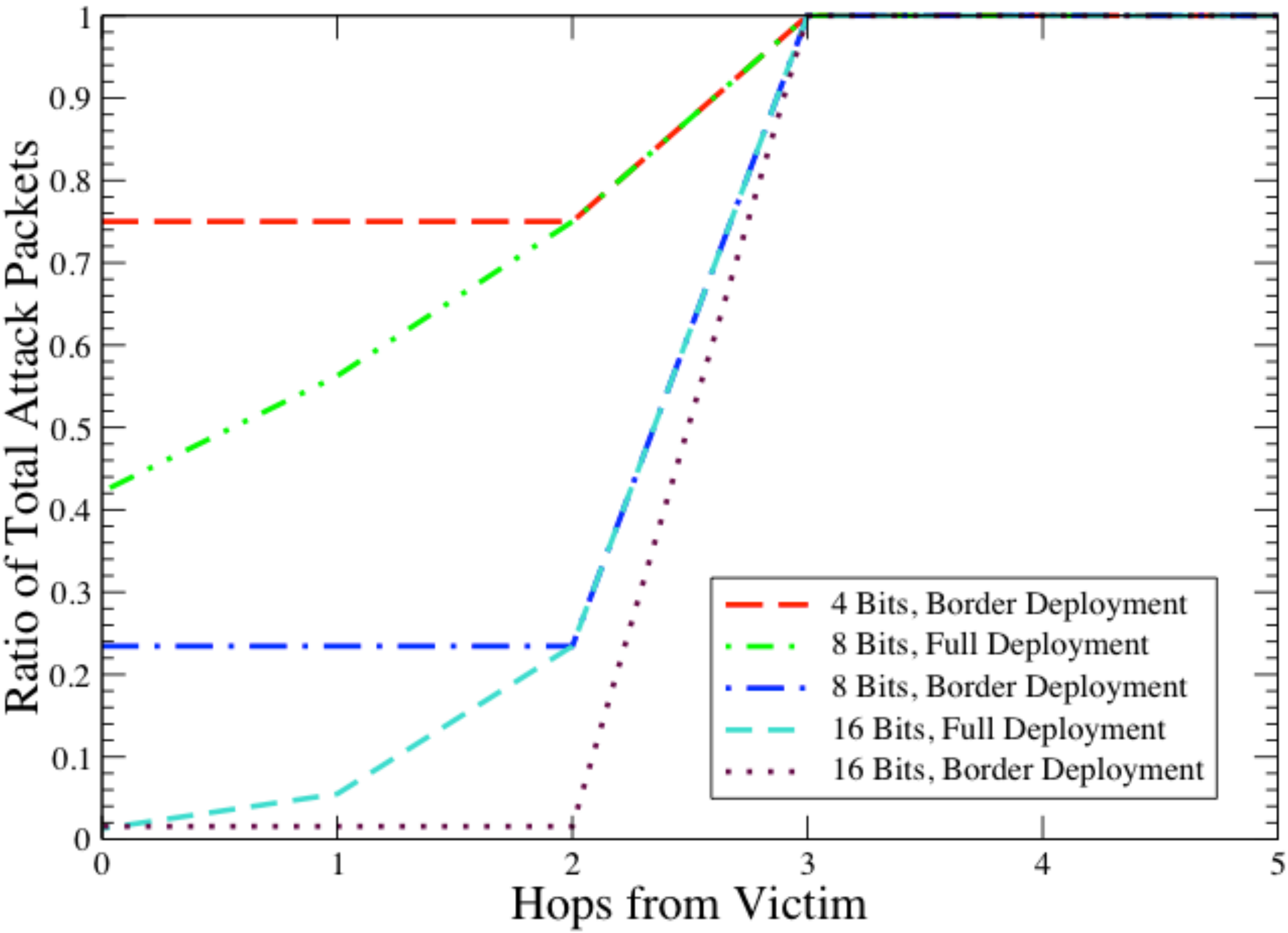

Ratio of Total Attack Packets
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
Hops from Victim
0
1
2
3
4
5
4 Bits, Border Deployment
8 Bits, Full Deployment
8 Bits, Border Deployment
16 Bits, Full Deployment
16 Bits, Border Deployment

The probability that the client can connect after k tries is:

$$\begin{aligned} &P(\text{ connect after k tries}) \\ &\quad = 1 - (1 - P(\text{connect after 1 try}))^k \\ &\quad = 1 - (1 - (1 - \epsilon_i)^i)^k \end{aligned}$$

the required number of connection attempts is:

$$k = \frac{\log(1 - P(connect))}{\log(1 - (1 - \epsilon_i)^i)}$$

A nice feature of this formula is that the expected number of connection attempts depends logarithmically on the connection probability, which indicates that even for large ϵ_i, a determined client can get a connection after a moderate waiting time.

Attack Mitigation Techniques

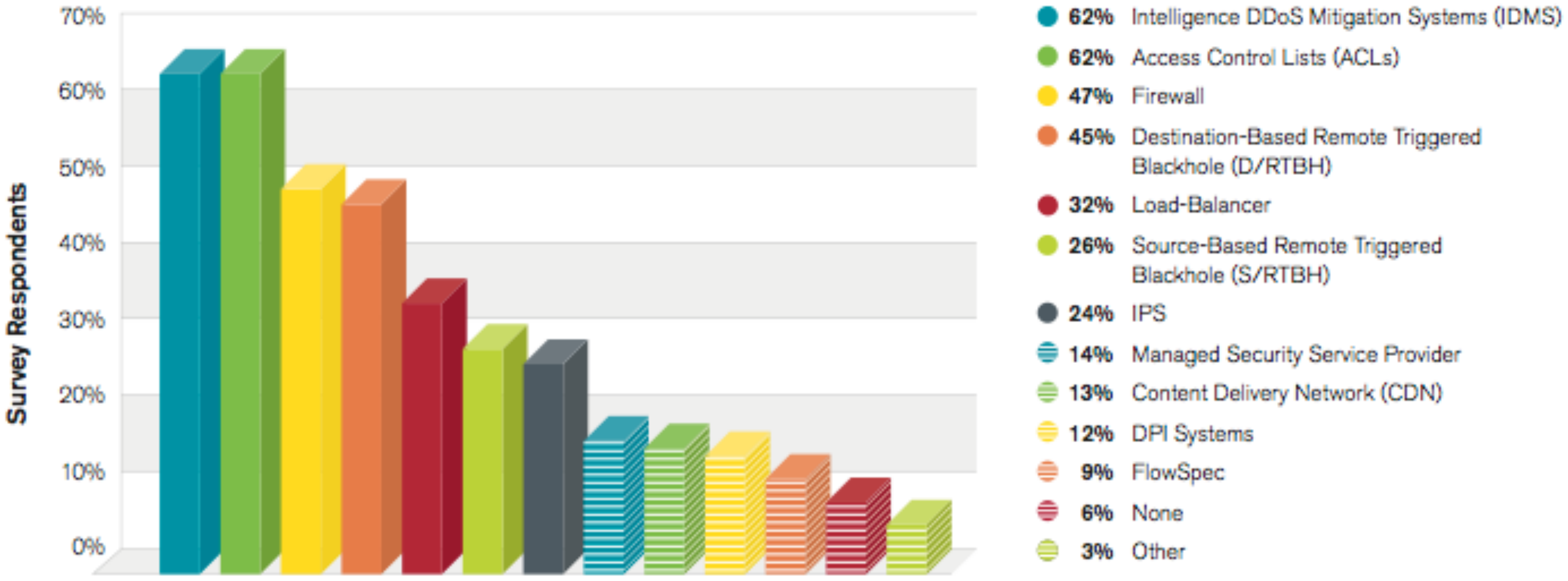
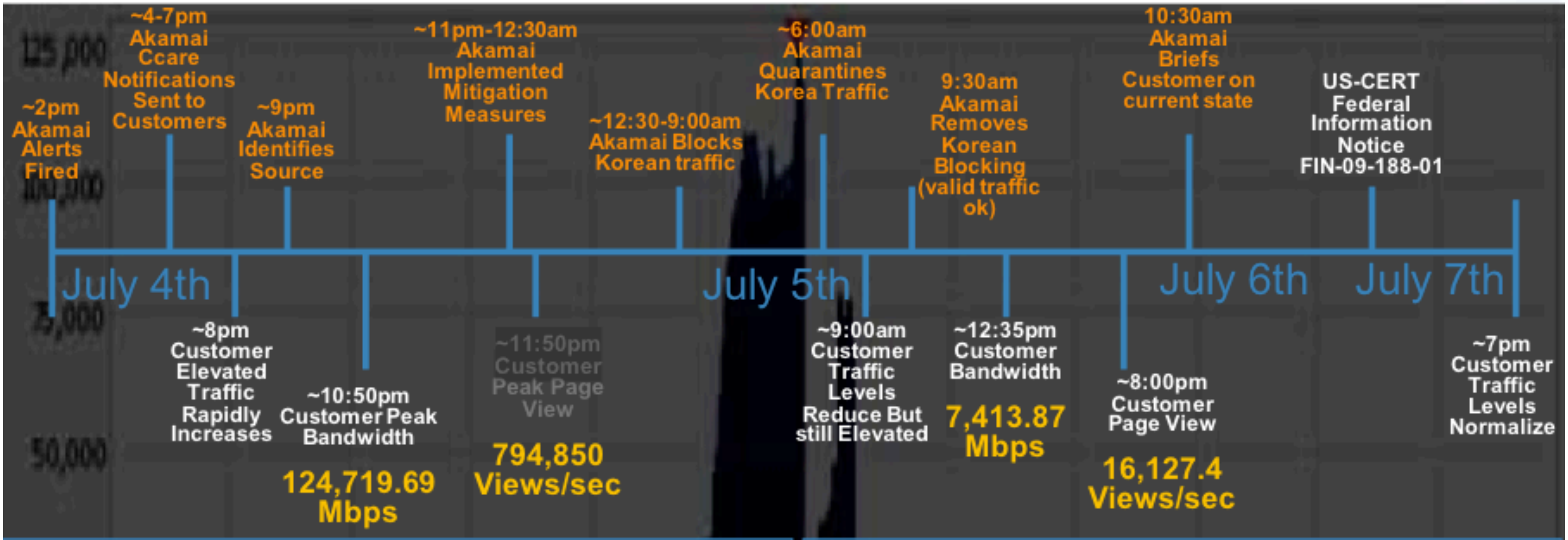


Figure 33 *Source: Arbor Networks, Inc.*

July 4th DDoS Attack Timeline

Multi-Phased Attack



~2pm Akamai Alerts Fired

~4-7pm Akamai Ccare Notifications Sent to Customers

~8pm Customer Elevated Traffic Rapidly Increases

~9pm Akamai Identifies Source

~10:50pm Customer Peak Bandwidth

124,719.69 Mbps

~11pm-12:30am Akamai Implemented Mitigation Measures

~11:50pm Customer Peak Page View

794,850 Views/sec

~12:30-9:00am Akamai Blocks Korean traffic

~6:00am Akamai Quarantines Korea Traffic

~9:00am Customer Traffic Levels Reduce But still Elevated

9:30am Akamai Removes Korean Blocking (valid traffic ok)

~12:35pm Customer Bandwidth

7,413.87 Mbps

~8:00pm Customer Page View

16,127.4 Views/sec

10:30am Akamai Briefs Customer on current state

US-CERT Federal Information Notice FIN-09-188-01

~7pm Customer Traffic Levels Normalize

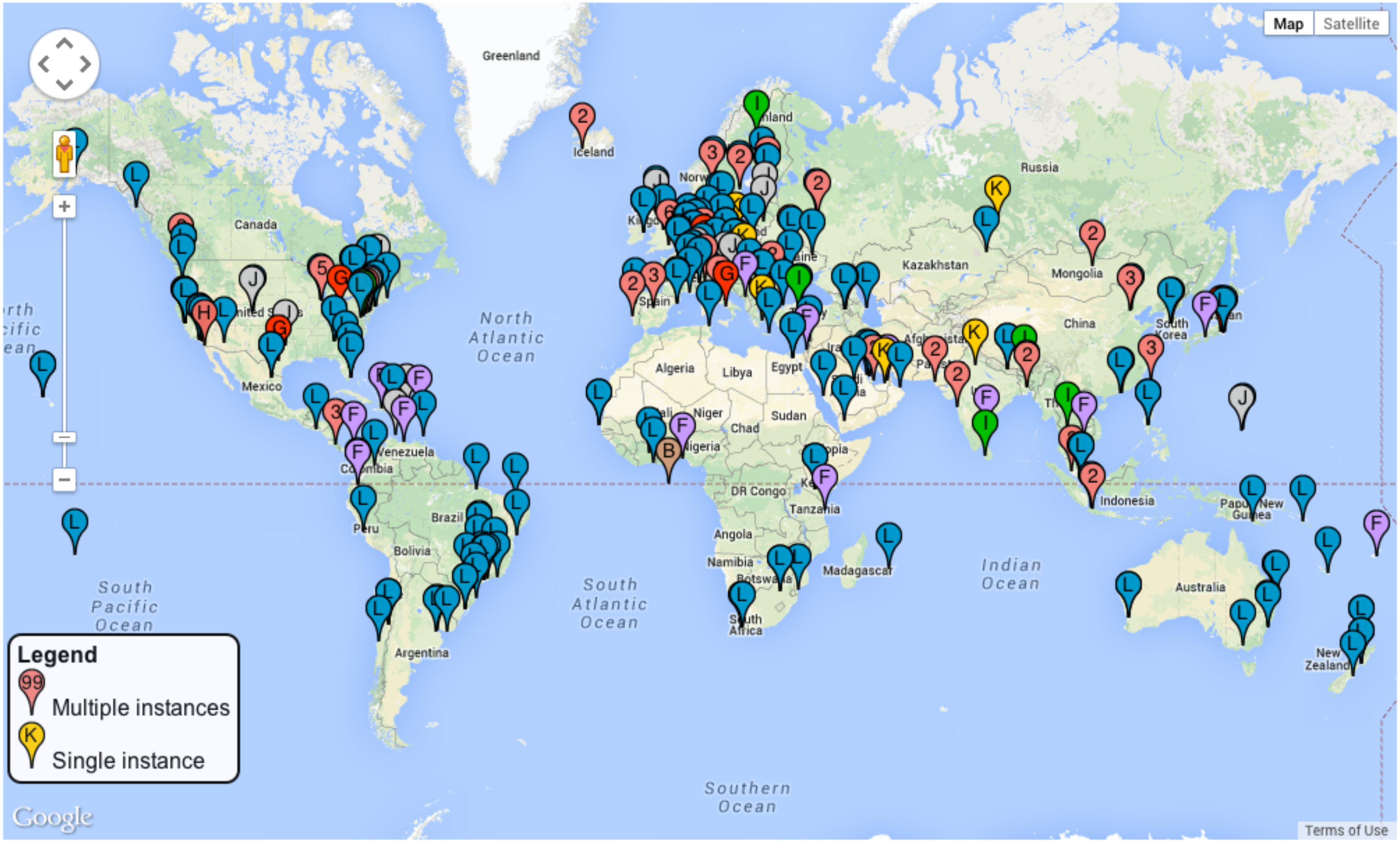
1st Wave of Elevated Traffic

- 1 Day Duration
- 7.4 Billion Total Page Views
- 192.5 TB Served
- Equal 12 OC-192's & 2,500 Servers
- 99.9% BW, 96.2% Request Offload

Subsequent Waves of Elev Traffic

- Next 3 Days of Attack
- 726.6 Million Total Page Views
- 42.2 TB Served

"The first list had only five targets — all U.S. government sites. A second list used by the malware on July 6 had 21 targets, all U.S. government and commercial sector sites, including e-commerce and media sites. A list on the 7th switched out some of the U.S. sites for ones in South Korea. …- Joe Stewart, director of malware research at SecureWorks



Server	Operator	Locations	IP Addresses	AS Number
A	Verisign, Inc.	**Sites: 4** Global: 4 Local: 0 **Los Angeles, CA, US *; New York, NY, US *; Frankfurt, DE *; Hong Kong, HK ***	IPv4: 198.41.0.4 IPv6: 2001:503:BA3E::2:30	19836