Pay Up or Else: IT Infrastructure Solutions Provider Helps Customers Navigate Range of Network Attacks

About ServerCentral

- IT infrastructure solutions provider specializing in the design, development and management of custom infrastructure solutions, including colocation, Infrastructure as a Service (IaaS), private clouds, network services and network protection
- ServerCentral customer was hit by an extortion-based DDoS attack
- Managed services providers need to remain vigilant in protecting their networks, as attacks can affect multiple customers—and all of their customers

Pay Up or Else: IT Infrastructure Solutions Provider Helps Customers Navigate Range of Network Attacks

We live in a managed services world—with organizations across industries outsourcing significant pieces of their operations to third-party specialists. The business case for managed services can be compelling. But as cyber-security threats rise, so have the stakes for managed services providers. These companies must not only protect their own networks and data; they must also be effective guardians on behalf of their customers and their customers' customers.

As an IT infrastructure solutions provider, ServerCentral fulfills those dual roles of securing itself and its customers. The Chicago-based firm routinely identifies network and DDoS attacks, which occur as frequently as every few days and range from small protocol floods through full-blown DDoS campaigns designed to extort money in return for stopping the attack. In fact, earlier this year, one of the company's clients was the target of an organized criminal effort that involved attempted extortion.

The ServerCentral client, which offers a web-based tool for project management, was one of a number of victims of the same criminal group. This group's MO is simple: it threatens to attack a network if an organization does not meet its demands for payment.

After refusing to negotiate with the criminals, the ServerCentral client was hit with a 20GB DDoS attack.The incident underscores the important role that ServerCentral plays in its clients' network security. As Director of Network Engineering Ron Winward explains, "ServerCentral takes as much pride in our customers' ability to execute and offer service as we do in our own ability to provide infrastructure in support of mission-critical applications and business functions. We are equally focused on providing 100% uptime to their customers and end users."

Detecting Extortion-Based Attacks

Winward explains that ServerCentral detects attacks in many different ways. In the case of the extortion-based attack, the customer notified ServerCentral of the threat.

"In some instances, customers will contact us, noting that something isn't right. They may recognize it as an attack or simply see something out of the ordinary," he says. "Attacks can also be detected by our network monitoring tools, which can identify anomalies and alert our Network Operations Center (NOC) of the incident."

ServerCentral engineering staff also regularly reviews network reporting data and can perform forensic research using historical flow analysis when needed. For customers that use Radware's DefensePro and DefenseSSL, ServerCentral's NOC and engineering staff are notified of detected events in real time.

After years of experience operating a resilient, high-performance network, Winward says ServerCentral was prepared to support its client through the extortion-based DDoS attack. In fact, the company has established a security model that it can apply to customer interfaces upon turn up.

"As a result, most customers don't even know they're being attacked until ServerCentral's monitoring system detects it," Winward says.

Planning for the Future

Groups responsible for many attacks—especially those that incorporate extortion—have a habit of stopping and starting an attack at random intervals. In other words, the attack could very well start up again at any time. Winward asserts that ServerCentral's core network architecture, deployment of carrier-class routers and forensic toolset help ensure that it's ready for even the most unpredictable attacks.

"We're able to quickly and easily manage the presence of an attack with a known or identifiable fingerprint," he says. "Offering DefensePro as a real-time option for individual customers further strengthens our position, especially for application-layer and SSL attacks."

He explains that the company keeps standby units on-site for rapid deployment, if needed—but acknowledges that the real-time responsiveness of DefensePro simply outmatches any reactive technique, no matter how fast it may be.

As attacks become both more sophisticated and seemingly easier to execute, Winward says that ServerCentral expects the number of attacks to double over the next 12 months. With that in mind, customer education is an increasingly important component of the company's strategy for attack management. ServerCentral is actively working to inform its customers about the risks—and steps they should take to proactively guard against them.

"As we see more and more attacks of all types, we have an obligation to share this knowledge with our customers so that everyone can be as vigilant as possible," he explains. "We know that attackers are focused on their 'job' 100% of the time. For ServerCentral, staying abreast of changes in attack patterns, objectives and execution is something that must remain 'on' at all times, as well."

"As we see more and more attacks of all types, we have an obligation to share this knowledge with our customers so that everyone can be as vigilant as possible. We know that attackers are focused on their 'job' 100% of the time. Staying abreast of changes in attack patterns, objectives and execution is something that must remain 'on' at all times."

Ron Winward
Director of Network Engineering,
ServerCentral