GLOBALX

JANUARY 2017

CYBER-SECURITY:

PREVALENCE, RISK AND PROTECTIONS

As we increasingly depend on an ever-more connected world, the risks of living in this world grow. While the internet offers massive conveniences and efficiencies, it also means that actors from anywhere in the world can have a massive and potentially negative impact on our personal and professional lives.

The biggest issue facing us is that life is ever more connected; the increasing power and prevalence of smart phones is just one example of how we have more technology available to us than ever before. It's hard to keep up—not only with tech developments, but with the risks to the masses of data we hold, as we continued to increase the volume and value we place on this information in these pocket-sized computing devices, our personal computers, tablets and workstations. Short of those with an IT degree or too much time to keep up with the current suite of threats out there, most of us stop worrying about our tech vulnerabilities and assume we are unlikely to ever have to deal with any malicious attack on our data.

To help you understand the current Cybersecurity Landscape, this paper will review today's threat matrix and look at what options we have to mitigate the most realistic risks. To this end, any review of this dynamic space will inherently only provide a snapshot of what is happening. As with any criminal enterprise, the scope of what is possible is limited only by the imaginations of the people concerned.

Why do cybersecurity threats exist?

In the early days, Hackers were largely motivated by recognition within their peer-group circles—generally by making a splash in the mainstream press. As such, impacts tended to be highly visible and disruptive in a short term. Since the early noughties however, malware has been focused much more heavily on becoming a profit centre for the creators. As such, the impacts tend to be lower key, but much more effective in the medium term; many victims have no idea they have been hacked for months or even years while the malware they've introduced to their system collects critical information such as online banking details and other system vulnerabilities which may be manipulated.

Generally speaking—depending on the type or scale of malevolent online behavior—there is almost no risk, but the rewards for hackers can be huge. For instance, an average Russian developer can legally earn a ~$24k salary in Moscow and meanwhile earn thousands selling malicious software on underground crime forums. If caught, Russian authorities are unlikely to prosecute the perpetrator, unless the hacker targets Russian victims (Plesser, 2014).

Further, the temptation for hackers grows with every new technology and our increasing reliance on the internet; with the wider use of untraceable crypto-currencies such as Bitcoin, it is now possible to extort money from people with an almost zero likelihood of the money being traced (Waddell, 2016).

Why should you care?

Well, that depends on how much value you place on the material on your various devices.

A review of the potential cybersecurity threats, common targets and methods of attack will help you to understand just how much—or how little—security should be undertaken to reduce the risk of serious damage or loss to hacking. This paper will help you to do just that. We start by identifying the type of Malware—which describes any software created with a malicious intent.

Defined: "Zero-Day" Defect

This is a vulnerability that has been discovered by miscreants and for which no known patch exists. These are the issues that keep security people up at night because no matter how good you are, if you don't know about the problem you can't mitigate against it.

Types of Malware

01 Identify Theft

This type of malware works to 'quietly' gain enough control of the computer so that it can monitor keystrokes or a users' personal information that will provide access to bank accounts, or to enable identify theft.

02 Extortion

Here, the hacker seeks payment—often via a Cryptocurrency such as Bitcoin which is truly anonymous and untraceable—before they will resume your affected device to normal service.

03 Espionage

Sometimes created by state-sponsored actors (Kushner, 2013), this type of malware may also be deployed as part of a commercial strategy (Zwienenberg, 2012).

04 Sabotage

Malware for sabotage can take many forms. Sometimes this is about physical destruction of machinery attached to affected devices like the Stuxnet virus (Kushner, 2013). Stuxnet is believed to have been a joint Israeli/US operation built to destroy approximately 1,000 centrifuges in an Iranian nuclear weapons enrichment plant. Other times sabotage is about brand damage; Sony has been hacked twice in recent years, resulting in massive negative global press and costs of an estimated $170 million.

05 Vengeance

Companies and individuals can be targeted by disgruntled employees, or former staff and competitors seeking to wreak havoc.

Targets for Malware

1. **Smart Phones.**
   Any device that people might choose to do banking on is a particular target.
2. **Websites.**
   These are generally a gateway to either a Server, or user desktops.
3. **Desktop Computers.**
   Malware can be introduced via the internet (email or websites) or via USB or Disk.
4. **Servers.**
5. **The Internet of Things or "IOT".**
   This refers to the multitude of new products which are internet connected like security cameras you can check from anywhere; a PVR which you can schedule a recording on while out and about. The issue is that these devices are often hideously insecure and often by design, cannot be secured. A little over 130,000 devices were recently harnessed to produce the biggest Distributed Denial of Service (DDOS) attack in Internet history (the case is detailed further in this paper).

Attack Vectors

1. Social Engineering

One of the more popular methods of executing a malicious program, Social Engineering describes where a perpetrator tricks a person to do something that will affect their machine. This is a method that has become much easier and more effective by targeting users of business-oriented social networking sites such as LinkedIn.

At a basic level, people are sent emails with malicious attachments which, if clicked, are likely to either install software that enables further access to the machine, or installs a variety of Cryptolocker in an attempt to hold your files to ransom (Simonite, 2016).

More advanced types of Social Engineering methods will target individuals with specific or personalised information to trick them into providing access to their machine or data. An example is a malicious email designed to make it look like the CEO is asking the CFO to authorise a wire transfer. By using targeted information such as job titles, these attacks are much more effective to the tune of $1.2 billion dollars in losses to business email scams (Krebs, $1.2b lost to business email scams, 2016).

2. Browser Vulnerabilities

If you can't persuade someone to do something to let you into their device via Social Engineering, then mounting attacks via the browser is the next easiest option. All browsers suffer from security vulnerabilities (Pauli, 2015). Massive amounts of valuable data can be collected from unassuming users visiting a presumably trusted website that is, in fact, a set up to collect a users' personal data.

3. Malvertising (Advertising infected with Malware)

In spite of the increasing popularity of ad-blockers (which if you don't already use, I strongly recommend) there are still many people who are served up a constant stream of adverts while using the internet. Because the cost of these ads are so low and the process for approving content is largely automated, malicious groups work hard to get their malware served up as part of an advertising network to enter your machine or network.

Malvertising can take two forms: either tricking people to click on an ad and then providing something plausible to click which subsequently infects their machine (Goodin, Google stops AdSense attack that forced banking trojan on Android phones, 2016). Or, if there are known Zero-day vulnerabilities in the wild, the malware can potentially be encoded into a video, or a picture and infect the machine simply by viewing it (Nichols, 2016).

4. Macro Vulnerabilities

If you can't get people to visit an affected website, then the next approach is to target macro vulnerabilities in a common application such as Microsoft Office. The more effective attacks come in phishing emails targeted to an individual, bearing a topical subject line to entice the user to open a Document or Spreadsheet attachment—a Russian hacking group sent out a campaign immediately following Trump's election win (Krebs, Russian 'Dukes' of Hackers Pounce on Trump Win, 2016). The attachment once opened may contain macros that effectively infect your system with a virus or a security risk.

5. Operating System Vulnerabilities

It doesn't matter which Operating System (OS) you use, they are all vulnerable. For years, Microsoft has had more vulnerabilities than any other OS, and as early as 2002 realised that security processes had to change (Maney, 2002). The change, however has taken years to take effect, but today—with integrated antivirus, greater protection against security vulnerabilities and regular patching—the Microsoft OS is significantly more secure than most (Secunia Vulnerability Review, 2014).

6. Hardware Vulnerabilities

While it is software that is typically targeted for vulnerabilities, it is also possible for hardware to be attacked. In 2015 an attack exploited physical weaknesses in computer memory chips to hijack the operating system running on them. By repeatedly accessing specific memory locations millions of times per second, attackers could cause changes to code so that an untrusted application could gain access to system privileges or bypass security measures that keep malicious code from accessing sensitive OS resources. This proof of concept was then applied to a JavaScript vulnerability that could exploit a simple Browser session (Goodin, DRAM Bitflipping exploit for attacking PCs: Just add JavaScript, 2015) and then again, it was then further refined into an attack against mobile phones.

7. Website Security

Websites are valuable targets for hackers. If a site can be penetrated, attackers have both a server to use maliciously, and means to target and attack visitors to that website. There are a myriad of mistakes developers can make when building a website that render it vulnerable to attack.

There are really two types of attacks: extortionist and vulnerability-based attacks designed to gain control of the website server. Because most websites are public facing, it is a potential entry point to a backend network and, once the server is available, the website can be configured to serve up malware to users of that website. Because website users are more likely to heed requests, and hand over information to their known and trusted website, big company websites are regularly targeted by hackers (Dede, 2010).

8. Network Based Attacks

There are a variety of different attacks that can be attempted against the network rather than just a server.

a. Distributed Denial of Service (DDoS) Attacks

DDoS attacks are designed to take a website off the air by simply overwhelming it with traffic. Motivation to bring down a site ranges from creating inconveniences for the website owner—for instance, one security researcher was specifically targeted by the miscreants he was investigating—to bribery.

The motivation to build a DDOS Attack is money; various packages and subscription services are available to purchase, priced by how long the denial of service will last. vDOS is a service that is estimated to have made $600,000 for its developers by selling malware that contributed to 150,000-plus DDoS attacks over two years between 2014 and 2016 (Krebs, Krebs On Security Hit With Record DDOS, 2016).

b. Man in the Middle (MITM) Attacks

MITM stands for 'man in the middle' and to understand this type of threat, you need just a little bit of understanding as to how the Internet works. When you go to a secure website (using https://), the SSL certificate that is served up is a cryptographic key that has been issued by a Certificate Authority (CA). The trust relationship for every CA has to be built into every browser—otherwise the browser doesn't know whether it can trust the certificate or not. In addition to this, the certificate is not tied to the specific CA at all, so any CA can issue a certificate for a domain that allows the browser to trust the visited site.

This means that if someone managed to breach a CA (and there are many of them) they could issue a certificate for a big-name website which would be indistinguishable to the average user from the real one; the browser would trust it. If you have control over the site that someone thinks they are visiting, then it is relatively easy to steal credentials (Ducklin, 2013).

c. Wi-Fi Network Attacks

Did you know: people sharing your Wi-Fi network can easily view the local network traffic? A few years ago the Firesheep extension to Firefox was released which would allow anyone to steal unencrypted credentials on the local Wi-Fi network. Companies as big as Facebook didn't encrypt that information by default until this attack and since, while most large companies (including Facebook) have fixed things up, public Wi-Fi remains a relatively risky exposure for your devices (Fitzpatrick, 2010).

Wi-Fi networks are, by definition, public. Information is transmitted over the air which means that people can directly target the wireless signal. For instance, in 2016, groups at the University of South Florida and Massachusetts demonstrated a new technique that observes changes in a Wi-Fi signal to identify a users' passwords and personal information as it is entered onto a smartphone (Chirgwin, 2016).

9. Vendors

Sometimes Vendors deliberately include vulnerabilities in their products which cause security problems. The first major instance of this was in 2005 when Sony included an invisible rootkit on approximately 22 million music CDs which, when inserted would illegally add a rootkit onto the target computer (Rootkit, n.d.). This software—which could not be uninstalled—modified the computer's OS to interfere with CD copying, but it also introduced vulnerabilities that were exploited by unassociated malware.

Sony denied being responsible for the malware which would 'listen' to a users' behavior and 'phone home' with this information; the company also denied any harm caused by the rootkits, but eventually addressed public outcry and government investigations with consumer settlements, a recall of affected CDs and a suspension of CD copy protection efforts in 2007. Lenovo were caught doing a very similar thing more recently, in 2015 (Khandelwal, 2015).

Mitigation

As you can see, a significant threat landscape exists in this ever-connected world, but a security strategy is really a risk management activity.

If your data is not sensitive, and has little commercial value, then the risks of hacking are relatively low. You do, however, need to think about the cost if something bad happens; if you can't afford the downtime in a major situation, or if the data is sensitive, costs increase and so, more attention needs to be paid to this.

Sometimes I find it bizarre anything happens without problems in the cyber landscape. But there are things you can do to help protect yourself. None of this should be news but it is always good to reiterate best practice.

Note: when thinking about this, understanding whether threats are local (i.e. on the current machine) or remote (over the network) is an important distinction as it will change the approach to the mitigation. It is easier to exercise a remote vulnerability than a local one. But be aware, that combining threats together in order to gain access to a local vulnerability is a stock tool of the potential miscreants.

1. User Training

This is—by far and away—the best first step you can take. Nothing can protect you from people doing stupid things, or being tricked when they don't know what to look for. The way to stop that is to train people.

Regular user training to provide examples of the latest threats and the type of scam being run is critical to make people engage their brains when faced with making a decision. How many people when they get a call from "Telstra" validate that they are in fact from Telstra?

2. Patching

The next most important protection is to ensure all your devices are regularly patched. The best way to apply security patches for any product is to automate this process; if the patching is manual, you're opening yourself to forgetting to update, leaving your products unprotected.

a. Phones

There is immense variability in the speed of patching for phones. Apple are by far and away the best for this due to their control of the entire ecosystem, followed by Nexus (now Pixel) phones from Google. Why not Google your phone manufacturer to look at patching cadences to ensure you're up to date?

b. Desktop PCs

These should be patched automatically within a day or two of a patch released (this happens once a month for Microsoft—otherwise known as "Patch Tuesday"). I get regular complaints from my users when the machines need patching, but there really is no choice; ideally, you should configure your machine so patches will apply automatically overnight and reboot the machine accordingly. If the machine is turned off, or something stops the machine from rebooting, give the user the choice of when to reboot. If they don't reboot then force the issue. It's a little painful, yes—but better than the alternative.

c. Servers

These are hard—you want them patched, but you need to be able to test them to ensure that the patches don't break critical infrastructure. Depending on what they do, this is more or less dangerous. You need to talk to your IT team to work out the best way of managing this process with a dashboard showing what is fully patched and what isn't so appropriate action can be taken.

When IT teams start talking about DevOps—this is often a shorthand for being able to treat infrastructure as code—which allows environments to be built up and torn down at the touch of a button. It is a complicated state to get to, but with effort it means that security fixes are trivial.

3. Paranoia

Patching isn't enough to secure your systems. Zero-days always exist (allegedly the NSA stockpile them in case they need them for any purpose, although this is denied (Hern, 2016)) and as such, you have to assume your systems have been, or will be, compromised. Consequently, a layered approach to security is best-practice. Given the size of the domain here, more detail is out of the scope of this paper. But having multiple, layered security defences will definitely help. Do not trust internal systems because they are inside the firewall.

Application white-listing is also very powerful as that stops people from running unexpected programs. This needs to be managed carefully however.

4. Don't use Public Wi-Fi unless you know what you are doing (Gordon, 2014).

In essence, by default, other people's networks should not be trusted. How often do you plug your computer into someone else's network? Every time you do so, you open yourself up to risk.

I personally never use free Wi-Fi and prefer not to plug into other people's network, just in case. 4G SIM cards are so cheap these days for huge amounts of data it is much better to provide those than to rely on luck that the network you plug into doesn't have anything malicious on it.

5. 2-Factor Authentication

Or 2FA—if you can remove the need for passwords, or use them in conjunction with a one-time key (OTP) to authorise actions, this is a really good mitigation activity.

6. Use a Password Manager

One problem these days is the sheer volume of passwords you need to remember. Because of this, most people use a small subset of passwords. The problem with this is that if one site gets hacked, other accounts can be compromised thus leading to identify theft. By using a password manager you can use individual passwords for every account you need (I currently have 111 passwords stored in my password manager).

All of the passwords I have in my password manager are random 20 digit passwords containing anything. For those passwords I have to remember, I use a pass phrase, not a password. A pass phrase is a combination of words which are (preferably) not generally used together. So a password like "iloveyou" is not secure because it is a known phrase (and very short). A more secure alternative might be "correcthorsebatterystaple" which is long and memorable (Password Strength, n.d.). Although now those words have been published, don't use them! Pick 4 other words at random. Preferably still, pick 4 words which might not be in the dictionary—strange place names, characters from books (not Harry Potter or other hugely famous books though). And switch up a couple of the letters with numbers.

The reason for this is that password breaches are so commonplace nowadays that there is a huge database for bad actors to learn from. To date in excess of 1 ¼ billion passwords have been stolen (Regnier, 2014) which means that Big Data analytics have been applied to the way people choose passwords. In addition to this, the use of highly parallel computing devices (otherwise known as Graphics Cards) have dropped the price of brute force attacks to levels thought unimaginable a few years ago (Szczys, 2012); once passwords have been stolen, the cracking tools can be applied cheaply for as long as is required to break them (Goodin, Anatomy of a hack: How crackers ransack passwords like "qeadzcwrsfxv1331", 2013).

Once you use a Password Manager, ensure you have 2FA enabled for it.

7. OWASP (Open Web Application Security Project)

This is a resource created by information security professionals for Website Developers. Their top 10 list of attack vectors should be required reading for any developer building a website. It is much harder to build secure code than just having to build something which works, but is not necessarily secure. But developers with the knowledge of what not to do can make their lives significantly easier by following OWASP as closely as possible (Top 10 Vulnerabilities, 2013).

8. Website Security

A website, is a website, is a website, right? Well, no. Over time the encryption strategies that protect websites change. For instance: https:// links used to be secured via SSL v1, then v2, then v3. Nowadays SSLv3 is deemed too insecure for use and you need to move to TLS v1.2 and above. There are a myriad of Websites which still support SSLv3—sometimes because older desktops do not support the newer schemes, but generally from inertia.

9. Vendors

Talk to security vendors; there are some really interesting solutions which learn what normal traffic looks like on your network and will then alert you if something odd happens. Intrusion Detection and Protection Systems are a godsend for larger firms.

Conclusion(s)

It used to be that the vast majority of companies did not see themselves as IT companies. This included companies such as Telstra in the 1990s—I was there! Over the years, this attitude has become more and more unhelpful as pretty much every company needs to consider their IT first and foremost if they want to disrupt their competition and grow accordingly as GlobalX's recent paper on Workflow demonstrates. Not having the skills in-house to manage IT to the appropriate level will limit your ability to prepare and react when required; this is not to say that outsourcing doesn't have a place, but it needs to be managed as part of your overall strategy and not just pushed out to make it someone else's responsibility.

Each of the issues mentioned here have ways to mitigate them; but in essence, without someone in your organisation who is reviewing the threat landscape on a weekly or daily basis, deciding what needs to happen in terms of mitigation (coaching, knowledge dissemination, platforms and systems) you will always be more vulnerable than those who plan ahead.

Given the size of the breaches and flow on business impacts when the customer notifications go public, can you afford not to?

And watch Mr. Robot. It is an entirely accurate look at the current threat landscape out there!

About the Author

David is Manager of Information Technology at GlobalX. With over 15 years' experience in the Telecommunications sector, David has held numerous roles including in Development, Business Analysis, Project Management and IT Management. David has worked for numerous companies including Optus, Telstra and British Telecom. David has a degree in Computer Science graduating with honours from the University of Sussex.

About GlobalX

GlobalX is an Australian organisation that develops and supports integrated productivity software solutions and services used by thousands of conveyancers, law firms and businesses. Each day, thousands of professionals rely on GlobalX's suite of market-leading solutions to make profitable decisions and effectively manage their property and legal matters in a way that allows them to do more, in less time—and to do it better than their competitors.

The GlobalX Solutions Suite: GlobalX offers four core complementary solutions: GlobalX Search, Open Practice, Matter Centre and GlobalX Conveyancing & Legal Support Services, in addition to related support and professional services to offer legal professionals a single, comprehensive source of quality business solutions.

Visit: globalx.com.au

Works Cited

Chirgwin, R. (2016, Nov 13). *Your body reveals your password by interfering with WiFi*. Retrieved from The Register: http://www.theregister.co.uk/2016/11/13/researchers_point_finger_at_handy_smartphone_exploit/

Dede, D. (2010, Oct). *NASA Web Site hacked and serving malware/spam*. Retrieved from NASA: https://blog.sucuri.net/2010/10/nasa-web-site-hacked-and-serving-malwarespam.html

Dockrill, P. (2015, Oct 29). *Wi-Fi signals can identify you through walls and even track your movements.* Retrieved from Science Alert: http://www.sciencealert.com/wi-fi-signals-can-identify-you-through-walls-and-even-track-your-movements

Ducklin, P. (2013, Dec 9). *Serious Security: Google finds fake but trusted SSL certificates for its domains, made in France.* Retrieved from Naked Security by Sophos: https://nakedsecurity.sophos.com/2013/12/09/serious-security-google-finds-fake-but-trusted-ssl-certificates-for-its-domains-made-in-france/

Fitzpatrick, J. (2010, Oct 25). *Firesheep Sniffs Out Facebook and Other User Credentials on Wi-Fi Hotspots.* Retrieved from Life Hacker: http://lifehacker.com/5672313/sniff-out-user-credentials-at-wi-fi-hotspots-with-firesheep

Goodin, D. (2013, May 28). *Anatomy of a hack: How crackers ransack passwords like "qeadzcwrsfxv1331"*. Retrieved from Ars Technica: http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/

Goodin, D. (2015, Aug 5). *DRAM Bitflipping exploit for attacking PCs: Just add JavaScript.* Retrieved from Ars Technica: http://arstechnica.com/security/2015/08/dram-bitflipping-exploit-for-attacking-pcs-just-add-javascript/

Goodin, D. (2016, Nov 8). *Google stops AdSense attack that forced banking trojan on Android phones.* Retrieved from Ars Technica: http://arstechnica.com/security/2016/11/google-stops-adsense-attack-that-forced-banking-trojan-on-android-phones/

Gordon, W. (2014, Nov 14). *How to Stay Safe on Public Wi-Fi Networks.* Retrieved from Life Hacker: http://lifehacker.com/5576927/how-to-stay-safe-on-public-wi-fi-networks

Hern, A. (2016, Aug 6). *NSA denies 'Raiders of the Lost Ark' stockpile of security vulnerabilities.* Retrieved from The Guardian: https://www.theguardian.com/technology/2016/aug/06/nsa-zero-days-stockpile-security-vulnerability-defcon

Khandelwal, S. (2015, Aug 12`). *Lenovo Caught Using Rootkit to Secretly Install Unremovable Software.* Retrieved from The Hacker News: http://thehackernews.com/2015/08/lenovo-rootkit-malware.html

Krebs, B. (2016, Aug 15). *$1.2b lost to business email scams.* Retrieved from Krebs on Security: http://krebsonsecurity.com/2015/08/fbi-1-2b-lost-to-business-email-scams/#more-32154

Krebs, B. (2016, Sep 8). *Israeli Online Attack Service 'vDOS' Earned $600,000 in Two Years.* Retrieved from Krebs on Security: https://krebsonsecurity.com/2016/09/israeli-online-attack-service-vdos-earned-600000-in-two-years/

Krebs, B. (2016, Sep 21). *Krebs On Security Hit With Record DDOS.* Retrieved from Krebs on Security: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

Krebs, B. (2016, Nov 16). *Russian 'Dukes' of Hackers Pounce on Trump Win.* Retrieved from Krebs on Security: https://krebsonsecurity.com/2016/11/russian-dukes-of-hackers-pounce-on-trump-win/

Kushner, D. (2013, Feb 26). *The Real Story of Stuxnet.* Retrieved from IEEE: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Maney, K. (2002, Jan 17). *Microsoft shifts its focus to security.* Retrieved from USA Today: http://usatoday30.usatoday.com/tech/news/2002/01/16/microsoft.htm

Nichols, S. (2016, Mar 10). *Flash—aaah-aarrgh! Patch now as hackers exploit fresh holes.* Retrieved from The Register:
http://www.theregister.co.uk/2016/03/10/adobe_flash_march_updates/

Password Strength. (n.d.). Retrieved from XKCD:
https://xkcd.com/936/

Pauli, D. (2015, Mar 26). *Chrome trumps all comers in reported vulnerabilities.* Retrieved from The Register:
http://www.theregister.co.uk/2015/03/26/chrome_trumps_all_in_reported_vulnerabilities/

Plesser, B. (2014, Feb 5). *Skilled Cheap Russian Hackers Power American Cybercrime*. Retrieved from NBC News:
http://www.nbcnews.com/news/world/skilled-cheap-russian-hackers-power-american-cybercrime-n22371

Regnier, P. (2014, Aug 6). *A Billion Passwords Have Been Stolen. Here's What to Do Now.* Retrieved from Time:
http://time.com/money/3086151/russian-password-hackers-heres-what-to-do-now/

Rootkit. (n.d.). Retrieved from
https://en.wikipedia.org/wiki/Rootkit

Secunia Vulnerability Review. (2014, Mar 14). *Microsoft continues to focus on security in their products.* Retrieved from Help Net Security:
https://www.helpnetsecurity.com/2013/03/14/microsoft-continues-to-focus-on-security-in-their-products/

Simonite, T. (2016, Feb 16). *Hospital Forced Bas to Pre-computer Age.* Retrieved from MIT Technology Review:
https://www.technologyreview.com/s/600817/hospital-forced-back-to-pre-computer-era-shows-the-power-of-ransomware/

Szczys, M. (2012, June 12). *25 GPUs brute force 348 billion hashes per second to crack your passwords.* Retrieved from Hack a Day:
http://hackaday.com/2012/12/06/25-gpus-brute-force-348-billion-hashes-per-second-to-crack-your-passwords/

Top 10 Vulnerabilities. (2013). Retrieved from OWASP.
https://www.owasp.org/index.php/Top_10_2013-Top_10

Waddell, K. (2016, Jun 9). *How to Run a Russian Hacking Ring.* Retrieved from The Atlantic:
http://www.theatlantic.com/technology/archive/2016/06/the-ragtag-russian-hackers-taking-computers-ransom/486404/