Security Trends in 2016: Pervasive Insecurity

Chase Abbott, 2017-06-02

The term pervasive insecurity defines widespread and unwelcome instability or weaknesses in standardized systems. These systems are usually complex and can include poverty, political landscapes, or civil unrest. It's also a fantastic term to illustrate the train wreck of information systems security failures and publicized vulnerabilities last year. Over the last year we've seen booming trends against embedded device exploits, data ransoming, and similar public displays of nefarious behavior. Why was 2016 such a banner year for exploitation? Who got pwned? What's our next steps to not protect ourselves but prevent our selves from being unknowing agents in coordinated attacks across the internet?

The Data Didn't Look Good Then, Do You Think It Got Better?

In 2010 researchers at Columbia University published results of a internet scan including basic analysis of connected devices and their potential for exploit using only low or basic levels of effort. Researchers were trying to discern past exploits, large scale attack feasibilities, amount of discoverable devices, and potential methods of securing devices. The numbers they published would be intimidating by today's standards but given we've had 6 years to continue the trend of inscurity, it's only getting worse.

Creepy Results Of Default Credential Scan (2010)

- IP's scanned: 3,223,358,720
- Devices Targeted Post Discovery: 3,912,574
- Vulnerable Devices: 540,435
- Vulnerability Rate: 13.81%

Section 4.1 of the paper specifically calls out the DDoS potentials of devices identified in the study. Remember... 2010 people. If this threat isn't new and was well documented back in 2010, why is 2016 special?

Infecting the Internet Of Things In You House

Mirai was your big news source of late 2016 not because it exploited what the Columbia researchers knew in 2010, it was the largest publicized example that insecure connected systems pose. First KrebsOnSecurity experienced a ~620Gbps DDoS attack and shortly after OVH Cloud Solutions experienced a 1Tbps peak bandwidth attack. The reported 150,000+ connected home devices participating provided from 1Mbps to 30Mbps of bandwidth; together it was the largest known DDoS attack published to date. The true reasoning theorized by Brian Krebs may or may not be true but we didn't witness the potential Mirai posed. By releasing the source code Mirai's secret weapon of quietly locking systems could be outdone by someone willing to modify the code further. Diluting the compromised devices with multiple sources reduce each command and control servers effective attacking potential and so far, exploiters haven't been known to work together yet.

You Didn't Do What To The Database?!? And Our Data Is Where?!?

Poor MongoDB. It was the first public name associated with a string of database ransom requests starting late in 2016 and extending to... well... it's still going. Bleepingcomputer's coverage on security researchers Victor Gevers and Niall Merrigan investigation of multiple groups responsible for deleting databases and leaving ransom notes (not per the norm of encrypting and leaving on service). To date the attacks are against MongoDB, CouchDB, Hadoop, and Elastic Server services. Reading the tweets by Victor and Niall, the fever pitch of updates is comparable to race track announcers. And just like the Columbia researchers warned, these are not high level complex attacks. The systems compromised were exposed instances with no modified access controls or elevated authentication and the combined tally of pwned systems is hitting 50,000. As of today, Cassandra databases are now receiving threats to secure data. This is becoming a Game Of Thrones nailbiter and I want to keep reading!

> Someone is warning unaware unprotected Cassandra database (https://t.co/2UcEiraM5l) owners by creating an empty "your_db_is_not_secure" db. pic.twitter.com/XDfvSPjeno
>
> — Victor Gevers (@0xDUDE) January 24, 2017

You Don't Learn Anything The Second Time The Horse Kicks You

The leak of sexy swinging data from Adultfriendfinder.com and their subsidiaries was a lesson in failures to learn from prior mistakes and a lack of data governance. Using known local file inclusion exploits and demonstrated to CIO magazine by security researcher 1x0123, password files and database schema on Adultfriendfinder.com production servers were made publicly visible. This exact LFI exploit was later used to release user data. How many were affected you ask? Oh... a little over 412,000,000+ users and no my finger did not get stuck on the zero key. Frustratingly for their users in 2015 3.5 million Adult Friend Finder accounts were to be released unless a $100,000 was paid to an angry admin in Thailand who claimed company owned his friend money.

Exposed from the more recent AFF hack database details showed deleted users accounts were only being updated with a @deleted.com suffix (read the below Leakedsource link for details). Anyone that created an account and then deleted it never really had their data removed. This sets up Adult Friend Finder for a large class action lawsuit if the 63 million current users file along with anyone who ever had an account; all are eligible to file. It could've been prevented. A security audit, basic data governance, basic understanding of exploit vectors. The business decisions or failure of AdultFriendFinder systems teams may never go public but it does illustrate that security failures happen to any company size and not small dev shops. Leakedsource.com's has great details of the breach for some nice happy hour reading.

Moving On... I Hope

Oh 2016, thank goodness you're over but I have a feeling 2017 isn't going to be any better. From the data we know the threats have been around and apparently we're not doing enough to mitigate them but how do you tell your mother or brother to remember to check that telnet is disabled and ssh is only allowed from internal ports? How do you tell your grandparents to "go be security experts" suddenly because they have an internet-connected picture frame? You can't so now what? ISP's and backhaul networks need to be more responsible about preemptive monitoring for elevating malicious traffic. The technology is there but why should they pay for our inabilities to secure our systems? Manufacturers need global accountability to prevent releasing vulnerable products. They know that, but no single entity is regulating their sales so until someone clamps down and imposes restrictions, c'est la vie right? But really:

- We don't need connected hairbrushes
- We don't need connected toasters
- We don't need remote notification that our laundry is done

We don't need a lot of things... but we want them. Our desire drives consumption and in turn will drive the industry, secured or not. Like our friends at Columbia University illustrated, we are living in a world of pervasive insecurity and that's never going to change. I'll be at my boat now. There's no internet there, only ocean.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com