PROLEXIC

DDoS Attacks End Here.

The global leader in DDoS protection

Prolexic by the numbers

Founded
Prolexic was the worlds first “in-the-cloud” DDoS mitigation service and now the most mature

Financial Institutions
Prolexic protects some of the largest Financial, SAAS, e-Commerce, Hospitality, and Gaming companies in the world including 16 of the world’s largest banks

Largest and Most Sophisticated
With over 750 Gbps of attack bandwidth and 4 tier one carries globally
Prolexic is 3x larger than the nearest competitor

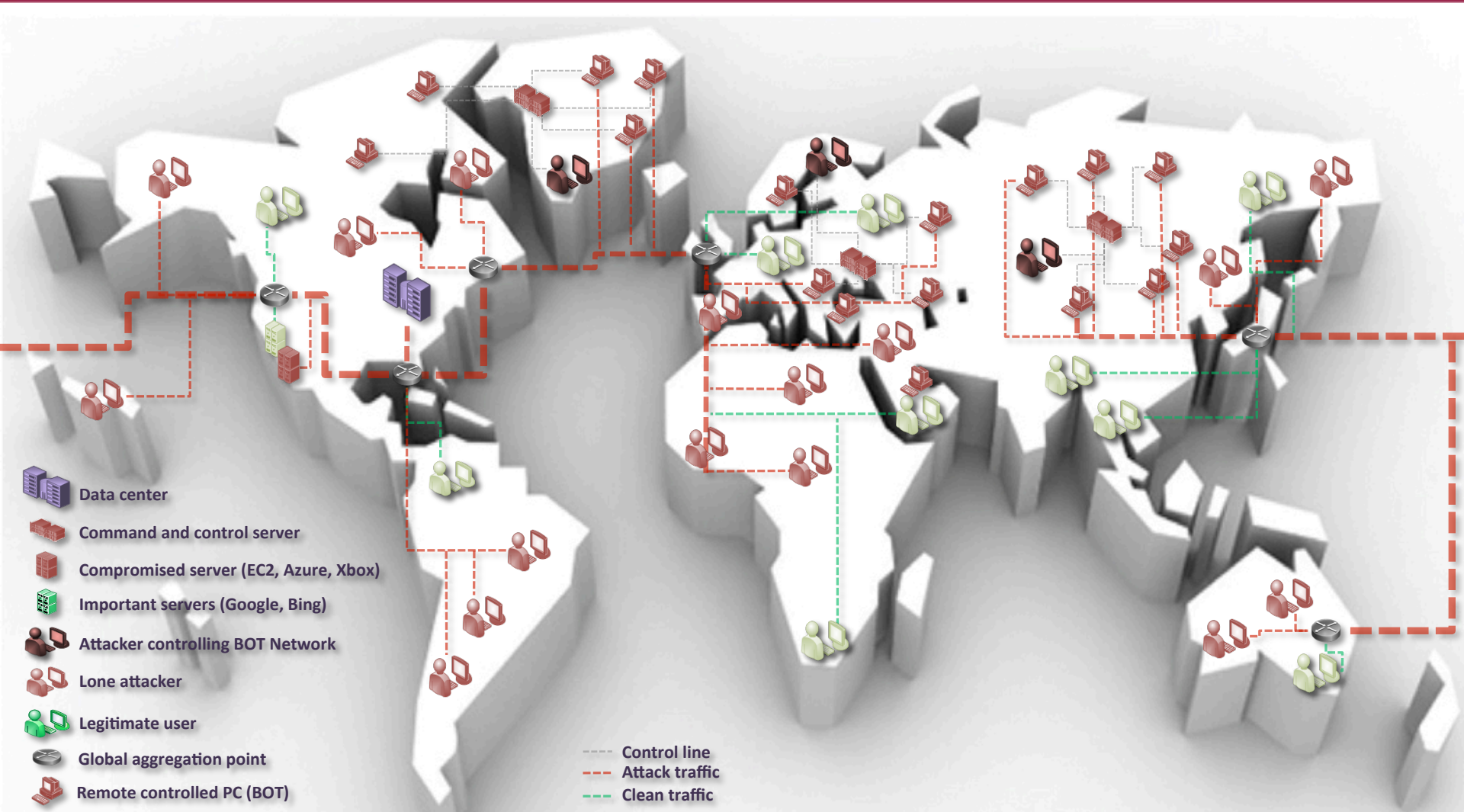
Biggest Attack
Prolexic fought off the largest attack in 2012
72 million packets per second SYN flood

Distinct Technologies
Prolexic uses over 20 different mitigation and analysis technologies where others use 3 or 4

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

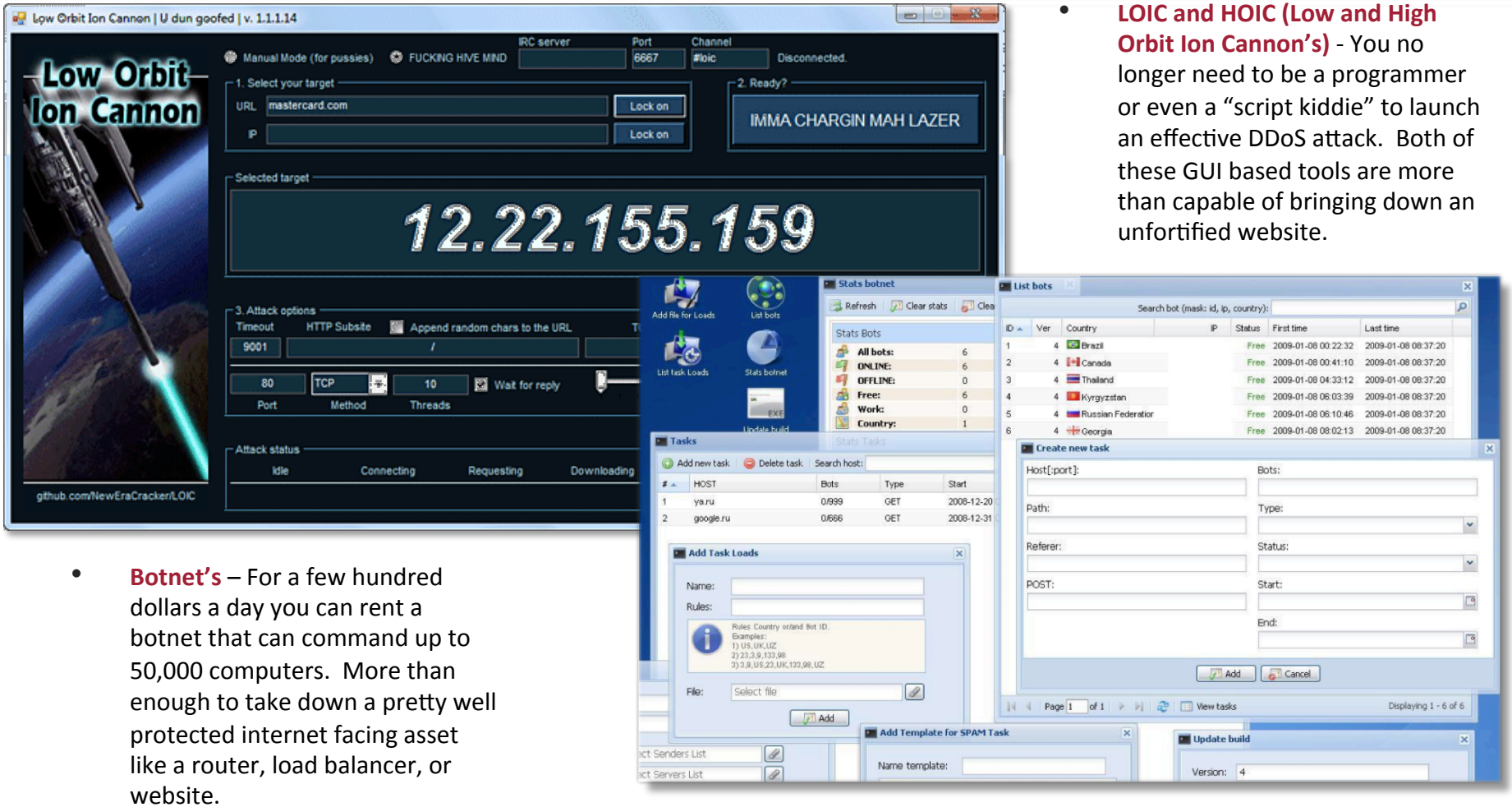
Anatomy of a DDoS Attack - the “Actors”



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Attacking simplified



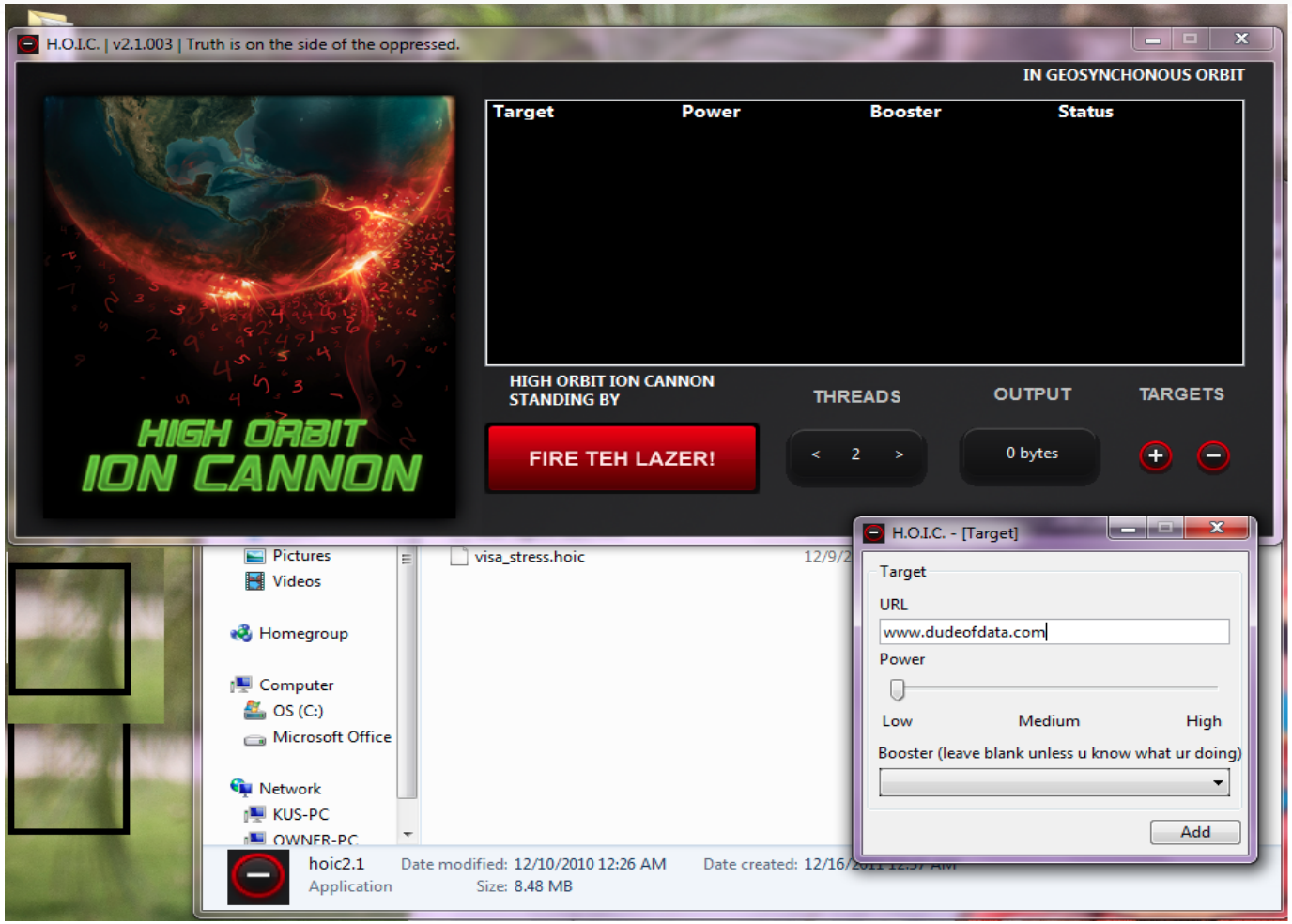
- **LOIC and HOIC (Low and High Orbit Ion Cannon's)** - You no longer need to be a programmer or even a "script kiddie" to launch an effective DDoS attack. Both of these GUI based tools are more than capable of bringing down an unfortified website.

- **Botnet's** – For a few hundred dollars a day you can rent a botnet that can command up to 50,000 computers. More than enough to take down a pretty well protected internet facing asset like a router, load balancer, or website.

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

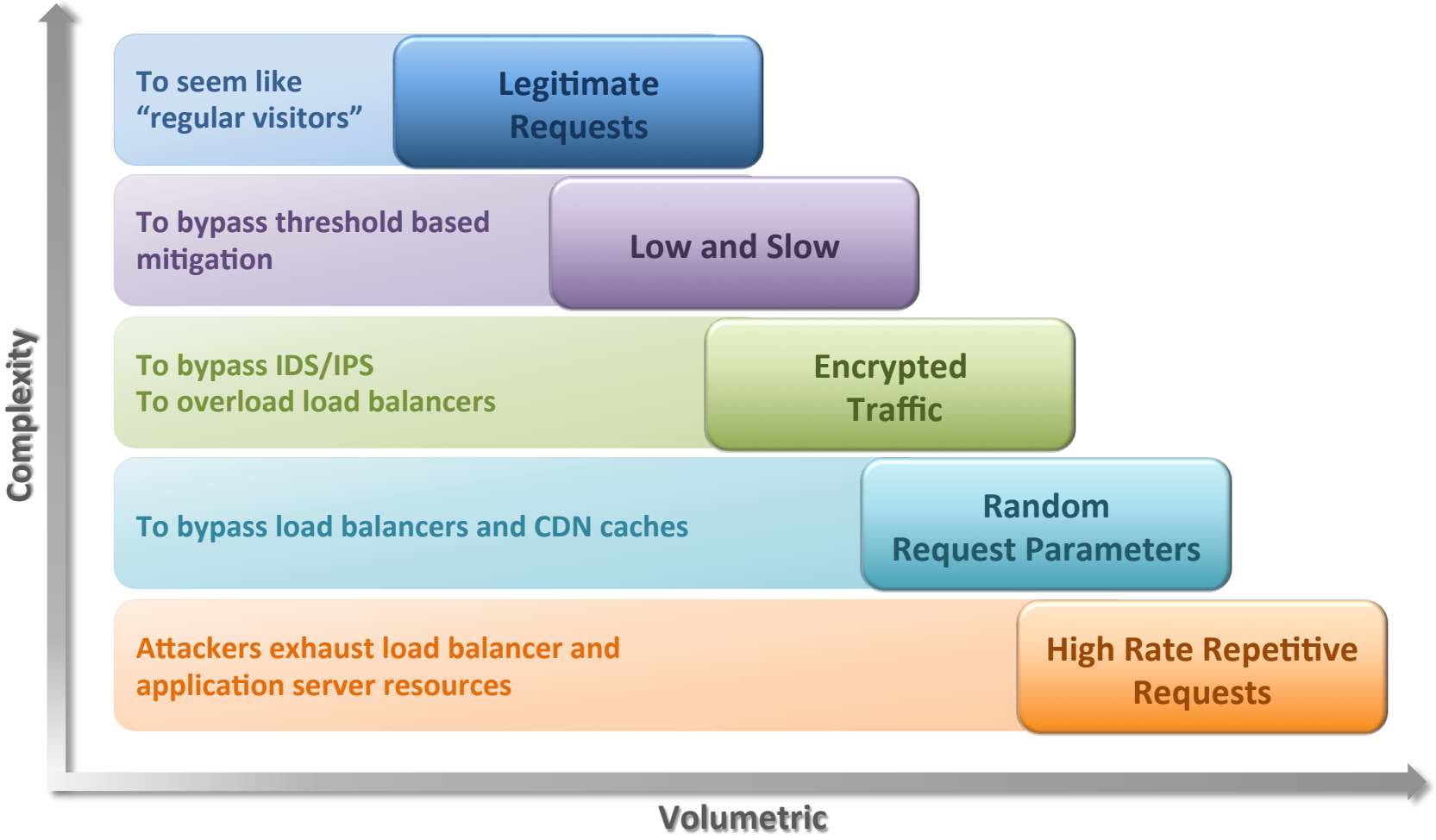
…new and improved…



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Why DDoS attacks are hard to stop



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Why Prolexic succeeds - global coverage

Scrubbing Centers (peering):

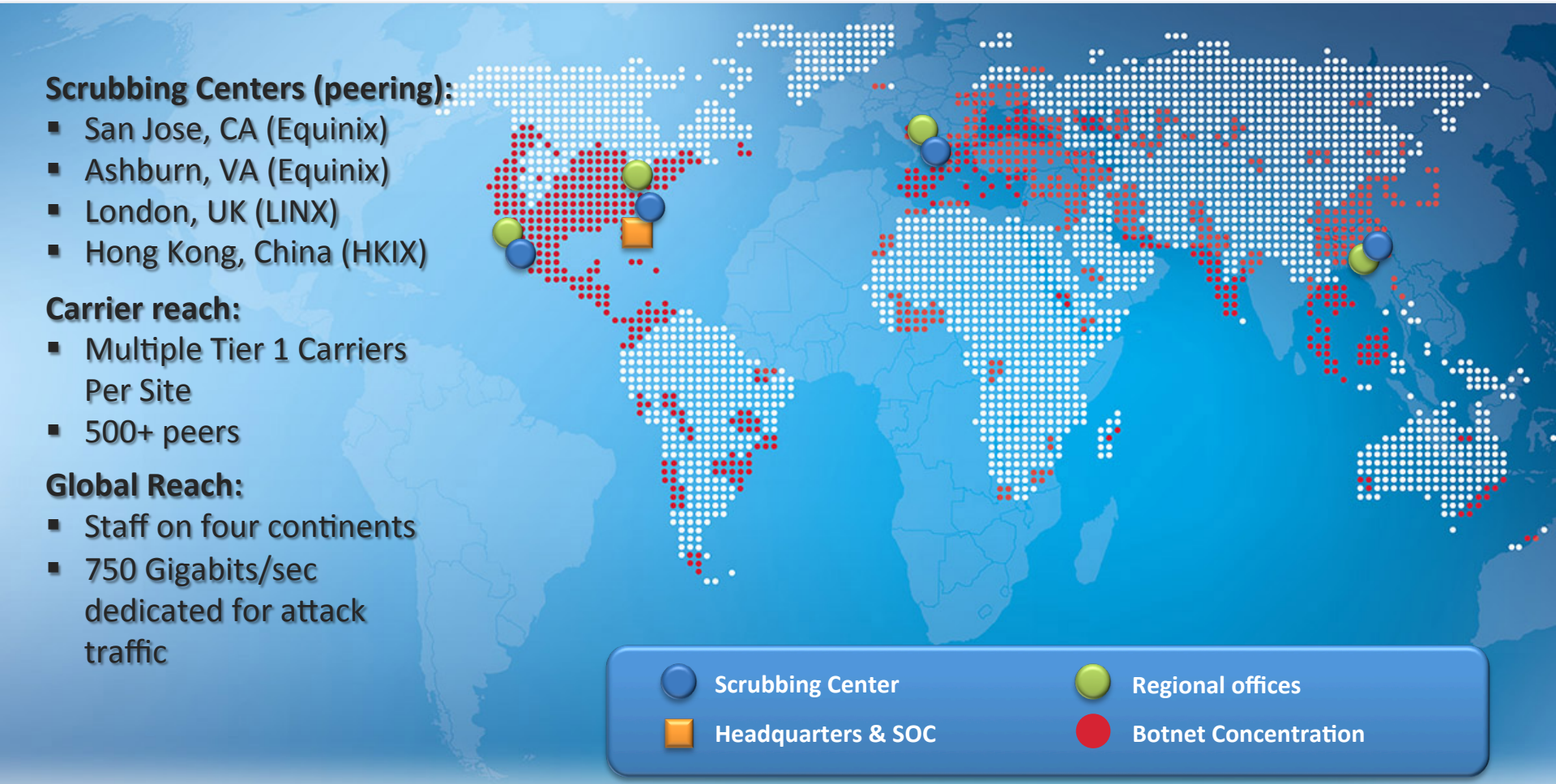
- San Jose, CA (Equinix)
- Ashburn, VA (Equinix)
- London, UK (LINX)
- Hong Kong, China (HKIX)

Carrier reach:

- Multiple Tier 1 Carriers Per Site
- 500+ peers

Global Reach:

- Staff on four continents
- 750 Gigabits/sec dedicated for attack traffic



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

The gold standard for DDoS mitigation

- Largest network dedicated to attack traffic in the industry – by far
- The fastest restoration in the industry
  - Typically just 1-5 minutes after traffic flows through our scrubbing network
- The first company to offer a 15-minute “time to mitigate” service level agreement
- 24/7/365 Security Operations Center staffed by experts who react in real time to DDoS attacks

CONFIDENTIAL

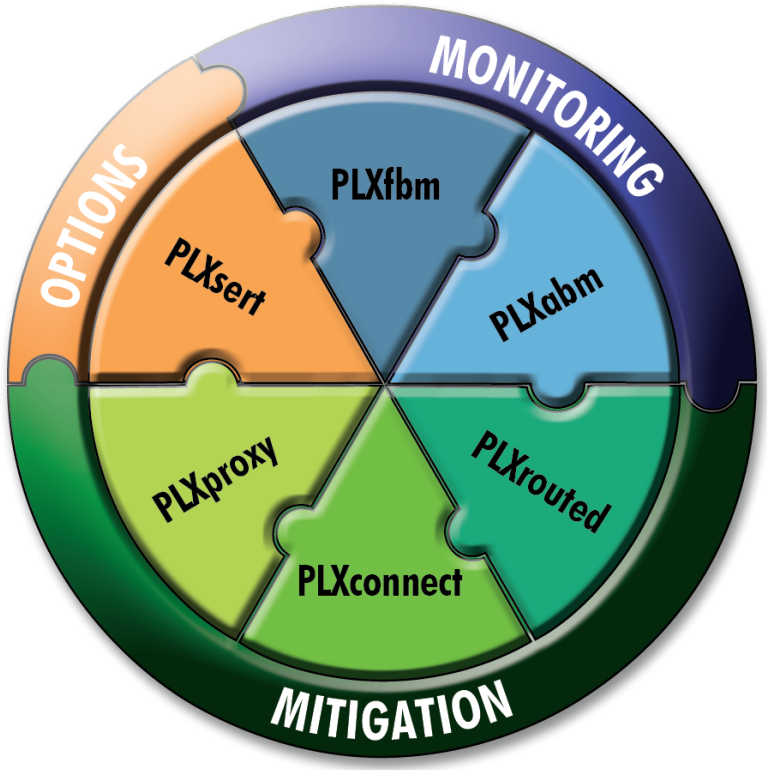
Our solutions

Setup

- Standard Provisioning
- Emergency Provisioning (under attack)
- Professional Services

- One time fee
- Setup varies on number of sites and routers
- Special procedures if provisioned while under attack

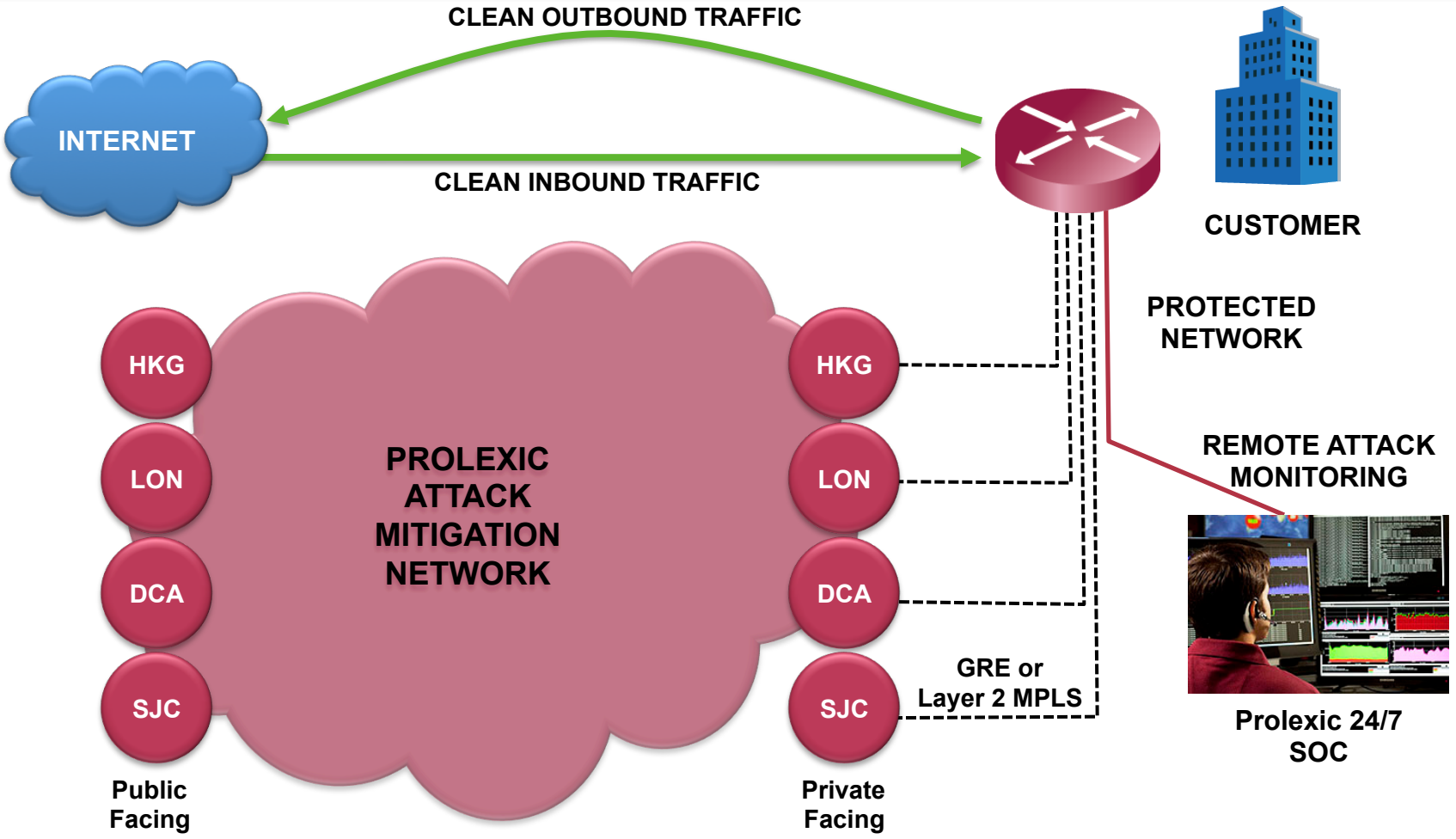
Solutions



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

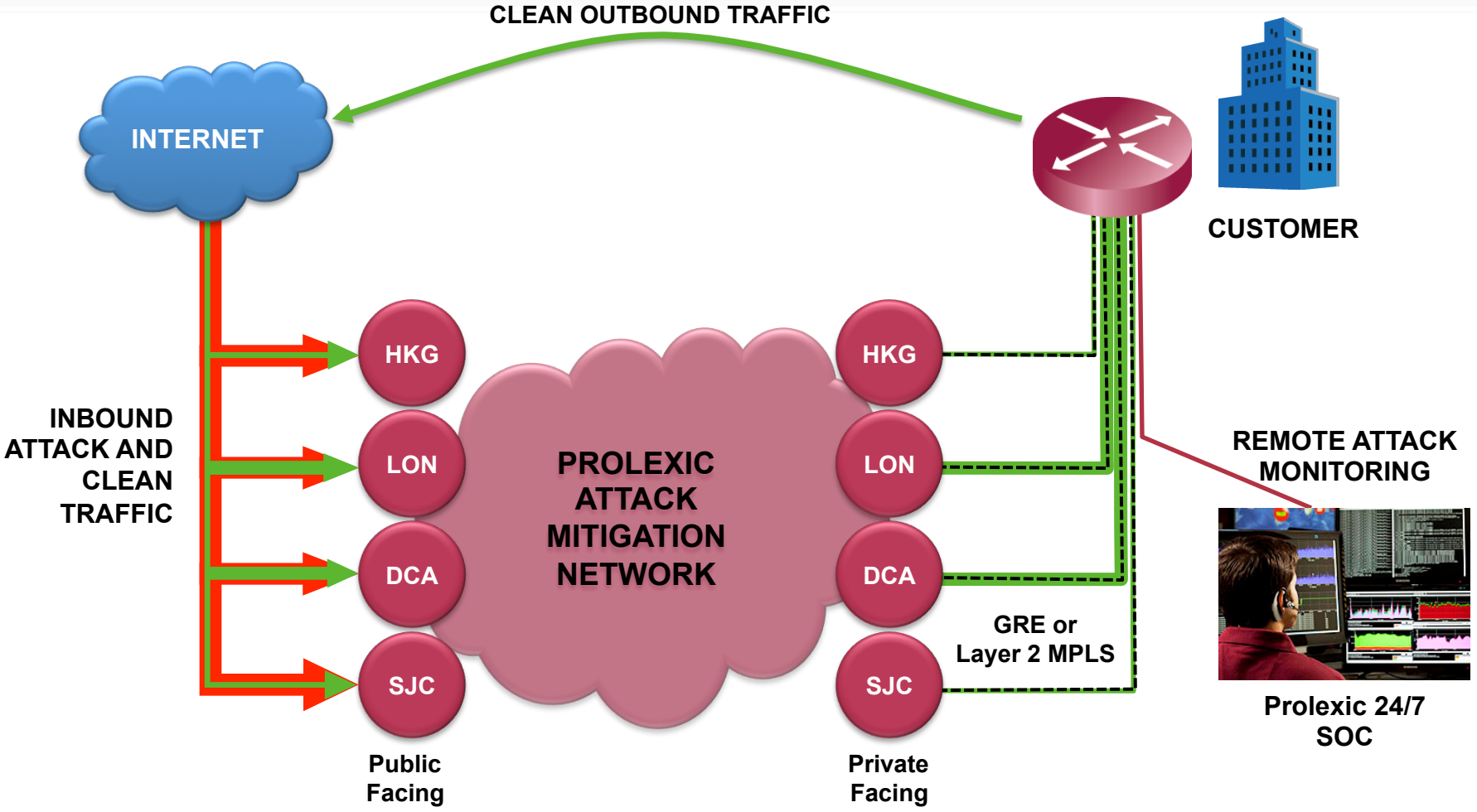
Routed - Inactive



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

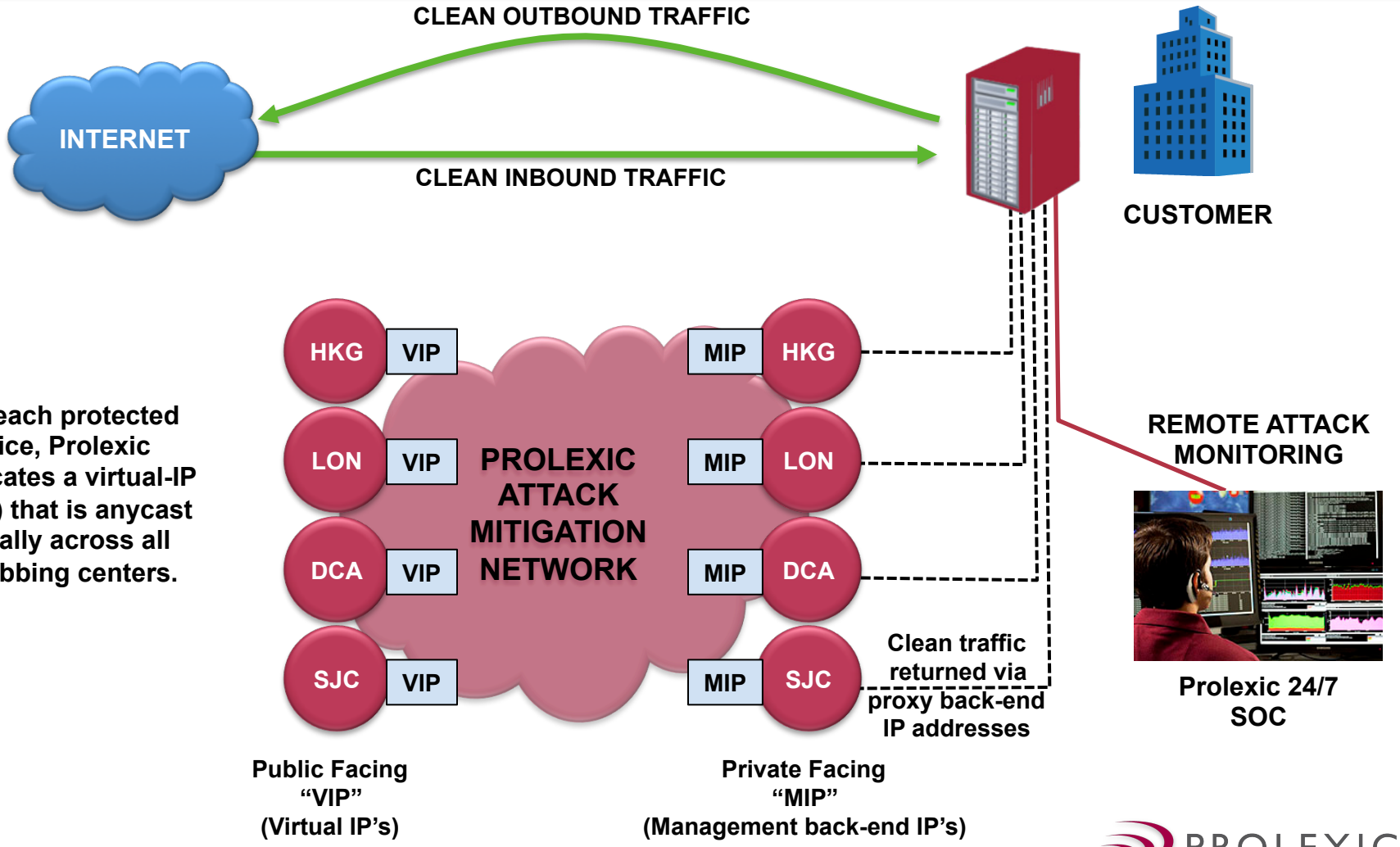
Routed - Activated



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Proxy - Inactive

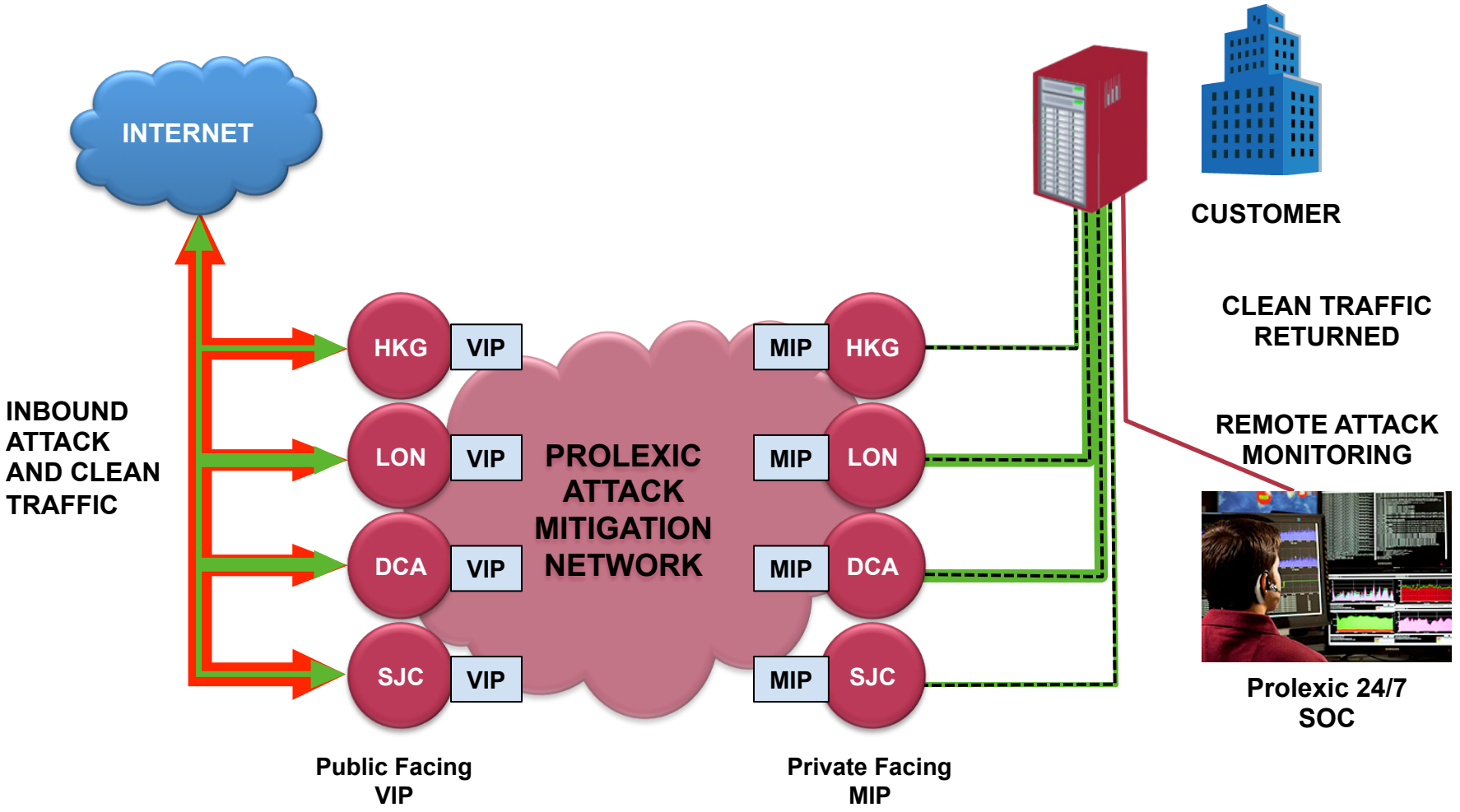


For each protected service, Prolexic allocates a virtual-IP (VIP) that is anycast globally across all scrubbing centers.

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Proxy - Activated



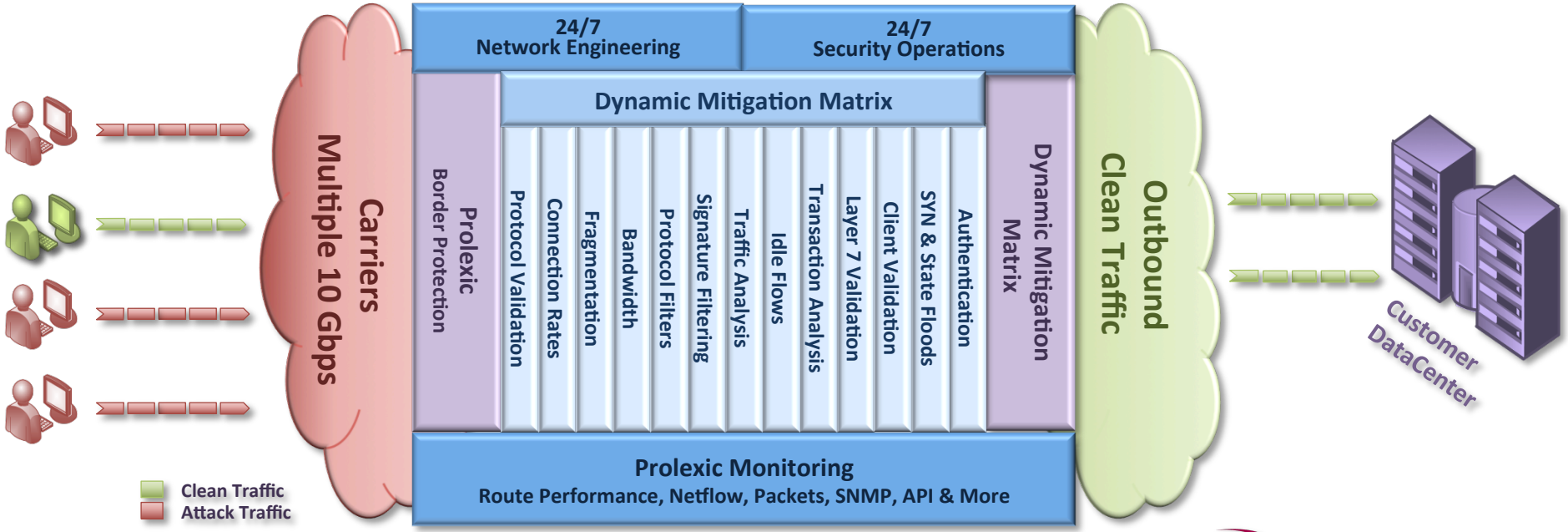
CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Why Prolexic succeeds – multi-faceted defense

Over 20 different analysis and mitigation technologies

- Distributed global network removes bot traffic close to source
- Monitoring up to Layer 7, including proprietary FIPS-140-2 SSL/TLS
- Layer 7 Attack Analysis
- Modular mitigation system: best in class + proprietary systems
- "Threshold" as a last resort – highly discrete low false positive rate
- Full protocol stack, not limited to HTTP and HTTPS

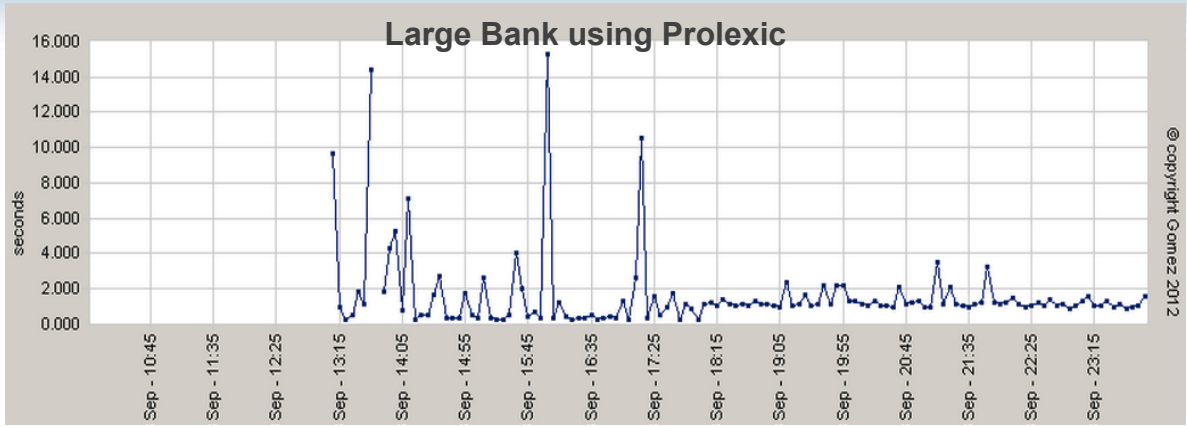


CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

New Round of State Sponsored Attacks – 9/12

Two different banks facing the same attacker



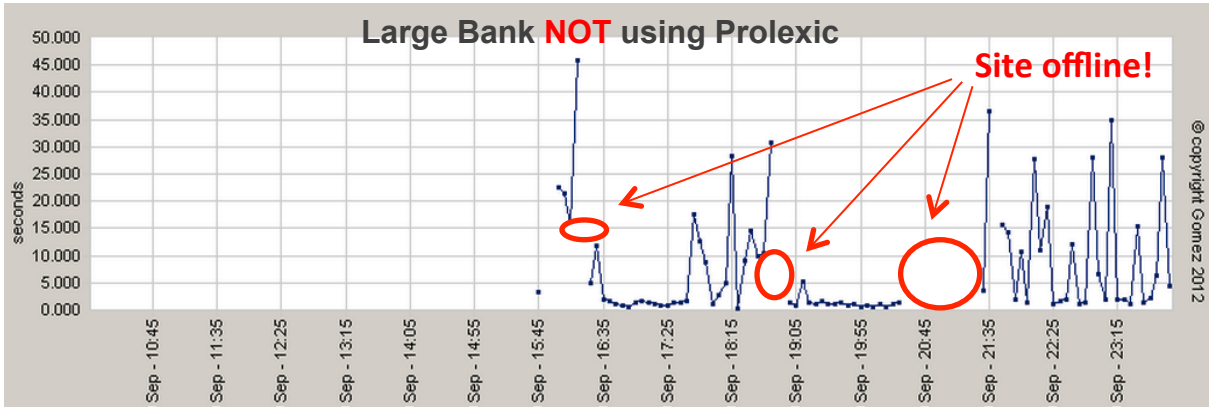
Bank A

- Latency reached 15 secs when others involved
- With just Prolexic: <2 secs
- Functioning web site and acceptable page load times
- Spikes before 9/17 = others involved; after 9/17 = Prolexic responding to new attack vectors

"Over the past 24 hours, as we worked together to address a very dynamic and complex threat, the team sensed we were working with a true partner and not just a vendor" [Bank SVP]

Bank B

- Latency as high as 45 secs
- Site unusable or offline
- Spikes show trying new approaches and failing
- Thought they were protected by multiple vendors, but none could mitigate attack effectively



Latency measured under attack using Gomez

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Anonymous attack 2011

*"Anons involved in the [redacted] attacks worried about **Prolexic's** ability to withstand an assault"*

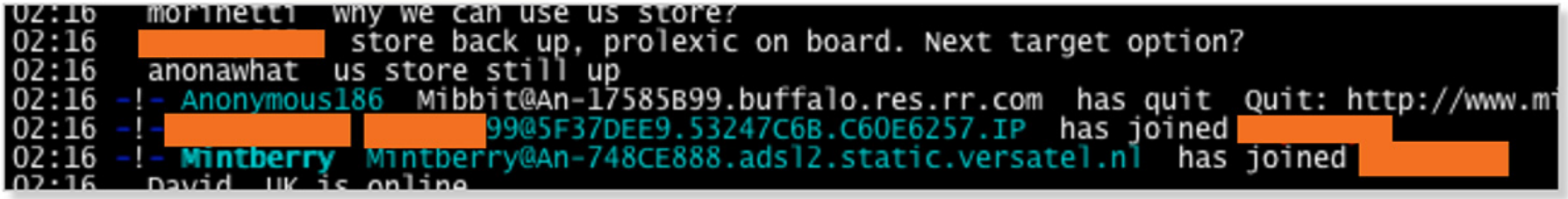
-arstechnica.com

*"It is an effective tool used by Anonymous, but it's not exactly something that [redacted] hosting provider and their newly hired DDoS mitigation service, **Prolexic**, can't handle. With the hiring of **Prolexic**, who has been hired to fight against Anonymous attacks before, this could mean DDoS attacks will be of no threat to [redacted] hosting provider."*

- jailbreakscene.com

*As of yet, there hasn't been any confirmation from [redacted] that **Prolexic** has been brought in, but Anonymous' IRC chat was buzzing with frustration at sudden, newfound difficulties. "Prolexic is holding up," said one guest, while another confirmed that "it's getting harder to DDoS [redacted]ps.com."*

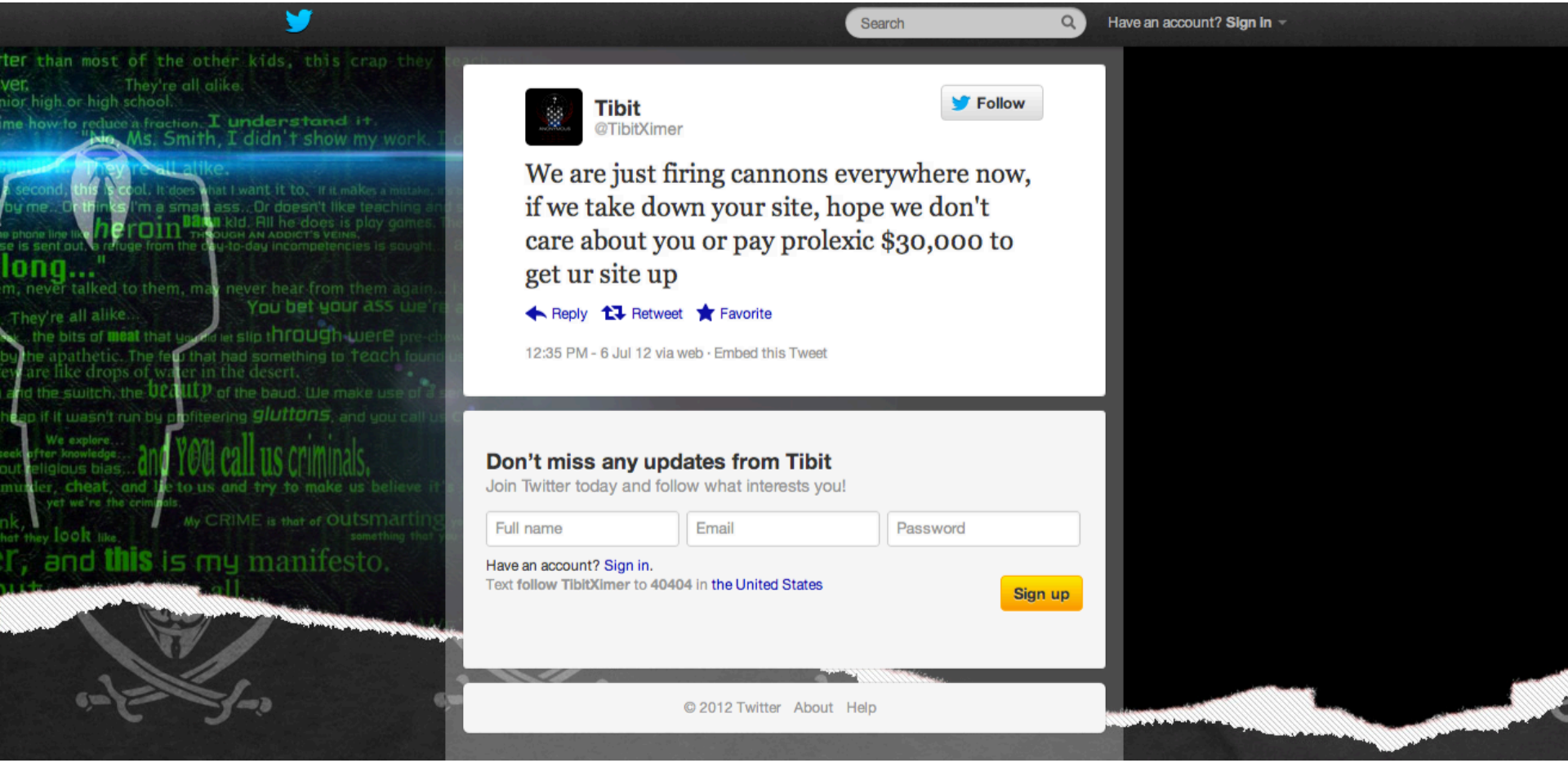
- diedagain.com



CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Anonymous tweet



PROLEXIC
DDoS Attacks End Here.

Gartner on DDoS mitigation services

- "Client calls on DDoS have increased"
- "DDoS mitigation services should be a standard part of business continuity/disaster recovery planning and be included in all Internet service procurements when the business depends on the availability of Internet connectivity."
- Most enterprises should look at detection and mitigation services that are available from ISPs or DDoS security-as-a-service specialists."

Gartner, "Hype Cycle for Infrastructure Protection, 2012", 7/31/12

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

They thought they were protected

"We had purchased DDoS protection services from our CDN and then… The attack started slowly. At first our CDN was able to contain the attack but as the size and complexity increased we went down. We were down for several days before we contacted the FBI and really started to put pressure on our CDN. ***The FBI pointed us to Prolexic****. When we questioned our CDN they informed us that they knew about Prolexic but failed to tell us. We contacted Prolexic and within the hour they had the attack under control and we were back up and running."*

- **e-Commerce customer 2011**

"We thought we were prepared. We had purchased hundreds of thousands of dollars worth of mitigation gear and then… We started seeing unusual traffic patterns one day. It started to escalate to the breaking point. We were then put in a position where we were going to have to make substantial changes to our applications. ***We contacted the Secret Service and they put us in touch with Prolexic.*** *We turned the attack over to Prolexic and they had the attack well under control within the hour."*

- **Financial customer 2011**

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

What we deliver – every day

Attack Category	TTM - Time to Mitigate (typical)	TTM - Time to Mitigate Guaranteed (SLA)
UDP/ICMP Floods	1 minute or less	5 minutes
SYN Floods	1 minute or less	5 minutes
TCP Flag Abuses	1 minute or less	5 minutes
GET/POST Floods	10 minutes or less	20 minutes
DNS Reflection	5 minutes or less	10 minutes
DNS Attack	5 minutes or less	10 minutes

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Why do we care?

- More than 7,000 DDoS attacks per day
- 15-25% of internet computers have been compromised by botnets
- Botnets for rent: US$200/day, some are free
- 24-hour outages can cost millions
- Downtime can cost up to US$1,000/second
- 1-5% share price declines after DDoS

Source: CRS Report for Congress, The Economic impact of Cyber threats", 4/1/2004

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Prolexic gives you more

- **More capacity:** No one has a larger mitigation network to absorb DDoS attacks. No one.
- **More responsiveness:** Prolexic begins mitigation within minutes – and we have an SLA to prove it.
- **More experience:** Prolexic fights more DDoS attacks than many of our competitors combined – thousands each year.
- **More support:** Our Security Operations Center monitors attacks 24/7/365, notifies customers, and compiles intelligence on botnets.
- **More flexibility:** Choose the level of service and options that are right for your organization.
- **More peace of mind:** No attacker has been too smart and no DDoS attack has been too big or complex for Prolexic.

CONFIDENTIAL

Why perimeter device DDoS mitigation fails

- Cannot stop attacks that are too large or complex
- Large CAPEX and OPEX
- High CPU load, low throughput and performance
- Blocks legitimate traffic causing high false positives
- Attackers easily overrun perimeter devices by simply hitting it with more traffic than the upstream Internet connection or more traffic that the device can handle
- Zero day and HTTPS attacks will not be detected or mitigated

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Why telco DDoS mitigation fails

- Cannot stop DDoS attacks that are too large or complex
- Can only protect their own bandwidth - multiple vendors needed to cover all bandwidth
- Can't stop attacks over 8-10 Gbps best case and will null route (black hole) customer to maintain network stability
- Can't protect against Layer 7 attacks like HTTP & HTTPS
- Limited knowledge of DDoS attacks and equipment

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Why CDN DDoS mitigation fails

- Cannot stop complex DDoS attacks or those targeting backend IPs
- Large bandwidth overage fees to stop large DDoS floods
- Layer 7 attacks (HTTP/S) that look legitimate pass through CDNs
- Attacking back end origin IP addresses completely bypasses CDN
- Akamai, the world's largest CDN, has integrated Prolexic into its global network to provide DDoS protection for many key clients

CONFIDENTIAL

DDoS is coming to a network near you

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.

Questions? Contact Vibe Security.

www.vibesecurity.com sales@vibesecurity.com phone: +352 20203272

CONFIDENTIAL

PROLEXIC
DDoS Attacks End Here.