Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 2

A Network Too Smart to Get Hacked

By Becky Bracken

Frankly, it's not just that hackers broke into the China Telecom and Warner Bros network in June and posted passwords and secure files that must have stung at the next day's in-house, postmortem meeting. But, what probably stung worse was the message that the culprits, who call themselves "Swaggsec," left to claim the credit and do a little end zone celebration:

"Hacking China Telecom was as simple as we assumed it would be," Swaggsec wrote in their message posted on Pastebin. "As BBC reported, China and Brazil are the most vulnerable to a cyber attack. I assume China neglected the international news source's article. China Telecom's SQL server had an extremely low processing capacity, and with us being impatient after about a month straight of downloading, we stopped. However, a few times we accidentally DDoS'd their SQL server. I guess they thought nothing of it, until we left them a little message signed by SwaggSec. They realized they were hacked, and simply moved their SQL server. No changing of admin passwords, or alerting the media. At any moment, we could have, and still could, destroy their communication infrastructure leaving millions without communication."

In the same week, India Telecom's site was shut down by a group calling themselves, Operation India, an offshoot of Anonymous in protest of the company's perceived internet censorship. And then there's just the plain old cost-of-doing business fraud and theft.

Today's communications networks, particularly mobile networks, are under siege from an exponentially growing number of devices and network entry points. Capturing the rich data available at the network level and processing it in real-time provides carriers with everything they need to protect their networks from every new up-and-coming Swaggsec, Anonymous and Operation India.

And those are just the small-time rogue hackers. There are bigger players to be concerned about from Chinese equipment manufacturers who have

been accused of building secret "back doors" into networks; to what the American Civil Liberties Union (ACLU) calls the Surveillance-Industrial Complex being pushed by the American Government and forcing private industry--even without their knowledge--to spy on it's network users.

Communications Service Providers (CSPs) need to build networks that can outsmart everyone who wants to get their hands on sensitive network data and, "Big Data" can help.

The Who, What, Where and Hows of Security Policy

According to Bill McGee, Cisco Sr. Manager of Security Solutions, by capturing the rich level of data available at the network level, carriers can know in real-time some crucial things about every person—and device—accessing the network including:

- Who are you?
- What are you trying to do on my network?
- When are you trying to do it?
- How are you coming into my network?

"The idea that the network and all the data that touches the network generates a rich level of information and that if I can extract that, I can better manage security," McGee says. "You want to design a system that's able to leverage a network and that pulls things like net-flow data or connectivity data an add that to the decision-making tree."

One of the existing problems is that network operators often make piecemeal or myopic decisions when it comes to network security instead of building a long-term strategy with the network in mind. When selecting vendors, CSPs need to make sure their solutions can handle next-generation traffic and data.

Today's communications networks, particularly mobile networks, are under siege from an exponentially growing number of devices and network entry points.

"People tend to impulse buy when it comes to security and data," McGee adds. "You need to have a long-term strategy. We've been passing voice traffic on our network for about eight years, there are still firewall vendors who can't handle that," McGee adds. "Then you have to either block that traffic or punch a hole through the firewall to allow voice traffic."

The BYOD Problem

New big data-oriented network security solutions drill down to the device level an automatically enforce policy related to that particular device. This is something that in the past, networks would have had to rely on for humans to enforce.

McGee explains the solution Cisco employs that allows policy decisions to be made at the device level with it's SecureX solution. The network detects new devices coming on to the network and allows limited access until the user can verify that the device meets that network's policy. A very important feature for the emerging bring-your-own-device (BYOD) challenge.

"So now I say, 'no device attaches to my network without me knowing about it,'" McGee explains. "An I can restrict access until I know that device meets my policy standards."

For those who doubt the reality of having to configure networks for any type of device, McGee points to the annual survey Cisco commissions, "The Connected World Report." When asked in 2011 how important internet connectivity is to their daily lives, the responses were unequivocal.

"They, especially the younger respondents, put it up there with oxygen and water," McGee says. "And their device is part of who they are."

Networks that are able to support any device will need data-based device-level security. And for doubters who think BYOD is akin to network anarchy and think no unauthorized device can ever be allowed on the network, McGee has a warning:

"It's probably already happened and you just don't know it yet," he says.

A recent Amdocs survey of service providers around the world found that most respondents feel that security is the biggest challenge to their business customers' BYOD initiatives. 73 percent of North American service providers, 75 percent of EMEA providers, 88 percent of CALA respondents and 50 percent of APAC service providers reported being worried about BYOD security. Big Data, device-level security solutions, are the answer to that problem.

Toxic Data

With the massive amounts of data generated and stored in a Big Data environment, it's important to differentiate the various security threat levels particular to the type of information it contains. In the Forrester report, "The Future Of Data Security and Privacy: Controlling Big Data" analyst and author John Kindervag identifies some data as "toxic."

"Toxic data is any data that could be damaging to an organization if it leaves that organization's control," Kindervag says. "Typically, toxic data includes custodial data — such as credit card numbers, personally identifiable information (PII) like Social Security Numbers, and personal health information (PHI) — and sensitive intellectual property, including business plans and product designs." Then, there is the data that networks have, but do not own, like customer billing data. Kindervag recommends a big data scheme that recognizes these varying levels of necessary data security and creating silos accordingly.

New big data-oriented network security solutions drill down to the device level an automatically enforce policy related to that particular device. This is something that in the past, networks would have had to rely on for humans to enforce.

So Many "Ways In"

"Typical threats include denial of service (DoS) or distributed denial of service (DDoS) attacks where target servers are overwhelmed with gratuitous traffic aimed at them in order to cause service disruption," Johnnie Konstantas, Director of Product Marketing for Juniper Cloud Security says. "Other threats include malware and viruses embedded in legitimate applications streams like database traffic or social media, and infections of mobile devices like smart phones and tablets which can then be used as launching pads into the network so that valuable data can be exfiltrated."

Konstantas adds that security starts with monitoring all of the ways data can get "in" the network. The most common of these are:

- **Mobile devices**: malware for android and all things "device" abound. Monitoring these for "bad" apps and unwanted access as well as controlling their authorization on the network is key.
- **Data center perimeter:** network firewalls have always been the first line of defense here but the proliferation of attacks requires high-performance devices that can handle automated attack attempts while allowing legitimate traffic to flow without disrupting business.
- **Web servers:** the latest data breach reports show that the vast majority of attacks are launched against web traffic and servers. When it comes to protecting them, no number of measures and counter measures are too many.

"As Big Data initiatives ingest more and more data that provide enhanced business value to corporate leaders, enterprises will face significant risks and threats to the repositories in which they keep that data," Kindervag adds. He goes on to recommend Forrester's "Zero Trust Model" of security that only

allows the, “right user to get the right data at the right time.” This approach demands network monitor usage patterns, killing potentially damaging or sensitive data to keep it out of the hands of criminals and protecting sensitive data from unauthorized access.

Sound hard and expensive? Maybe not. Moving toward a “Zero Trust Model” Kindervag asserts, can be accomplished by doing four things right now:

1. Moving controls from the edges of the network closer to the data itself
2. Leverage existing technologies you already have and make sure they’re updated to protect against the latest threats
3. Direct the legal department to establish clear policies on data storage and disposal
4. Diligently control access to data and update access as employees leave or change roles within the organization

Big Data is here and CSPs are looking for new ways to make it work for them every day. But the potential security threats are real. Kindervag summed it up beautifully when he said, “Companies are just starting to experience the joys of Big Data. Like any new love affair, the participants are blind to the flaws of their beloved.”