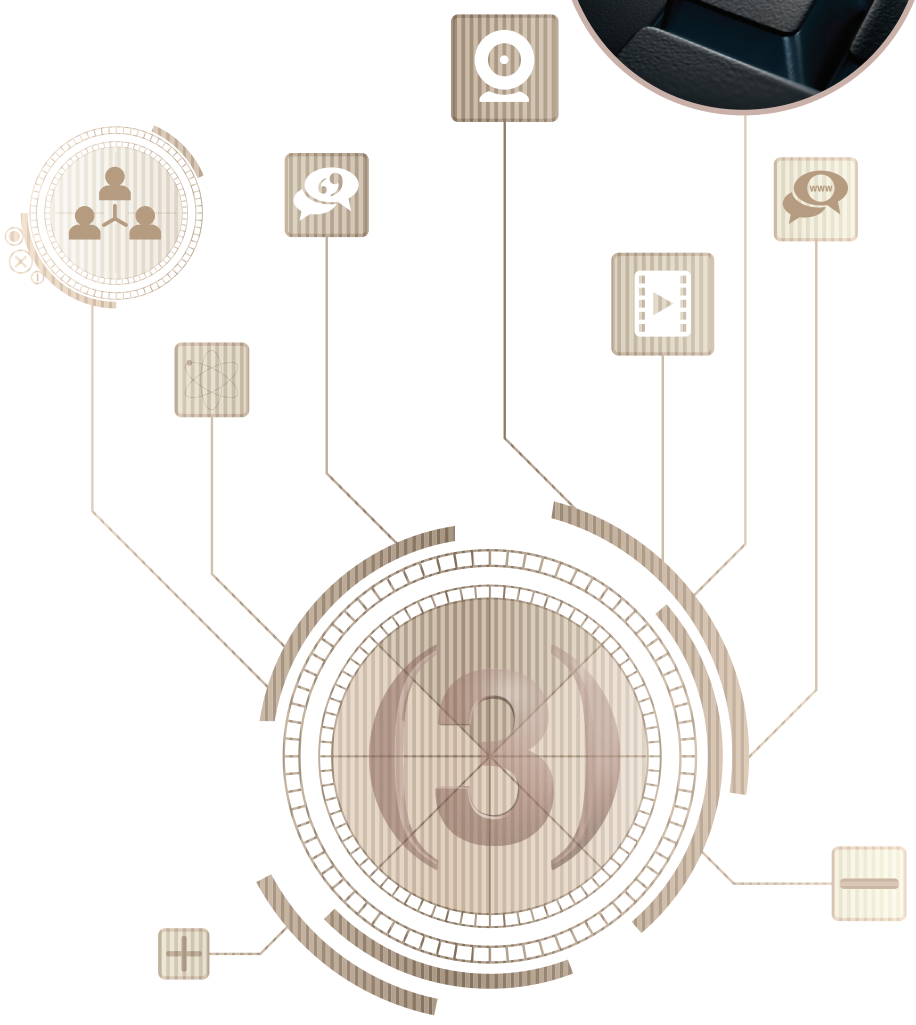
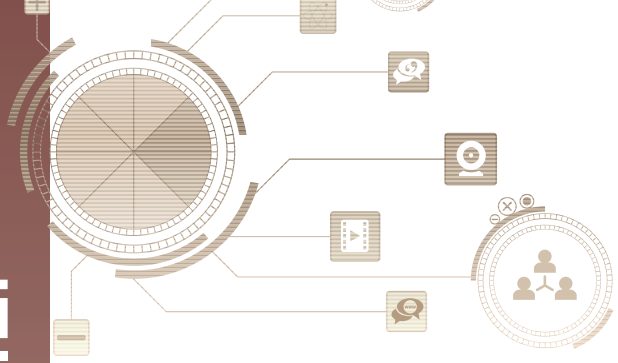
APPLICATION BRIEF

HEADING OFF CYBERATTACKS BEFORE THEY HIT



APPLICATION BRIEF



Level(3)

Situation

It's 3 a.m. in Chicago. Although the doors to this U.S. retailer's flagship store are locked tight, the doors to their online business need to be open, because it's 10 a.m. in Madrid and Paris, 12 noon in Moscow, and prime shopping time for their customers in many other parts of the world as well.

Cybercriminals know disrupting continuity of operations can be crippling to e-commerce and are planning to launch a distributed denial of service (DDoS) attack against the retailer, aiming to paralyze the company's website. As a matter of fact, they recently posted a blog bragging that an attack would be made on one well-known housewares retailer; they didn't identify which business would be targeted but they did indicate that they would soon follow with details of who would be attacked and how much money they will demand to abandon the assault.

Vulnerability

A "typical" DDoS attack leverages a vast number of computers, infected with botnets, which simultaneously inundate an organization's website or other computer resource with requests or data until it slows to the point of being useless or crashes. Unfortunately, "typical" doesn't characterize the situation. "The reality of security is that change reigns supreme," Frost & Sullivan's VP of Research Mike Suby writes. "The cyber underworld is rearming itself to reach its objectives."[1]

Every organization linked to the Internet is vulnerable to DDoS attack and cyberextortion, and doing business requires that link. Very few companies have the capital or in-house resources necessary to run their business and keep track of newly developed threats and the latest security measures. Even fewer have the experience and special skills applicable to parsing actionable information from the huge volume of threat and status data they collect every day.

Strategy

Mitigating DDoS attacks by shielding the targeted organization is possible, but doing so requires understanding the difference between normal and abnormal Internet behavior. Network service providers (NSPs) are in a unique position to do just that. With up-to-the-second visibility into network traffic and years of patterns to use as reference, NSPs that also provide managed security services can distinguish legitimate activity from illegitimate demands on resources, isolate attack traffic, and redirect the "scrubbed" requests and data to the retailer.

One part of engaging Level 3's security services involves building a relationship between a company's IT team and Level 3 security experts. In initial conversations, Level 3 can learn about your business and vulnerabilities. Ongoing dialogue enables your organization to stay informed on new threats, especially in regard to when to take action.

[1]Don't Leave your Organization Exposed – Join forces with a Trusted Security Services Provider, Frost & Sullivan, August 2012, Mike Suby

APPLICATION BRIEF

By tracking social media, the retailer in this scenario had indication that they were a DDoS target; communicating that suspicion enabled Level 3 to focus special attention on the retailer's site. The attack was launched, Level 3 intercepted, and business went on without interruption. As events unfolded, once the attacker knew that Level 3 security was involved, they gave up.

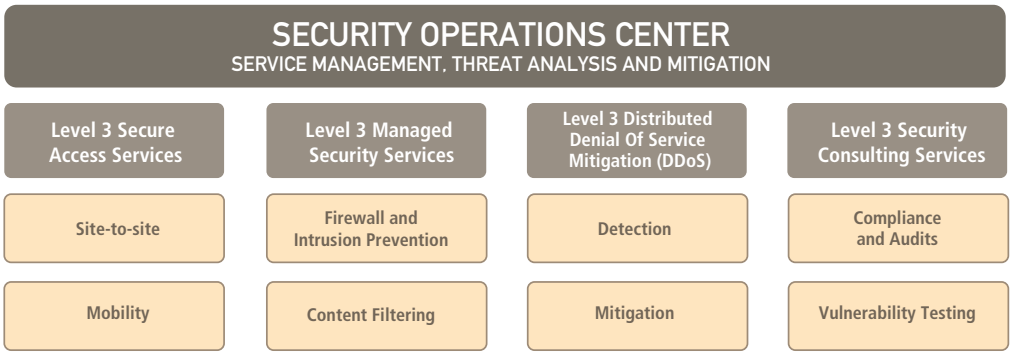
Level 3 Security Services

Global e-commerce never rests, and neither does Level 3. Level 3 Security Solutions elevate the network protection available to your company by allowing you to take advantage of our network threat insight and the experience we gained by securing our own infrastructure and the visibility we have through our Security Operations Center (SOC). Our goal is to team with you to safeguard your data, minimize vulnerabilities and carve a path for fast remediation and better business continuity.

The Level 3℠ Distributed Denial of Service Mitigation offering was developed to protect our customers by leveraging:

The Level 3® Distributed Denial of Service Mitigation offering was developed to protect our customers by leveraging:

- Detection capabilities based on industry-leading anomaly detection technology
- Continual, consistent security operations and trouble management through around-the-clock network and device monitoring
- 160+ Gbps of bandwidth balanced across multiple datacenters "in the cloud"
- Ability to respond in real time to next-generation attacks



Over view of Level 3's Security Solutions. In this Application Brief, Level 3 helps a global retailer mitigate a DDoS attack before it can bring the company's website down.

Learn More

To take steps toward better protecting your employees, networks and business, visit www.level3.com.