XO Network Security SENTINEL

Vol. 4 Issue 3, October 2014

Shellshocked

Between September and December of 1944, the U.S. Army fought the longest single incessant battle in its history: The Battle for Hürtgen Forrest. You won't find many movies about or pop culture touchpoints to Hürtgen Forrest, even though it was one of the most harrowing military campaigns in the history of close quarters combat. Why? Because after Normandy and the Battle of the Bulge, it was just another epically horrific battle. Just another inglorious chapter in the Book of Things that Suck.

On September 24th, news broke that yet another apocalyptic network security exploit was upon us. Like any demonic presence, this exploit went by many names: Bash. Bashdoor. Bashbug. Shellshock.

The UNIX/LINUX command line exploit has been with us since 1993. It allowed ne'er-do-wells to append botnet executables to the concatenated end of function definitions stored in the environment of value variables. It had never been quite as easy for cyberscum to lean back in their task chair and loose their flying monkeys on unsuspecting legitimate traffic, clutching Cairn Terriers made of flashing light and skipping along our networks in adorable digital gingham skirts.

The worst. The worst of the worst. "And the award for the longest-running, most damaging security exploit in the history of exploits goes to…"

Meh.

Considering the scale, there was not much hue and cry this time. What happened to Chicken Little? What happened to good, old-fashioned, two-feet-off-the-ground-at-the-same-time panic?

After the previous security salvos and skirmishes we've seen in 2014, XO was battle-hardened. We knew what to do with Shellshock. The mitigation processes were already in place. The customer communication channels were established. XO immediately knew which assets were affected (and which were not affected). The configuration of our IP/MPLS Core Network had already been hardened against any possibility of extracting confidential information of XO or our business partners. Where the customer portals and managed security elements were concerned, we had plenty of practice and plenty of twitch muscle chambered to move against the next big apocalyptic exploit.

We can't imagine the scope of the *Next,* Next Big Apocalyptic Exploit™ that will be foisted upon us in a week, in a month, or perhaps next quarter. But we're ready for it. We'll patch. Then we'll patch the patches. Then we'll wait for the next sleeper cell exploit to blink its beady eyes awake and crane its neck forward and we'll do it all again; a little faster than we did it the last time.

We'll keep marching forward. One day they are going to run out of trees to hide behind.

The Last Time We Fold out the Kids' Table

All but a single XO vendor have been migrated off of the generic AceTele vendor VPN group and provided with their own vendor specific access! Notifications are being prepared and the shutdown of this group is imminent.

We await our last group of valued partners to succumb to peer pressure and migrate to their own access so that XO can flip the switch on AceTele for good.

Another Fruit Basket from Belize!

The next chapter of our vendor VPN and extranet migration efforts turns to Ceridian. You know, that minor function of XO operations we colloquially refer to as payroll? Hey, no problem. But if at any time on November 4th you happen to see our VPN guy driving to a non-extradition country at high speed, we suggest you contact your local authorities and make your mortgage payment as quickly as you can.

After this major migration, XO will only have a handful of vendors left on our old equipment.

Purple Prose

XO upgraded their enterprise SharePoint presence. Just in time. The previous version was so old that the revision numbers were written in Sanskrit symbols. No more! SharePoint Version bird eye ankh has been replaced with SharePoint 2012.

All of the handy Network Security page links you bookmarked still work, but they take you to a lonely unkempt vault of outdated information with a faulty fluorescent bulb covered in cobwebs blinking erratically overhead.

The latest and greatest (and purpler) Network Security pages start here. Ironically, (or inevitably, depending upon your innate saturation of cynicism) the 2012 version of Microsoft SharePoint does not play well with Internet Explorer 8.0; standard XO install. The new SharePoint is best viewed in Chrome or Firefox. We ask you to update your bookmarks, lest you find yourself asking a Wes Craven villain for a platform installation doc.

Breaking Glass and Faking Names

XO has successfully tested our Authoritative DNS failover! We worked with our DNS vendor, Neustar, to test a new failover system that allows us to roll back our domain name servers to a previous 12 hour period should things go awry. Neustar is backing up the DNS zones to separate environments so that if we need to roll back due to problem, we're ready for reset.

Can't Touch This

DNS DDoS Mitigation testing is ongoing. We are close to selecting a vendor to protect our DNS caching platform for the ongoing attacks we experienced since taking ownership of our own DNS caching last year. We expect to choose a vendor and begin deploying this new platform before the end of the year.

The Largest Security Team in Telecom/IP

In October of 1986, NBC ran a one-time commercial teaser for its upcoming launch of the sitcom *ALF*. The commercial was a mock press conference where mock journalists asked straight-man questions to furry, brown puppet Gordon Schumway (aka Alf), ensconced behind a presser podium.

One reporter stood and asked, "Alf, how many people work on your show?"

Alf cocked his head and considered the question. "Mmmm, about half."

I had occasion to flash back to this witticism recently when I was at a Trade Show function with XO's security guru, Andrew Gough. A vendor asked Andrew, "How many people does XO employ?"

Andrew knew the answer. "Approximately twenty-six hundred."

The vendor's follow-up question: "And how many of those are responsible for security?"

Andrew answered, "All of them."

Truer words. XO has several parallel teams charged with finding security gaps and spackling them shut, as well as repairing network functions that are "broken" after a security incident. But the culture of XO is to encourage every single XO employee and business partner to proactively consider the security consequences of our day-to-day business activities.

Are we filling out VPN or network access paperwork for a vendor without fully understanding *why* that vendor needs access to a given XO element, platform, or network?

Are we giving out phone numbers and job titles of other XO employees to unknown outside callers who may be using them for social engineering?

Are we selling a service to a potential customer conditional upon an XO location audit where auditors must enter CO facilities to check the security of data that XO doesn't even collect in the first place?

Are we designing platforms and processes with Old School string password authentication when two-factor RSA token authentication is available?

Have we cleared a biometric scan lock on a door, only to turn around and hold the door open as a courtesy to a vendor we don't know quick-stepping toward us?

Every XO employee is responsible for security. It's an "additional duty as assigned" for all of us. XO is working hard to assemble the largest Security Team in the entire Telecom/IP Sector.

Welcome to the team. Don't forget to add us to your CV.

RADIUS: Keeping Haters Warm Since 2001

It's no secret to anyone on this email distribution list that we have had several serious events affecting all logins to the network elements.

You're frustrated. We're frustrated. Thanks for the phone calls and all the creative new vocabulary you've taught us. I always thought my mother was a saint, but… Who knew?

From our perspective, much of the "kaboom" is preventable if folks vet their apps with a few general rules in mind: Application should login to pull the configuration no more than once a day (besides provisioning/troubleshooting, of course). Please route your stat collections through SNMP and at a rate no less than once every five minutes. Also, we're a bit uncertain about why you'd need multiple concurrent sessions or frequent login instances.

But we don't know everything. If you find yourself skirting the weedy periphery of our guidelines above, we'd appreciate a phone call so we can identify you as a fellow Bigfoot hunter and not a Sasquatch.

It's all fun and games until somebody gets 'squatched.