HACKING AND COUNTERHACKING: TRENDS AND TECHNOLOGIES FOR PERSONAL AND ORGANIZATIONAL INFORMATION SECURITY

Sreekanth Malladi, Ph.D.
Saint Leo University

Abstract

The landscape of IT computing has been changing continuously over the last two decades. Recent trend has been toward big data on cloud storage being accessed by numerous apps on countless mobile devices. The shifting landscape introduces new threats to IT security, the most impactful being “hacking”. In this paper, we present a survey of the latest trends and technologies used by hackers to attack individuals and businesses. We also present best practices to counter hacking both for individuals and businesses.

1. Introduction

Information Technology (IT) is the technology used to store, process and transmit information. It started with the use of stand-alone computers in the 80’s, followed by networks of machines in the early 90’s, Internet in the late 90’s, and client-server architecture for e-commerce in the early parts of the 21st century. Lately, the trend is shifting toward using cloud and mobile computing. The data being handled is massive, and there is an explosion in the number of devices being used due to advances in mobile computing. Software that is used for these is raging with hundreds of new apps being released every day.

But with this changing landscape of computing, the landscape of threats is also changing. Correspondingly, countermeasures against threats must also change. Not doing so has shown severe losses to companies relying heavily on IT over the last two years: Target, Home Depot, JP Morgan, and Staples to mention a few that we know of.

We have researched these issues, and analyzed the current trends for threats faced by individuals and businesses who depend on IT on a daily basis. Hacking, which is the deliberate abuse of any aspect of computing was found to be the biggest threat, accounting for most losses to businesses (Symantec, 2014).

We have investigated deeper into hacking with the aim of understanding the changes in the trends and techniques related to hacking. We have also analyzed the changes to IT that people have to make to their usage of IT in order to have strong protection against hacking. We describe our findings in this paper. We give an update on attack vectors used for hacking. We also suggest countermeasures to hacking (aka. counterhacking) that improves security of information for individuals and businesses.

Organization. The rest of the paper is organized as follows. In Section 2, we present an overview of the changing trends in Information Technology (IT). In Section 3, we discuss the changing trends in threats to IT, in particular, hacking. In Section 4, we present countermeasures against hacking. We sum up with a Conclusion.
2. Background – Changes in IT landscape

Since the advent of computers, IT has been ever changing. It started with isolated machines being used to store and process data. In the late 80’s and early 90’s, networking of machines was the revolution in computing. It was followed by the introduction of Internet, connecting computers globally and allowing for e-commerce in the client-server model on the world-wide-web.

Since the early years of this century, there have been drastic changes to networks, systems, and software:

1. The amount of data involved is enormous in comparison to previous generations (leading to the term “big data”);
2. Client-server model was changed in many places to the so-called “cloud computing” model where data, services, platforms and even infrastructure is being stored and accessed remotely;
3. Systems or machines have seen exponential growth in numbers, especially with the advent of mobile devices and BYOD environments;
4. The changes to systems and networks has caused software (or apps) to increase both in type and number.

3. Changes to the threat landscape and hacking

3.1 General trends

The next step is to assess how exactly the usage landscape has changed the threat landscape. Data breaches are continuously on the rise: In 2012, there were 93 million identify thefts, but in 2013 they shot to 552 million, as can be seen in the figure below obtained from a report by (Symantec, 2014):

While there are many threats to information such as natural disasters, theft, accidental loss etc., hacking seems clearly the biggest threat. In fact, (Symantec, 2014) mentions that hacking has accounted for 53% of all 259 reported data breaches against organizations:
As big a threat as it is, individuals are being lot less targeted by hackers compared to businesses. As Cormac Harley observes, targeting individuals is not a rewarding effort for hackers (J. Bonneau, 2012). For instance, each credit card number is worth about 7 cents in the market for resale. Hence, it would take at least thousands of credit cards breached at once, to make the effort worthwhile. Hackers are preferring to use softer techniques such as phishing (Nigerian scam, London scam etc.) to attract potential individuals (or victims) to exploit their innocence later and obtain some money. Such techniques are easily scalable to millions of targets at very little increase in expense.

Some general observations we have made about hacking organizations:

a) Organizations are being targeted for the most part for making profit out of stolen data, credit card data being the most common (Target, Home Depot, JPMC etc.).

b) Non-profit and governmental organizations are also being targeted for espionage, terrorism, and hactivism, where monetary gain is not the real motive (e.g. dragonfly attacks). Some nations also seem to be sponsoring hacking; at the least, they do not have laws to punish or prosecute those who hack into organizations in other countries (Symantec, 2014) (Camejo, 2014).

c) Attacks on organizations are emanating mostly from overseas, with Russia and China accounting for most successful and impactful attacks (Microsoft, 2014) (Camejo, 2014).

d) While everyone is at risk of getting hacked, perhaps obviously, organizations with the weakest protection measures are at most risk, and seem to be hackers’ primary targets, since they offer the path of least resistance. Also, even with strong protection measures, those that partner with others that may not have good measures are lending themselves vulnerable (e.g. Target breach). This is probably why cloud providers such as gdrive, dropbox, skydrive etc. are not reporting breaches, since they employ very good security practices and also do not partner with others unlike e-commerce sites that must partner with financial institutions. However, this is not to be taken for granted, since connections to cloud providers are secure only when routing security, both internally and externally is ensured (Camejo, 2014): Internally, ARP poisoning could be used to divert people from connecting to the legitimate cloud servers. Externally, Internet routing tables could be poisoned for the same effect.

3.2 Trends in attack vectors/techniques
As mentioned before, when it comes to techniques for hacking individuals, social engineering is the preferred choice. But with changes to mobile technologies, especially with the introduction of smartphones, users are now open to a range of new hacking techniques. The biggest threat to mobile computing is the loss of privacy. With apps trying to access more information than they need to, and with users willingly providing information about themselves through different ways like social networking, they are now exposed to more ways of losing their privacy. Although hackers are not preferring to target individuals since it is not very rewarding usually, if they can obtain information about a large set of individuals, they can use it for many purposes including selling the information online (Johnson, 2014). Imagine if information about a family’s work, routine, habits etc. is available to a child molester. *Ransomware*, which is a particular type of malware that asks users to deposit money into a paypal account at the nearest gas station has been a popular technique. It comes in both the genuine and fake variations. In the genuine variation, hackers lock up the phone using their own password and any apps such as findmyphone app on iphone. They then ask the individual for ransom to unlock. The fake version is just a pretense of the same. For instance, a common approach has been to claim on the browser tab that the FBI is monitoring their machine and that they would let them go if they paid a ransom.

As far as organizations go, there have been no major changes to attack vectors. The biggest change has been in remote code execution. Until a few years back, exploiting regular, benign code such as web servers, ftp, rpc services etc. was the common technique (e.g. SSL HeartBleed, “shell shock”¹). The idea was to look for vulnerabilities in network services where one could cause a buffer overflow in one of the array data structures used which would allow attacker’s code to be executed with the same access permissions as the network service.

However, possibly with the more careful design of network software, and better security of the system and environment within which they operate, this technique has not been reported as being still used by hackers. Another reason could also be that it is not cost-effective for hackers to analyze software, the underlying code for which is often not available. Hence, they are resorting to an easier approach: to inject malware such as “Kaptoxa”² into networks with the help of soft techniques such as social engineering (e.g. attaching malware to phishing emails). This is not only easier but also scalable, since it allows hackers to inject the malware into many targets in a single shot. This type of malware is called “Trojan software” or simply “Trojans”. No wonder why malware and in particular Trojans are now considered as the greatest danger to information of all hacking techniques, as shown in the recent statistic provided by Microsoft’s Threat Intelligence Report (Microsoft, 2014):

² “Kaptoxa” was used in both Target and Home Depot breaches as reported by [http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/](http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/) to syphon credit card data.
These ideas can be best described by the following figures. Consider the following figure describing a typical organization’s structure of technology and people as to their proximity to data:

The one below shows the path that the hackers were taking previously. Here, the attacker first scans the Internet for potential target networks. Then, he analyzes the network for accessible systems that could be connected to via vulnerable services. Finally, he launches an attack such as a buffer overflow on the vulnerable service, execute his own code with the same permissions as the vulnerable service. He could craft his code to do things such as creating an administrator account, email the password file, change critical data etc. More significantly, he can start a network service in one of the internal machines and then connect to it from his location as a client. Such inbound connections can be filtered by a firewall, though in some cases, techniques have been used to evade filtering as well.
Currently, hackers have changed their technique a bit (Camejo, 2014) (Murray, 2014). They are choosing their first point of entry as vulnerable (or corrupt) employees who are willing to do things such as opening attachments in phishing emails. If that allows them to plant malware in a vulnerable machine, they can then use it as a “hook” into the company and explore more machines that they could “own”. In the process, they look for older machines that are still hooked up but ignored by everyone and left unpatched (for years sometimes). They also look for servers with weak passwords. Since they now have a hook into the network, it is easier to hack into machines that have better security than the initially exploited machine and invisible outside the organizational network. This process is illustrated in the figure below:
A very important aspect of this new style of hacking is that the hacker’s code is now a client that connects to the remote server maintained by the hacker. Hence, it is not sufficient to filter inbound traffic. Outbound traffic must also be filtered.

4. Countermeasures for hacking – Counterhacking

It is now time to look at countermeasures for hacking or simply “counterhacking”. Once again, we will start with individual security and then organizational security. Some aspects are overlapping, in the sense that some techniques for security are much similar. Also, individuals also work for organizations and protecting themselves is crucial for organizational security.

4.1 Counterhacking for individuals

We will give some general advises for improving individual security. These are not all encompassing, in the sense of transforming someone into being perfectly secure, but cover the important aspects to ensuring good protection. We will categorize them into networks, systems, apps etc.

4.1.1 Networks

When connecting to network services such as http, ftp, smtp etc. it is advised to always use encrypted, authenticated sessions using TLS. Its predecessor, SSL is better than unencrypted communication, but reportedly not as good as TLS (Turner, 2014).

It is also advised to always use a firewall that limits inbound traffic. Although firewalls that filter outbound traffic as well are better, it is usually not necessary for individuals, because of the limited amount of sensitive data, expense and reduction in speed of the communications. Also for the same reasons, either a built-in or a freeware firewall usually offers adequate protection (e.g. Avast).

4.1.2 Systems

Unpatched systems are one of the most vulnerable and commonly targeted by hackers. It is important to patch systems regularly with manufacturer released updates. Further, for Windows owners, Microsoft recommends that it is important for them to use Microsoft updates, not Windows updates, since the former updates all Microsoft software including Windows (Microsoft, 2014).

With mobile devices, the first and biggest decision is, which device to purchase? While Android is undoubtedly the most popularly used, it is also the least secure, possibly due to its popularity. There, the trade-off is between security and personal preference. Blackberry seems highly secure with very few incidents reported, most likely due to its low consumer preference (Johnson, 2014).

4.1.3 Apps

Security precautions against vulnerable apps and malicious apps are recommended. To be protected against vulnerable apps, it is recommended to install only apps from reputed and trustworthy companies. Further, they must be patched and repaired whenever they need to be (e.g. MS updates). They should be first checked with a good anti-virus software to detect Trojans or other hidden malware. A good anti-virus will also protect against malware downloaded from web sites or emails. The term anti-virus is actually a misnomer, since most people use the term “virus” to mean “malware”. Also, many are unaware that inexpensive yet effective antivirus are available for mobile devices as well from many including AVG, AVAST etc.
4.1.4 Data

Individuals usually store lot lesser sensitive information about themselves, whose breach can cause financial losses. However, with attacks such as Ransomware, it is recommended that important data such as personal pictures and documents be stored on an external hard drive and backed up often. Cloud storage could be used in addition, for data whose secrecy is not crucial. It could also be combined with an external hard drive (Symantec, 2014).

4.1.5 Social engineering

It is important to be safe against social engineering is important both from a personal perspective and potential impact to an organization that the person might be working for. It is advised not to open or worse yet, download attachments from unsolicited and/or untrustworthy sources. Further, people should be cautious against attempts such as fake Ransomware (e.g. “FBI SURVEILLANCE” threats). In most cases, a response should be avoided.

4.1.6 Passwords

It was surmised by many around 2000-2004 that with advances in computing, the dependence of passwords will decrease. However, it has been noted that the dependence is actually increasing. Though passwords are the easiest authenticators for people to “carry”, the requirements of uniqueness and complexity make it uneasy for people to use them as well. This is an issue with no magic bullet, but at this time, it seems that an easy way to ensure uniqueness and complexity is by choosing a common string as the base for all passwords but including a site’s characteristics (name etc.) to it for obtaining different passwords.

4.2 Counterhacking for organizations

4.2.1 Defense in depth

The classical technique of a layered defense methodology is still widely recommended for organizational security. From a technical standpoint, this involves the use of multiple security solutions such as firewalls, antivirus, IDPS, spam filters etc.

4.2.2 Security solutions

A major change in firewalls over the last few years is that most organizations are filtering outbound connections as well, not just inbound. This is important, since hackers are now having the internal machines connect to them as clients to machines operating as servers at the hackers’ end.

Using commercial antivirus is strongly recommended, due to their up-to-date maintenance of malware signatures, product support and publication of benchmarks for comparison with other antivirus tools. A major change in antivirus products has been that they now analyze not just signatures of malware code, but also other characteristics such as their size, victim OS, download speed etc. (Symantec, 2014).

It has also been recommended that “combo packages” where the packages include a set of security tools, for example a firewall, IDPS, antivirus, web security combined into one are not advisable. This allows hackers to know the characteristics of the package since they are from the same manufacturer, (according to a CISO, whose identity we are unable to reveal here due to requirements to maintain
anonymity). Also, such packages are not as flexible or scalable as independent products. On the other hand, packages may have lesser maintenance and smoother operation, so they might be suitable for smaller organizations.

4.2.3 Penetration testing

Regular penetration testing of networks is recommended. Consultants are available who can be hired to conduct expert penetration tests and submit detailed reports of vulnerabilities. Most of them can operate remotely, even from other countries! Pondurance is such a company. They described a presentation where they have caught a live hacking attempt from someone in China on a company based out of Mexico City, by testing it from the US (J. Henderson, 2014).

4.2.4 Legal issues

Note that compliance with legal requirements is often thought by organizations as sufficient protection. However, it has been pointed out by many CISOs as adequate only for “legal sufficiency”, but not security (Pete Lindstrom, 2014). Therefore, organizations must have a strong defense in depth program as well as a rigorous audit and awareness program.

As far as involvement of law enforcement is concerned, many are not aware that organizations have a right to non-disclosure for a reasonable time period even when they have been victims of hacking. It has been suggested that it is usually not advisable to contact law enforcement as a first step, since doing so will result in loss of control of data and property for the organization as well as opening it up to legal complications, especially if found non-compliant with required laws (Smolanoff, 2014).

5. Conclusion

In this paper, we have presented advances in the most dangerous threat to data in recent times, namely hacking and also approaches to counter it. We have particularly focused on changes in approaches to hacking and counterhacking over the last few years. We noted that while there have not been major changes to the attack vectors, the volume of existing methods such as malware is growing rapidly.

We would like to go over the important points briefly again: Following a business principle, hackers are targeting to prefer organizations, not individuals because of the higher cost-benefit. The biggest aspect of hacking has been malware. The major change to remote code exploitation is that hackers are using social engineering techniques to inject malware code into organizational networks and then using the machines as clients to servers that they maintain. Also, they are launching such attacks from overseas, not within the U.S, domestically, due to fear of prosecution. State-sponsored hacking and industrial espionage also have been on the rise which do not give any pecuniary gain.

Individuals have to be careful against social engineering like spam, have good data backup plans, choose strong & unique passwords and follow the principles that we recommended for security the privacy on their mobile devices.

Defense-in-depth approach is still widely recommended as the best protection approach for organizations. Firewalls filtering outbound traffic is a major change in security solutions. A strong audit and awareness program is crucial to ensure security against social engineering attacks, which is often the first step in hacking.
There is no end-product for efforts to improve security for it is a process; a perpetual cat & mouse play. With the ever growing varieties and quantity of devices and software, the techniques and tools for hacking are bound to increase. Therefore, a strong strategy for counterhacking is vital for organizations. We hope that this paper presents a good overview of where hacking and counterhacking stand currently.

References


