

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



ABOUT SUMMIT

- 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
- Summit 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

Overview

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 cybersecurity 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, Summit fulfills those dual roles of securing itself and its customers. The 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 Summit 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 Summit client was hit with a 20 GB DDoS attack. The incident underscores the important role that Summit plays in its clients' network security. As Lead Network Architect Chris Haun explains, *"Summit 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

Haun explains that Summit detects attacks in many different ways. In the case of the extortion-based attack, the customer notified Summit 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."* Summit engineering staff also regularly reviews network reporting data and can perform forensic research using historical flow analysis when needed.

After years of experience operating a resilient, high-performance network, Haun says Summit 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 Summit's monitoring system detects it," Haun says.

 *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."*

— Charles Rumford, Principal Infrastructure Architect at Summit.

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. Charles Rumford, Principal Infrastructure Architect at Summit, asserts that Summit'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," says Rumford. "Radware Cloud's scrubbing service lets us jump in quickly when a customer's under attack. Summit also offers dedicated DDoS protection for customers looking for a more tailored, hands-on solution."

As attacks become both more sophisticated and seemingly easier to execute, Rumford says that Summit 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. Summit 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 Summit, staying abreast of changes in attack patterns, objectives and execution is something that must remain 'on' at all times, as well."

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

© 2025 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.

