

Cyber-Attacks Pattern, Statistics and Remediation

Bajjuri Avinash Reddy¹ Santosh P Korupolu² Rithvik Gosukonda³

^{1,3}Department of Cyber security ²Department of Electrical and Computer Engineering

^{1,3}University of Maryland ²University of Alabama at Birmingham

Abstract— Cyber-attacks landscape is changing rapidly due to exponentially increasing cybercrime every year. In the last few years we have been seeing the unprecedented increase in internet usage because of economically and easily available smartphones that are almost always connected to internet. and because of advent of IoT (Internet of Things). These smart phones and mobile devices provide an ease of access to social networking sites, online transactions, cloud computing platforms, and automated processes (IoT) with the help of respective applications. But with the ease of access and technological evolution comes the progress of cybercrime, which continually develops new attack types, tools and techniques that allow attackers to penetrate very well engineered infrastructure and cause damage, but still remain untraceable. Information security has always been a zero-sum game i.e., the easier it is to use, the harder it is to defend it against the attacks, the harder it is to use the easier it is to defend it from the attacks. This article aims to give an overview of the cyber- crime, its' patterns, statistics and remediation techniques based on patterns and trends in cyber-attacks in last few years. Based on the extensive study, this article presents remediation techniques that companies may undertake to ensure improved security, thereby defending their business from attacks (from information security viewpoint).

Key words: Cyber-Attacks

I. INTRODUCTION

There is no exaggeration in saying that today's world is run by big data, social networks, online transactions, cloud computing, cloud storage and automated processes performed through the use of IoT systems. In this data driven world, information is worshiped. In such world information security and data privacy are continuously facing risks. With the development of new and sophisticated tools and techniques, cyber-attacks are consistently increasing and are also causing more damage than ever before. Attackers are continuously trying to gain unauthorized access to networks, servers, software's etc., by using the bugs that are already available in the network by analyzing and targeting the individual or entity with the intention to compromise the confidentiality, integrity and availability of information, building their targets from single individuals to small or medium sized companies and even business giants. Every year we say that this year we have seen a very high raise in the cyber-attacks, while that is a fact, we have to realize that each coming year we will be awaiting bigger and more sophisticated cyber-attacks. With the rapid integration majority of electronic devices into IOT and growing usage of smart phones among people with minimal or no knowledge of cybersecurity will pose a bigger threat for information security because these devices are the soft targets for a hacker to create a botnet, which is used for Ddos attacks that will hurt information security, business continuity and data availability of the victim. This

trend of Ddos and ransomware attacks has reached new heights in 2015 to 2018. This purpose of this article is to reveal the results, patterns, statistics and remediation techniques noted through the analysis of the attacks by various organizations, and to present remediations that should be considered for improvement of security and the decrease of world-wide cyber-crime. This article reveals the many results and statistics of the extensive study on attacks reported over last few years by various organizations. It ends by quoting some of the precautions and best practices that companies may take in order to ensure improvement of controls covering the information security or cyber security and also decrease the security breaches.

II. LITERATURE REVIEW

We can't shy away from the fact that Cyber- attacks are real and are sitting right at our front door and one can be a victim anytime if they are not careful enough. While more development work and vulnerability/ bugfix efforts are being put in operating system or software provider, more sophisticated attacks are being engineered everyday by the attacker to intrude and gain unauthorized access to the data, yet little is universally known about cyber-attacks. According to study done by Symantec, there is a generally lack of understanding of the different types of attacks, characteristics and possible results, which may pose an obstacle in trying to defend the information security.

Over the past few years we have been observing more sophisticated and progressively engineered techniques like "Man in the middle attack, Brute force attack, DDoS (Distributed Denial of Service), Malware (viruses, worms, trojans, spyware, ransomware, adware and rouge-ware), Phishing, Social engineering to name a few. If an attack is performed by integrating two or three attack techniques commonly termed as "hybrid attack" generally used in target attacks, defending your infra is a very challenging task. However, traditional attacks remain as the most common type of attacks faced by organizations. If one can understand the various stages of an attack, defending against them will be a little easier than not, below are the stages of an attack:

A. Reconnaissance:

In this stage attacker selects the target and determines the vulnerabilities of the target and gets his ammunition ready. In most of the cases the ammunition for the attack is phishing email (spear phishing) to spread the malware.

B. Scanning:

After identifying the target, the hacker scans the network to identify the soft spots that would enable them to obtain access. In this stage attacker might use common tools available on the internet or customized or more enhanced self-designed tools to scan the targets network to find the

soft spots. In some cases, it might take months to scan for vulnerabilities.

C. Take control:

The intent of an attack is usually to secure access to resources, from finances to sensitive information. Tools like Rainbow Tables, key stroke logger allows hackers to take credentials and infiltrate any system that the administrator account has access to. Once the hackers have seized elevated privileges, they can take control of the network.

D. Maintain Access:

The next step for the invaders is to ensure control over the network is maintained for the amount of time needed to fulfil their tasks. At this point, the hackers have overcome various security controls, but are more likely to be discovered. Intrusion and extrusion detection methods include moving content to external sites and internal devices; thwarting initiation between data centre servers and networks; finding connections to nonstandard protocols; and noticing abnormal network or server operations.

E. Assault:

The assault phase doesn't occur in all cyber-attacks. Hackers might resort to modifying or disabling a user's hardware. Unfortunately, even if the intruder is discovered by the victim at this stage of the game, it's too late since they have control of the network.

F. Obfuscation:

It might seem appropriate to hide one's fingerprints following a crime, but hackers aren't exactly doing the same. Some intruders will leave a mark behind as a staple claiming authorship of the stunt to gain fame or to confuse the forensic examination process. Many trail techniques are used including log cleaners, zombified accounts and Trojan commands, to name a few.

Detecting threats early as they occur in real time is essential for shielding a network from cyber-attack. With the noted list in hand, network operators can recognize when a system is being breached and take the necessary steps to keep intruders at bay. But statistics says that battling the attacks is not a success because according to a report by FireEye and Mandiant, approximately 97% of organizations have had at least one hacker bypass their defence architecture. According to Microsoft an attacker resides in a network for an average of 146 days before detection or becoming active, also McAfee says that the average of 780,000 records were lost to hacking in 2017.

III. RESEARCH METHODOLOGY

This attentive review of cyber-attacks pattern and statistics is done by reviewing the specialized international literature, forums and analysis of the last few years major cyber-attacks. The agenda was to provide an overview of the cyber-attacks happening around the world, understand the means of operating and to study the impact of these attacks on businesses or individuals, as well as the remediation techniques to be taken as for prevent these attacks or in worst case to provide you with a contingency plan. The research was based on attacks identified and traced among

the last few years. Given the huge number of cyber-attacks that happen around the world on daily basis, as well as the limited information companies usually display when they are the victim of such attacks and the fact that some attacks are hard to be traced, it is impossible to provide complete or vivid picture of these attacks. However, the study was based on the information resulted from aggregating data regarding attacks detected and traced in the last few years, collected from news and attacks history, as well as from reports and surveys issued by globally major market players such as anti-malware vendors, various news and events, as well as events reported by major players in the industry of security and consulting: Cenzic,

CISCO, FireEye, Kaspersky, McAfee, RSA Mandiant, Sophos, Symantec, Verizon, comparitech.com, forbes.com, rcrwireless.com, blog.netwrix.com, it-pro.co.uk and hackmageddon.com.

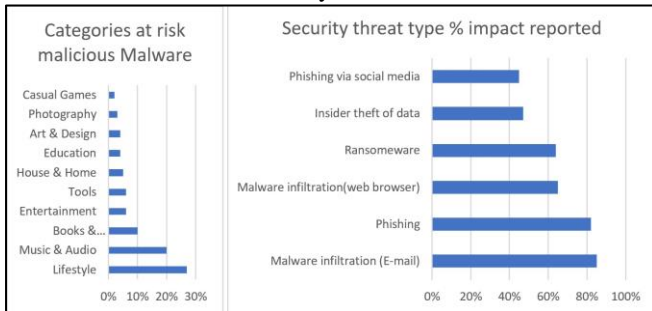
IV. RESULTS

The results produced are based attentive study done from articles from various news and events, as well as events reported by major players in the industry of security and consulting: Cenzic, CISCO, FireEye, Kaspersky, McAfee, RSA Mandiant, Sophos, Symantec, Verizon, comparitech.com, forbes.com, rcrwireless.com, blog.netwrix.com, it-pro.co.uk and hackmageddon.com.

A. General Results

McAfee Labs' report, Symantec year in review of 2017, shows the clear increase in various types of cyber-attacks, these analysis also strongly supports the idea that cyber-attack will increase exponentially and also assumes that world will see more sophisticated attacks on a large scale, these revelations shows the strength of hackers network and development, improved strategies and tools for hiding their identity/location and obtain sensitive data. According to the report from Symantec, 'Attacks on Internet of Things devices increased by 600% from year 2016 to 2017, this can be due to hypergrowth in the number of devices connected to IoT, poor security hygiene, and high value data available on IoT devices. One other trend that has been noticed is the rampant increase of mobile attacks, which can be due to widespread usage of mobile phone usage among people with minimal or no knowledge of security. Our study has found that there is 54% increase in mobile malware variants from 2016 to 2017. In fact, Internet Security Threat Report details the number of new mobile malware* variants rose from 17,214 in 2016, to 26,579 in 2017 – a 54% change. It looks like the hidden ideology is "you need not compromise the software if you own it". Out of all the malicious applications blocked on android and IOS platforms, below bar chart represents the category wise risk of malicious malware infection. The results outline the fact that attackers continually develop new ways to exploit networks, programs and data. Statistically, 2017 was a banner year for ransomware and 2018 running strong to become a banner year for crypto mining. According to the report, business and consumer ransomware detections have increased 90% and 93% respectively, largely because of families like WannaCry, Locky, Cerber and Globeimposter. In fact, the

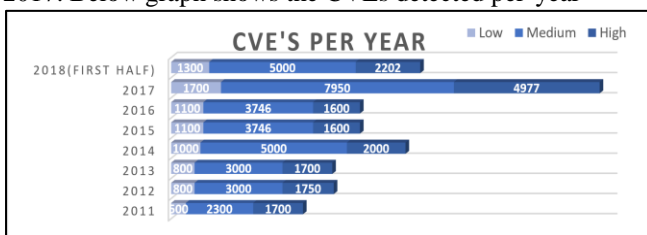
monthly rate of ransomware attacks against businesses increased up to 10 times the rate of 2016 and overall 700% increase in 2017 from 2016. We have also highlighted the concerns from various security threats.



B. Main Drivers

An interesting fact that the study reveals is that, looking at the root-cause of the security breaches and cyber-attacks, the causes of these attacks are mostly because of the human error and the system vulnerabilities. The results outline the fact that a very low percent of attack succeeds because of attacker's skills and knowledge, and mostly because of vulnerabilities and human errors from the vic- tim's side – that is, faulty programs, insufficient level of controls to ensure information security.

In the Vulnerability report by skybox security, it is noted that there is huge spike in the number of CVEs (Common Vulnerabilities and Exposures) published. A total of 14,646 new CVE's were published by the end of 2017 representing a 127% jump over the previous year. This spike was due, in part, to increased resources in the MITRE organization and the National Vulnerability Database (NVD) which publishes CVEs, as well as an increase in vendor and third-party vulnerability research. Also, 2018 shows no sign of slowing down. At the end of June, 8,502 CVEs had been published by NVD since the beginning of the year, already exceeding figures for all of 2016 and putting 2018 on track to exceed the record-breaking stats of 2017. Below graph shows the CVEs detected per year

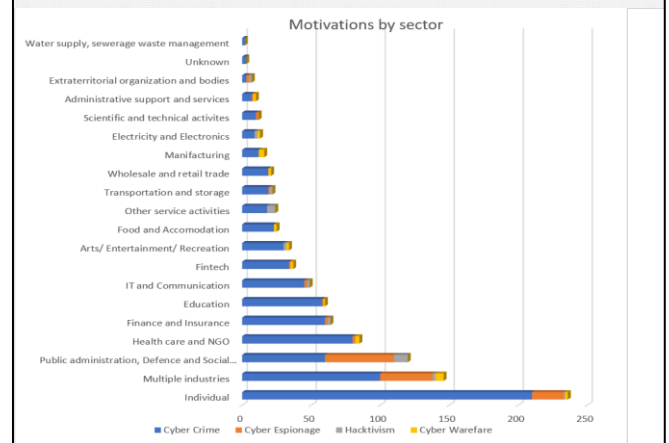
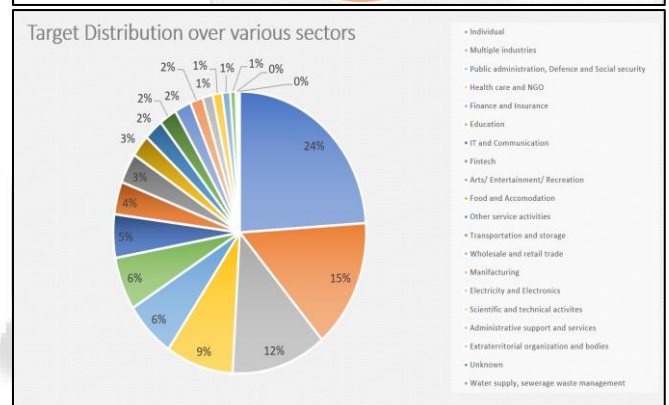
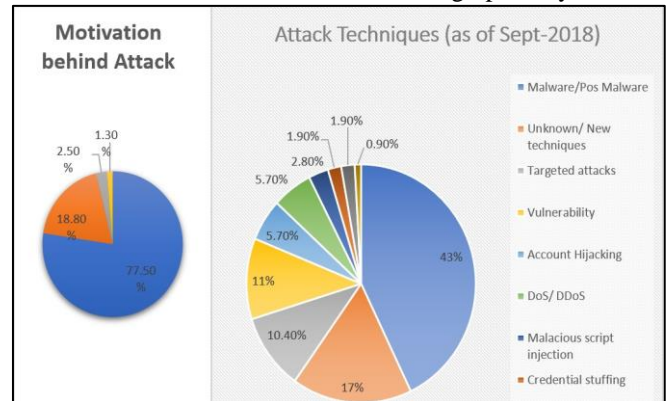


C. Distribution of These Attacks over Various Sectors

It is hard to determine the exact number or percentage of different types of attacks a rough figure is ascertained. The most common attacks are Malware attacks, targeted attacks, Vulnerability leveraged attacks, account hijacking, DoS/ DDoS, malicious script injection, credential stuffing, misconfiguration, defacement, phishing and Social engineering. Nevertheless, the results could easily be split into four categories, depending on the objective of the attack: cyber-crime, cyber espionage, cyber war and hacktivism.

The study revealed the fact that companies of various sizes and business sectors have been the victims of

cyberattacks in the last few years. Regardless of the entity's size, all areas, from the public sector and NPO's NGO's to private companies in Finance, Media, Online services, Tourism, Telco, Retail, Education, Automotive, Security, Energy & Utilities, Food & Beverage, Internet and online services domains are targeted by cyber-attackers. In geographical perspective the study focused from to points: the geographical origin of the attacks, as well as the destination. The results are shown below graphically:



D. Correlation and Revelation of the study

The study revealed interesting pattern, which is relative correlation between the business sector and the types of attacks, i.e., cyber espionage is most likely aiming Government, Media and Law Enforcement sectors, and quite unlikely targeting other business sectors. The results for the last few years outline a relatively strong correlation between the types of attacks and industries. The correlation shows that while the public sector is the most likely target of cyber espionage, cyber war and hacktivism techniques,

while cyber-crime targets all business sectors. The results also show that attacks are not totally due to outside hackers, but are also due to current or former employees, management, etc. While Ransomware has taken center stage in 2017, coin-mining has taken center stage in 2018, also Ransomware has lost its ground in 2018, but mobile attacks are becoming more rampant day by day, which we believe is natural considering the spread of smartphones globally, which might be an easy target due to almost permanent connection to the internet, use of applications for which entire access is provided in desperation to avail benefits of freely available applications, also these devices are barely switched off and contain a lot of personal information of not just that mobile user but also the information of all the contacts.

V. SECURITY BEST PRACTICES

Now a days, Government institutions like Secure Domain Foundation (SDF) or the International association of Cyber-Crime Prevention (IACP), most of the private organizations like Google, Microsoft etc., and educational institutions have formed teams to collectively fight against the cyber-attacks. These organizations are trying to make the public and other sector company aware of the cyber risks like how they can be exposed to the cybercrime, and how they can defend themselves against attacks. These organizations are putting together huge efforts to analyze bugs and vulnerabilities in their own as well as other companies' codes in order to take all necessary measures to improve the software products to mitigate cyber risks and vulnerabilities. Few organizations are organizing the events like "hack - if you can", bug bounty, Defcon etc., to proactively find the bugs and vulnerabilities in the applications or programs before the release.

The increasing trend of cyber-attacks has also motivated financial companies to launch an insurance product covering costs needed to recover after a cyber-attack events. In addition, these companies also launched a product dedicated to analysis, assess and support mitigate clients' cyber risks. One of the most essential aspect of cyber-crime and cyber security is the legal aspect. Laws and regulations are continuously developed to prevent or limit the cyber-attacks. However, the sensitivity of the subject is given by the fact that each set of laws and regulations are geographically limited to a certain region, in spite of the internet access being available internationally, connecting people from all around the world with no boundaries.

While there are lot of initiatives from public institutions, it is one's own responsibility to safeguard their own information and keep them away from cyber bullying. The most important thing that everyone has to understand is that "cyber security is not a destination but is a continuous/cyclic process that involves Plan -> prevent-> Detect -> Respond and repeat. Few of the measures that are defined by the best in the field to keep yourself or your organization away from the cyber-attacks are as follows:

- Continuous risk assessment.
- IT infra health assessment and redundancy planning.

- Complex Authentication techniques like strong password, password expiry and Two factor authentication.
- Organizations internal commitment and responsibility.
- Always follow minimal access strategy i.e., no one should be provided with access to information more than required.
- Data Retention (Data backup plan) should be planned by keeping in mind the revelation by Microsoft that malware stays in you network for an average of 146 days before being detected.
- Depending on the risks to be addressed, several controls may be implemented in order to ensure the confidentiality, integrity and availability of data like preventive controls, Detective controls, Corrective controls via change management system.
- Regular audits and certifications from approved bodies.
- Plan and implement relevant file level access using User Access Control (UAC)
- Regularly patch all the infrastructure devices including software programs
- If a zero-day vulnerability is discovered or revealed by any third party, make sure that the relevant patch is applied at the earliest up on release.

VI. CONCLUSION

As a saying goes "Good is not enough when better can be done and better is not enough when best can be done", there is always a great room for improvement in the world's fight against cyber-crime. It is clear that there is a generally lack of understanding regarding cyber security among public, Hence, the problem of increasing cyberattacks and cyber bullying is not easy to solve. The authors believe that the first thing to do in order to handle the problem of increasing cyber-crime is to spread awareness, from an individual level to corporate organizations of what lays in the cyber world. One other main obstacle is with the laws pertaining to cyber security across regions and countries, almost each country has its own set of laws and regulation governing the invasion of data privacy and theft, While internet is a need for everyone in today's world, it is an international platform for attackers, thus the only way to defeat the cyber-crime is for authorities to think and act at a global level, thus supporting the rights and safety of individuals and organizations around the world. Last but not least, it is the responsibility of each individual, company or authority to ensure a certain level of security, in order to support the information security and data privacy, as it is the right of every individual, company and service provider to decide what and how they retain, manage and with whom they share their data. While installing application on mobile devices, give only minimal permissions that are required for application to work, also report if the application is requesting for irrelevant access. Cyber laws should be periodically updated by closely following the evolution and trends of cyber-crime, as well as countermeasures, especially focusing on the universal awareness on cyber-crime and regulatory decisions and facts should by all means support the cyber-security.

REFERENCE

- [1] Cisco – Annual cybersecurity report 2018, detailed information available at (<https://www.cisco.com>) website visited on 7th-October-2018.
- [2] Cisco – Annual cybersecurity report 2017, detailed information available at (<https://www.cisco.com>) website visited on 10th-October-2018.
- [3] Symantec – Annual cybersecurity report 2017 detailed information at [http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7DISTR23 Main-FINAL-APR10.pdf?aid= elq](http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7DISTR23%20Main-FINAL-APR10.pdf?aid=elq) website visited on 10th-October-2018.
- [4] Skybox security more information at [https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox Report Vulnerability Threat Trends 2018 Mid-Year Update.pdf](https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_Vulnerability_Threat_Trends_2018_Mid-Year_Update.pdf) website visited on 21st-October-2018.
- [6] Hackmageddon.com more information available at (<https://www.hackmageddon.com>) website visited on 10th-December-2018.
- [7] Forbes security report -[https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/ #642580d048e3](https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/#642580d048e3) website visited on 10th December 2018.
- [8] Netwrix blog -<https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/> website visited on 7th-October-2018.
- [9] Uk Itpro blog - <https://www.conferencecall.co.uk/blog/what-are-the-different-levels-of-cyber-attack/&https://www.itpro.co.uk/security/29224/the-cyber-security-threat-in-charts> website visited on 7th-October-2018.
- [10] RSA report – detailed information available at <https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf> website visited on 15th-October-2018.
- [11] University of Maryland announcements – detailed information at <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds> website visited on 10th December 2018.