Cybersecurity in Miami

Dr. Brent Kirkpatrick[*]

July 7, 2016

Intrepid Net Computing

www.intrepidnetcomputing.com

[*] bbkirk@intrepidnetcomputing.com

Abstract

Using publicly available data, Intrepid Net Computing has evaluated cybersecurity in the cities of Miami and Coral Gables, Florida. We use buttressIT^{TM} , a proprietary audit methodology based on data science and artificial intelligence.

This report outlines the cyberinfrastructure currently in use. We assess the cybersecurity vulnerabilities of the services offered by a number of Internet Service Providers. We reveal some activities of the most prominent hackers and give IP addresses for their rogue servers. We suggest solutions to these security problems.

1 Introduction

Hacking harms our whole economy, from small business to big business and from the technology industry to the healthcare industry. On average, businesses loose millions of dollars in each cyberattack. The cost to our economy as a whole is on the order of billions of dollars.

The average cost of a single data breach is now $4 million [1]. The average cost per stolen record is $158. Compared with information from 2013, this is a 29% increase in the cost of data breaches. The cost of recovering from hacking is soaring.

In a world where data theft is popular, the best measures are preventative, rather than restorative. By employing state-of-the-art security measures, companies can spare themselves the outrageous cost of recovering from data theft. The cost of implementing these security measures is minuscule when compared with the cost of recovering from theft. Preventative measures include: audits, upgrades, and proper network design.

Intrepid Net Computing addresses today's cybersecurity challenges with data science and artificial intelligence. In our world of ubiquitous computing, the number of computers in the average workplace out-numbers the number of people. Computers are everywhere: in cars, in cell phones, in watches, in toys, in calculators, as well as in the more traditional devices: laptops, tablets, and desktops. In this world, cybersecurity has become commensurately difficult. To address these challenges, Intrepid takes a system-level view to collect and analyze data that reveals the cybersecurity of a group of networked computers.

The remainder of this report will discuss several key components of the Internet infrastructure and its security. Each component will be graded on the subjective scale used by Intrepid Net Computing to compare the security of various locations. This is a shield rating where the number of shields awarded each section indicates how prepared Miami is to face cybersecurity challenges. Five shields indicates optimal preparedness and zero shields indicates critical problems.

2 Physical Infrastructure

The physical infrastructure of the Internet is unknown. Dozens of organizations contribute to creating and maintaining the existing infrastructure which consists of fiber-optic cables, telephone cables, coax cables, dedicated high-speed cables, underwater cables, satellite connections, and cell towers. Since no single entity is responsible for the entire infrastructure, nobody knows the layout of the entire network. Each organization knows the layout of their portion of the network, but this information is not always communicated between organizations or with the government.

Discovering the layout of the physical infrastructure in the city is a scientific problem. In data science, when we wish to discover the structure of an unknown network, we turn to statistical methods that infer the network from data. In biology, these methods are used to reconstruct the tree of life [2] or the network of life [3]. Similar methods can be used to discover the layout of the Internet.

Intrepid Net Computing has collected data and used a network-discovery method to estimate the layout of the Internet. Figure 1 shows our estimate of the layout of the Internet infrastructure. The darker edges indicate the 'Internet backbone' which consists of dedicated high-speed, high-bandwidth data lines that were installed in the late nineties and early part of this century. The backbone was created to connect key computational infrastructure abroad and in the United States that includes universities, supercomputer centers, and government laboratories.

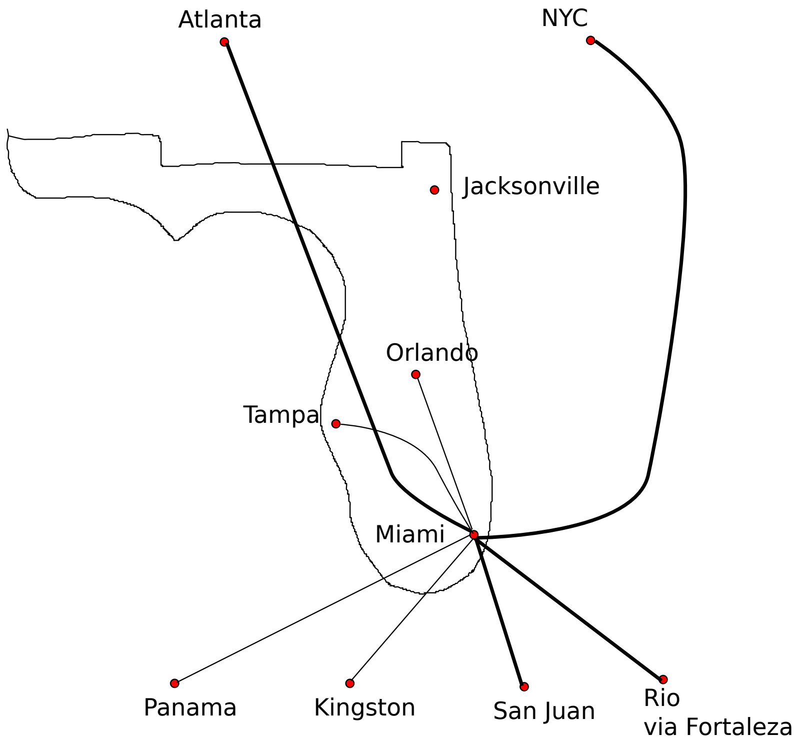

Figure 1: **Layout of the Internet.** This is an estimate of the layout of the Internet infrastructure in and near Miami. This map is not to scale and near is referring to cyber-distance, not physical distance. While there may be some incorrect lines in this figure, this estimated layout is largely accurate. Darker edges show dedicated high-speed lines.

`buttressIT`$^{\text{TM}}$ Rating

★★★★☆

The Internet backbone runs through Miami. Miami is a hub of undersea cables [4] that provide Internet service to the Caribbean and parts of Latin America. There are several Internet Exchange Points [5] in or near Miami, including the Verizon Network Access Point of the Americas [6]. This makes Miami, not only the financial capital of Latin America, but also it cyber-capital. It is no surprise that much of the high-tech industry in Florida is located in Miami.

The speed of Internet service in Miami is fairly good with fiber optics installed in many residential neighborhoods. The speed is not part of our rating.

In terms of reliability, the physical infrastructure in Miami is quite reliable. There are occasional outages with the primary threats being due to hurricanes.

In terms of security, the physical infrastructure is fairly secure from physical hacking. Only physical hacking is included in the rating for this section. Relative to other parts of the country, there is quite a lot of software hacking in the city, which we consider next.

3 Software Infrastructure

Crucial elements of the Internet infrastructure involve software that routes data through the physical network. Similar to freeway interchanges and cars, there are computers on the Internet, called routers, that help data choose the proper path through the Internet network. The data packets are like cars on the freeway, each with its own destination. The routers are interchanges, and the domain name service (DNS) acts like highway signs.

If the software infrastructure functions properly, then traffic on the Internet is reliable. This means that when you, as a user, connect to the Internet, your traffic will reach the destination that you intend. In other words, when you communicate with a server, it will be the server that you think it is.

If the software infrastructure is insecure, then traffic on the Internet may not reach its destination; it may get routed to a different destination than the user had in mind, or it may not be authentic. For example, suppose that you want to visit your bank's web-site to do a financial transaction. The first step of the process is for your web-browser to use the DNS system to look up the IP address of your bank's web server. After that, your web browser creates a connection with the bank's server and an exchange of information occurs. If the DNS system gives a fraudulent response, then you might actually connect with a hacker's server that is masquerading as your bank. If the traffic is fraudulent, a hacker might be able to inject incorrect information into the transaction. Any of these possibilities can result in data and identity theft.

Intrepid Net Computing uses `buttressIT`™ a proprietary audit technology to asses the quality of the software infrastructure. Our approach examines the routers and DNS servers to determine whether they are hacked. We also look at the generation of DNS technology that is installed a local network.

`buttressIT`™ Rating

⛉⛉⛉⛉⛉

There is relatively little security in the software infrastructure in Miami. The city relies on the good intentions of its users to maintain security. This strategy does not work, as there appear to be many sophisticated hackers, either in the city or targeting it from afar.

More recently installed or configured Internet service has better software security. Some businesses, such as Starbucks, rely on successful software companies to provide their Internet, and this service can come with better-than-average security.

Organizations that have their own IT departments have the opportunity to set their own security standards. These include universities, hospitals, and banks. However, many of these organizations are falling behind on security upgrades and training.

Secure Public WiFi Hotspots

A number of businesses are progressively secure, and some of these businesses offer public WiFi hotspots. If you are traveling in Miami or working away from home, please use one of these secured networks for sensitive Internet transactions.

Neighborhood	Business	Location
Miami	Starbucks	on US 1 across from the University of Miami
South Miami	Starbucks	Barnes & Noble in the Sunset Mall
Dadeland	Dadeland Mall	off US 1

4 Internet Service Providers

The two largest providers of business and residential Internet are AT&T and Comcast. Additionally, there are a number of other companies and providers that own infrastructure or buy bandwidth from the infrastructure owners.

buttressIT™ Ratings

Following the buttressIT™ audit method, we rate each of the major service providers for security. We rate based on physical and software infrastructure security. The speed of the connection does not factor into this score.

Provider	Product	Rating
AT&T	Residential	⬜⬜⬜⬜⬜
AT&T	Business	⬜⬜⬜⬜⬜
Comcast	Business	🟨⬜⬜⬜⬜
Google	By Contract	🟨🟨⬜⬜⬜

Generally, business service that has been installed and configured recently tends to be more secure than older business service that has not been maintained. Residential service tends to have worse security than business service. Generally, the ISPs are not keeping pace with security upgrades.

Some organizations run their own sub-network infrastructure and manage their own security. This means the organization can guarantee that upgrades happen and that state-of-the-art security is installed. This has a higher up-front installation cost, but can yield the best results for security.

5 Hackers

There appear to be hackers operating with impunity in and near Miami. The buttressIT™ evidence suggests that every computer in Miami may have been exposed to tainted updates. The buttressIT™ audit also locates several suspicious servers in the metropolitan area that are likely rogue servers.

One of the gravest risks, today, is DNS poisoning due to the frequency of hacks and the damage to systems. [1] Most ISPs software infrastructures are very vulnerable to these attacks. To poison a DNS entry, the hacker inserts the IP address of their own server into the DNS domain directory and creates a fraudulent DNS IP entry. This is analogous to a vandal changing a destination on a freeway sign at an interchange. That vandalism causes a similar kind of chaos as poisoned DNS entries on the Internet.

Suppose that you are interested in updating your computer's Adobe software. When you hit the update button, your computer will ask the DNS system for the IP address of Adobe's update server and then will request the update from that server IP address. Suppose, instead, that a hacker has poisoned the DNS entry for Adobe's update server and has inserted the IP address of a server they control. Then, your computer will be directed to get the update from the hacker's server. Since updates are trusted by your operating system, the hacker will likely get complete access to your computer.

Hacker's are typically interested in adding your computer to their bot-net, which an illegal, distributed computing infrastructure for launching attacks. In some cases, hackers will want your identity or financial information. In other cases, hackers might pilfer your business files and customer financial information.

[1] Proprietary data.

buttressIT™ Rating

⛉⛉⛉⛉⛉

Intrepid Net Computing uses the buttressIT™ audit method to detect DNS poisoning and identify servers that are either administrated by hackers or are zombie servers (legitimate servers that have been taken over by hackers). There seem to be a number of these rogue servers targeting computers in the Miami metropolitan area, and the DNS servers for the city appear to be poisoned.

The evidence collected during our buttressIT™ audit is highly suggestive that the following IP addresses are likely belong to rogue servers.

IP Address	ISP of Server	Server Location	Updates	Affected ISP DNS
198.105.244.130	Search Guide	?	Windows	AT&T
198.105.254.130	Search Guide	?	Windows	AT&T
66.109.26.212	Galaxyvisions	near Atlanta or NYC	CentOS	AT&T
23.202.57.101	Akamai	Univ. of Miami (UM)	Redhat	UM, AT&T, Comcast
23.202.62.138	Akamai	Univ. of Miami	Redhat	UM, AT&T
23.78.222.120	Akamai	South Florida	Adobe	AT&T, Comcast
23.78.223.179	Akamai	South Florida	Adobe	AT&T, Comcast

The Galaxyvisions server, 66.109.26.212, is very suspicious. In particular, since CentOS is an open source operating system with an up-to-date list of approved mirror servers, we looked for this server on the mirror list. It was nowhere to be found. This particular CentOS update server is most likely rogue.

The last two Adobe update servers are also startling in their unlikely DNS entries. They are listed with very inconsistent entries in queries to the DNS servers. This is highly suspicious, and an event that we have not observed anywhere else.

6 Solutions

The principle goal of cybersecurity is prevention. This means keeping up with the latest security innovations, understanding the risks, and being knowledgeable computer users. Knowledgeable users can direct their online activities to more secure services. Knowledgeable users know when to perform updates and when to ask for help. Knowledgeable users also know their risk profiles and restrict their most risky activities (i.e. financial transactions) to safe Internet connections.

Organizations that are responsible for Internet infrastructure need to be especially vigilant of risks and upgrades. Every ISP and web hosting service needs to introduce DNSSEC as soon as possible. Using old versions of DNS remains one of the most significant risks to the entire Internet.

Cooperation between multiple organizations is increasingly necessary to catch hackers and stop their activities. A single hacker might serve fraudulent updates for several software vendors by using one ISP to deliver traffic to their fraudulent server while attacking the DNS system of multiple ISPs. Since hackers use multiple technologies and attack multiple infrastructures to spoof many users, we must cooperate to stop their hacking.

Government aid is increasingly available from the FBI and the DHS. The FBI investigates cybercrime and the DHS works to prevent and track cybercrime. The DHS provides audit teams through the NCCIC's NCATS teams (ncats_info@hq.dhs.gov). The DHS also provides incident response capabilities through the CyberSecurity Advisors (cyberadvisor@hq.dhs.gov). Both services are free of charge and offered on a first-come-first-serve basis. The DHS also tracks cyberincidents through its information sharing programs: IT-ISAC, US-CERT, and AIS. The AIS system is a real-time database of security incidents. The FBI offers an industry-government cooperation program: IfraGard.

The technology industry also provides help in the form of security audits, intrusion response teams, and targeted security for specific software. Much of the effort is aimed at providing patches and updates for specific vulnerabilities. The system-level perspective of security deserves more attention. Intrepid Net

Computing offers data-centric audits, intrusion response, and breach clean-up. We also offer state-of-the-art enterprise and mobile security in packages that scale to your business needs.

Biography

Dr. Kirkpatrick has a bachelor's in computer science from Montana State University-Bozeman, a master's and a Ph.D. in computer science from the University of California, Berkeley. Dr. Kirkpatrick is an expert in deterministic and statistical computer algorithms, and his main application area is the field of computational biology, in particular genetics. Due to market pressures, Dr. Kirkpatrick has applied these skills to computer security. Intrepid Net Computing takes a data science perspective on solving challenging security problems.

References

[1] Ponemon Institute. 2016 cost of data breach study: Global analysis. *Ponemon Institute Research Report*, 2015.

[2] C. Semple and M. Steel. *Phylogenetics.* Oxford University Press, 2003.

[3] Dan Gusfield. *ReCombinatorics: The Algorithmics of Ancestral Recombination Graphs and Explicit Phylogenetic Networks.* The MIT Press, 2014.

[4] The Internet's undersea world. http://image.guardian.co.uk/sys-files/Guardian/documents/2008/02/01/SEA_CABLES_010208.pdf, 2008. Accessed: 2016-06-29.

[5] List of Internet exchange points. https://en.wikipedia.org/wiki/List_of_Internet_exchange_points. Accessed: 2016-06-29.

[6] Thomas Sparrow. Behind the scenes of latin america's Internet 'brain'. *BBC Mundo.*