radware

# FROM THE CORNER OFFICE

## INSIGHTS FROM A CHIEF INFORMATION SECURITY OFFICER

When it comes to cyber-attacks, too often telecommunication companies and service providers are burning both ends of the candle: they're safeguarding their most prized digital assets while trying to keep their customers secure as well.

Due to the collateral damage associated with successfully cyber-attacking a service provider, it's no surprise that these organizations are facing an increased likelihood of being attacked. Security executives at leading telecommunication companies are some of the savviest in the marketplace. They have to be to deal with everything from DDoS "burst attacks" to malicious use of messaging protocols and mobile-specific ransomware. To garner their insight, a chief information security officer at a top-five U.S. telecommunications carrier shares his recent experiences and insight.

## What were the top attack trends in 2016?

1. First and foremost, we've seen our network—and the networks we monitor and protect—experience **a tenfold increase in the volume of DDoS attacks**. In August 2015, we had a little over 5,000 attacks. In July 2016, it was 55,000 attacks that we could identify. Last year, 70% to 80% of attacks were less than a minute—mostly "white noise" events (a.k.a. "hit-and-run DDoS" or "burst attacks"). This year, we've seen attacks falling into the one- to five-minute duration, causing random business disruptions.

2. We've also experienced a **tremendous spike in malicious use in messaging protocols being tweaked to carry out attacks** - including MMS (Multimedia Messaging Service), SMS (Short Message Service) and traditional email into these numbers. More than 99% of the total volume in our environment we identified as being malicious or otherwise inappropriate to deliver to the customer.

3. The third trend is a large **increase in mobile-specific ransomware activity** targeting the two largest platforms: Android and Apple. We believe most of that activity is originating in a foreign country and being delivered via third-party app stores.

## Can you outline the size, scope and sophistication of attacks your organization has faced?

**Volume.** Across all categories of attacks, we've seen a large uptick in the total volume transfer that occurred. I'm not referring to gigs per second but the total volume. We saw our largest category of 500GB or higher have a four-fold increase. So in addition to a spike in burst attacks, we are also seeing longer-lasting attacks that are presenting more data.

**Vectors.** When it comes to vectors, attacks generally fall into three common protocols: NTP, DNS and CharGEN. Others may be used occasionally, but these are the three we see most commonly. Of those three, we'll see for two or three months that DNS will be most common, and then it switches to CharGEN. There's no clear pattern, which makes it hard to predict—just that the majority of attacks will use a common protocol and then it will change.

**Sophistication.** Attacks are also growing in sophistication. That holds true more so based on what we've seen with mobile-originating attacks. There's been a sharp increase in malware targeting Android devices and then leveraging them for DDoS events. Many of those malware packages we've identified weren't written specifically for DDoS events. It's typically ad clicking or some other purpose, but we've seen some very advanced malware being leveraged for DDoS.

## What are some best practices for managing security at a global telecommunication company?

We have a third party that serves as our Tier 1 Security Operations Center (SOC), the traditional security analyst team that looks at everything as if through a magnifying glass. They're the first ones expected to receive the alarm out of our event management system.

We're safeguarding thousands of apps—applications in our own corporate environments, applications for our enterprise customers and more than 20 million subscribers ranging from hotspots with connected Windows and Linux devices to Android and Apple devices. We lean on our vendor's Emergency Response Team and Advanced Services group to help us validate an appropriate implementation of our security policies. These are high-value devices so we want to ensure we're getting maximum value for those dollars, and those teams help us achieve that.

One of the first things I do every morning is go to our dashboards, which display alarms and DDoS trends in an executive view. Our SOC is looking at metrics on a 24x7 basis and our manager and director levels are looking at these dashboards daily. We've established five severity categories for attacks and each is further broken down by event or total volume transfer. Our goal is to provide the business with the complete story.

If an event falls into one of our two highest-severity categories (we average one highest-severity event per week and one to four second-highest-severity events per day), we have an incident management process that is initiated. First, we immediately notify various members of our security and broader carrier/technology organization. Second, we take a deep dive into the threat intelligence. Was the attack part of something broader—geopolitical, script event, collateral damage? Third, we present our findings as they pertain to any potential impact it may have caused. We provide per-incident analysis and, if needed, we have different thresholds in place on when and how to communicate. The bottom line: we're analyzing each and every event in some manner, and thanks to how our security architecture has been built and how we manage out IP space, determine who was targeted. Generally speaking, nine out of 10 events target our customers and the rest target our corporate assets.

Attacks and techniques change daily. You need flexible solutions and the ability to make adjustments just as frequently to protect the business. Pull those levers to keep pace with ever-changing threats to your applications and networks.

On a daily basis, I am asked the question, "Why?" I don't have a quantified response other than a gut feeling. However, those feelings are reassured and backed by our program development and threat intelligence. We leverage a series of tools to identify that attacks are increasing. We're now pretty confident that more and more advanced malware is being produced targeting the Android platform in particular.

### Black Friday: From Crisis to Confidence

When we first deployed a DDoS protection solution back in 2010, we actually had it on the network in a monitor-and-alert mode because at that time we didn't see a great enough risk to justify putting those devices inline as a permanent configuration. We would have them inline as we identified specific risks. A number of times we were referenced in a campaign, so we placed those devices inline during that high-risk period and then pulled them back out. But several years ago, we made the decision to place them inline again.

On Black Friday 2015—the busiest retail day of the year—we were the target of a large attack. I was able to send an email to our senior execs letting them know that it had occurred and we blocked it with a 100% effective rate. That was a big win for our security team.

You simply cannot paint a broad brush in architecture and platforms. You may protect 99 of 100 apps, but if that one app might be business critical, you still failed. Not all code development has the same level of quality or standards, and we've had to take that in account. Regardless of size or industry, an organization will have a reasonable, if not definitive, population of assets it's trying to protect. Solutions must have a broad range of coverage—focusing not just on traditional network protocol protections but also offering high-quality, in-session management and all the various techniques, like hold-down timers and HTTP protections.

When I have an incident, I have a very high level of confidence that when I engage Radware's ERT, I'm getting support from some of the world's leading cyber security experts.

Above all, I tell people that if they feel they are at increased risk for DDoS attacks, they should not underestimate the level of commitment required for maintaining these platforms. Attacks and techniques change daily. You need flexible solutions and the ability to make adjustments just as frequently to protect the business. Pull those levers to keep pace with ever-changing threats to your applications and networks.

## Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.