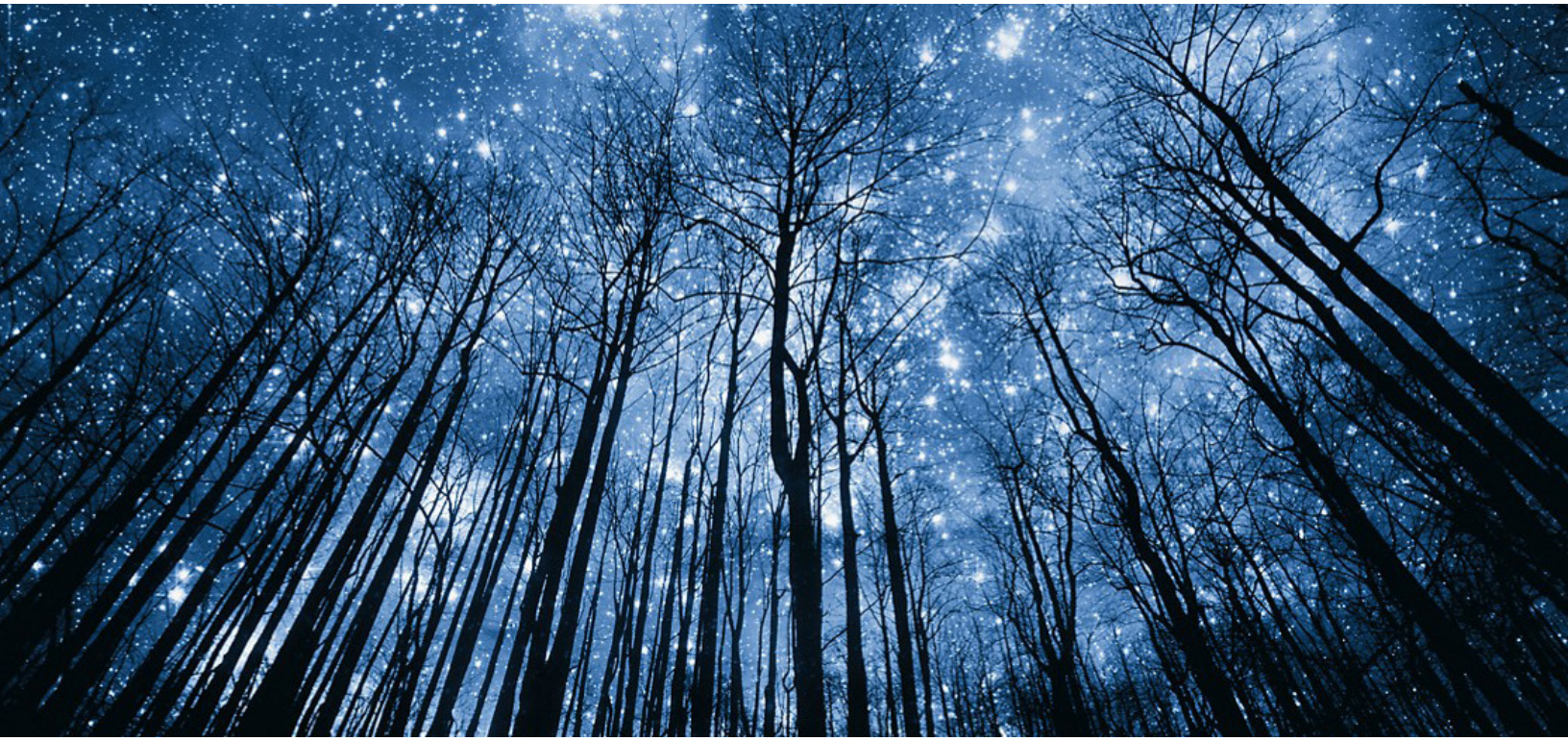
DELL Technologies

CYBERSECURITY: WHAT WE HAVE AND WHAT WE NEED



Ruthvik S J
Associate Sales Engineer Analyst
Dell Technologies

Urja Senani
Associate Sales Engineer Analyst
Dell Technologies

DELL Technologies
Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across Dell's multiple technologies and products with both skill and outcome-based certifications.

Proven Professional exams cover concepts and principles which enable professionals working in or looking to begin a career in IT. With training and certifications aligned to the rapidly changing IT landscape, learners can take full advantage of the essential skills and knowledge required to drive better business performance and foster more productive teams.

Proven Professional certifications include skills and solutions such as:

- Data Protection
- Converged and Hyperconverged Infrastructure
- Cloud and Elastic Cloud
- Networking
- Security
- Servers
- Storage
- …and so much more.

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Table of Contents

INTRODUCTION

History shows that there have been multiple cases of losses to financial institutions and individuals over the years due to cybercrime. Even the government and defense organizations have their fair share of significant amounts of cyber-attacks and disruptions leading to huge losses. In the US, the head of the new Cyber Command revealed that "*Pentagon's systems are probed by unauthorized users about 6 million times a day. Total losses are, through cybercrime globally, maybe as high as 1 trillion dollars*" [1].

Today, people can interact and communicate over the internet, browsing through several websites, without being worried about their data being exploited. The reason for this lies in Cyber Security. The Internet infrastructure grows at a tremendous rate. With most financial transactions happening online, the level of security required is extremely high. However, we also face an alarming increase in cyber-attacks and data breaches. And in India with the second largest Internet population in the world, the risks are immense.

Every year, cybercrimes reported across India increase at a significant pace. The most targeted are the finance and banking sectors. The onset of the pandemic has encouraged a surge of cybercrimes. With most platforms and services shifting to an online platform, the risk of cyber-attacks has been as high as ever. Recent victims include the online grocery platform, Big Basket, with the data of approximately 20 million users compromised in a data breach in November 2020, and Air India with the data of over 4.5 million users compromised in early 2021.

According to the Gartner Group, "*97 percent of the over 300 websites audited were found vulnerable to web application attacks, and 75 percent of the cyber-attacks today are at the application level*." [2]

These cyber-attacks come in different types and magnitudes. A malware attack can be a simple email while a botnet attack can bring down a whole website.

These cyber-attacks can also leave entire cities in a state of disarray. For example, in Dec 2019, the New Orleans mayor declared a state of emergency in the wake of a cyber-attack disrupting the city's services [3]. The application layer is most prone to cyber-attacks, such as SQL Injection and DDoS attacks. However, 95% of cyber-attacks are caused by human error [4]. This makes negligence, espionage, and insider jobs larger threats to cyber peace than Black Hat hackers.

Several generic solutions exist to tackle cyber threats, viz. Firewalls, Data Encryption, Email Filtering. An amalgam of these solutions with user awareness provides an adequate first-line defense against cyber issues. James Scott, Senior Fellow from the Institute of Critical Infrastructure Technology (ICIT), a Cybersecurity based firm, says: "*There's no silver bullet solution with cyber security, a layered defense is the only viable defense*."

CYBER SECURITY THREATS AND ATTACKS

Over the years there have been several variations of basic cyber threats. Cyber threats identify a system vulnerability and attack it strategically. These can be broadly divided into three main categories on the nature of the threat:

- Cybercrimes Against Individuals - online bullying, individual privacy barging, stealing individual data and asking for ransom, etc. Cyberattacks have negative effects on society as a whole and need to be controlled or monitored by the cybercrime branch.
- Cybercrimes Against Property and Networks - for instance computer vandalism, and the transmission of destructive virus programs like the Morris Worm. Such crimes cause losses worth millions of dollars across the globe each year by damaging other networks, computers, and businesses.
- Cybercrimes Against Government Run Organizations – these can include arsonist activities that barge into government-maintained systems and databases and steal potential data. This may occur either in the form of hacking, trespassing authority, fraud, etc. These attacks can incur a huge cost to the country and government.

A few of these cyber threats are discussed in detail below.

DDoS Attacks

A distributed denial-of-service, more commonly known as DDoS attack, is a planned attempt of hampering traffic to bring down either a targeted server, service provider, or certain network by staggering the infrastructure of the target and its environment via a flood of Internet traffic arising from various sources.

A successful DDoS attack requires networks of Internet-enabled devices. The devices in these networks are contaminated with the help of malware, which enables their control over a remote network by the hacker. Devices that are infected and controlled in this manner are called bots or zombies, and a group of such bots is called a botnet. Upon completion of the establishment of a botnet, the attacker provides remote instructions to every bot in the botnet.

When a botnet attacks a server or network, each bot continuously sends requests to the IP address of the network being preyed on, causing the server to overflood with requests. This results in a denial of service. Since botnets include legitimate devices connected to the internet, it becomes difficult to distinguish between normal traffic and attack traffic. There have been recent developments in DDoS attacks where IoT devices like CCTV cameras are also being used in the attack, taking advantage of their security issues [5].

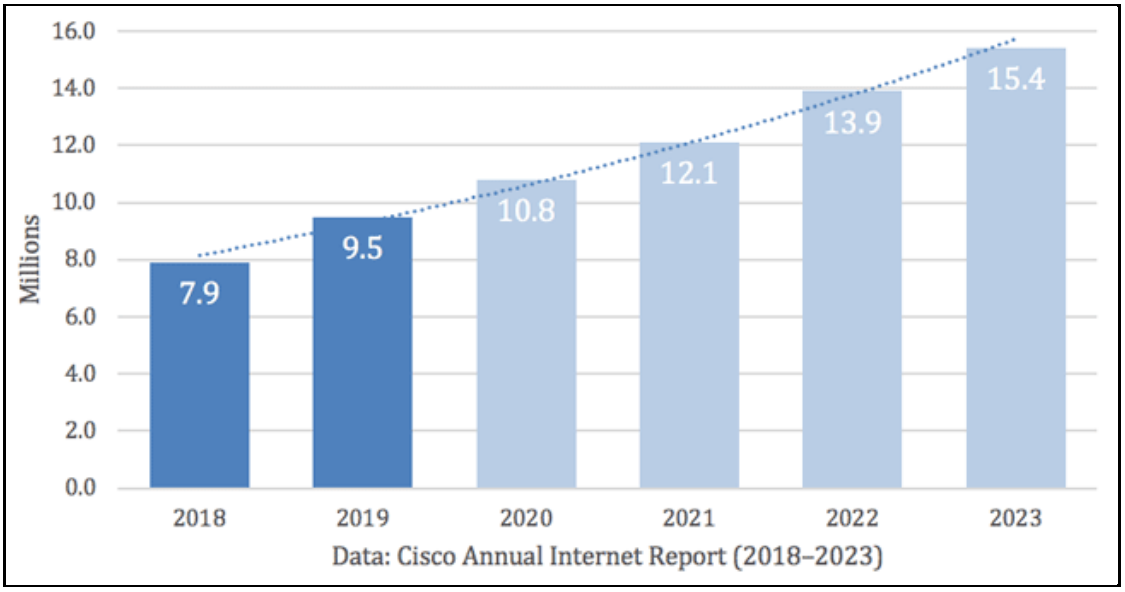


Fig1: Increasing frequency of DDOS attack and effect over years [Courtesy: Cisco Annual Internet Report]

Over time, there have been many DDoS attacks. Two of these attacks are [6]:

- Google - 2017: Thousands of Google's IP addresses were attacked by three Chinese ISPs. The attack lasted for around 6 months with the topmost traffic volume being 2.3 Tbsp.
- AWS - 2020: Amazon Web Services (AWS) alleviated one such DDoS attack during February 2020 which had a peak traffic volume of 2.3 Tbsp. The attack was a reflection attack, which exploited the exposed CLDAP servers to amplify traffic.

Malware Attack

Malware is malicious software that can execute unauthorized actions on the system without the knowledge of the victim. There are numerous types of malware attacks, some of the most common ones include Keylogger, Virus, Trojan Horse, and Worms.

- Ransomware - The attacker locks the user out of the system or threatens to leak the data of an individual until a ransom is paid.
- Keylogger - Keylogger is software that runs in the background of the victim's system. As the name suggests, it logs all the keywords from user activity and sends it to the attacker.
- Virus - Destructs or harms the system or data associated with the system.
- Worm - Worms replicate themselves and spread through networks.
- Trojan Horse - These are malware software disguised as legitimate software.
- Logic Bombs - Logic bombs are viruses that get triggered when a certain event occurs.

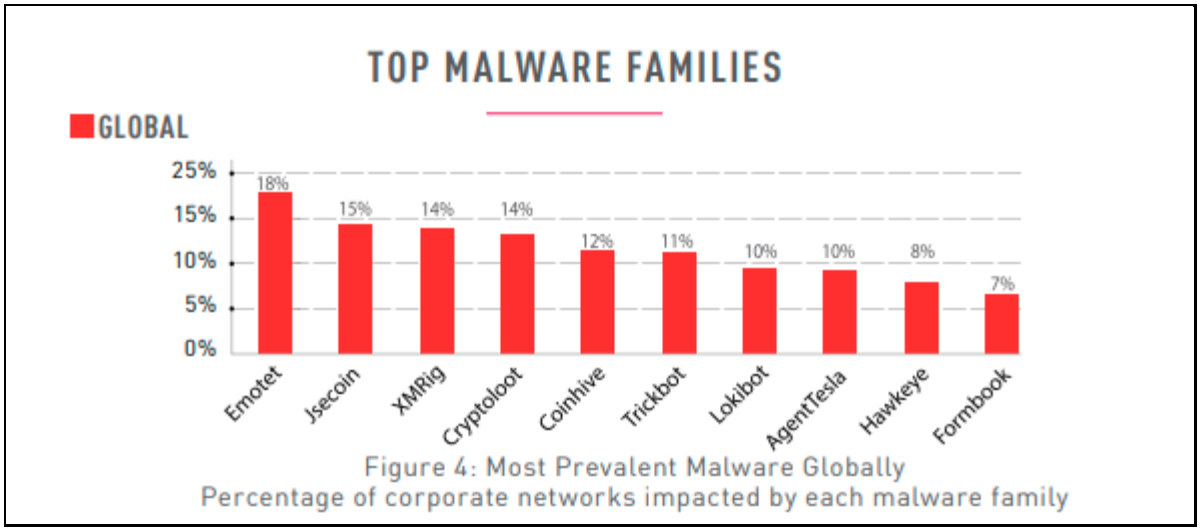


Fig 2: Most Prevalent Malware Globally Percentage of corporate networks impacted by each malware family [Courtesy: ntsc.org]

Famous Malware attacks include those of Emoted, a trojan that spread through spam and phishing emails in 2018, with over 3 million USD incurred in losses; and WannaCry ransomware that exploited a vulnerability in Windows, inflicting losses of over 4 million USD on FedEx, Nissan, and others. [7]

Password Attack

Password attacks are done to get the passwords of users. Five types of password attacks include [8].

- Dictionary Attack - Every permutation combination of dictionary words is tried. Such attacks can be avoided by not keeping passwords from the dictionary.
- Brute Force - The trial-and-error method is implemented to crack the password of the user. Permutation combination of all letters is tried. This requires a lot of computational power.
- Keylogger - If a keylogger is installed on the victim's system password, it records all the hits by the user during his activity on the keyboard and sends it to the attacker
- Rainbow Table - Attackers use a hash table to find the password
- Shoulder Surfing - When the attacker observes the keyboard of the victim when the victim is entering the password.

Network Attack

Network attacks gain unauthorized access to an organization's network to obtain sensitive information or to perform malicious activity. Network attacks are classified into two types [8].

- Active Attack - The attacker intrudes and disrupts the network's normalcy, actively modifies the data, and alters the system resources.
- Passive Attack - The attacker eavesdrops on the network to obtain sensitive information and does not modify any information.

Social Engineering Attack

Social Engineering attacks manipulate humans into giving out their sensitive information.

This attack is broadly classified into these types:

- Phishing Attack - Phishing attacks are non-targeted attacks. Phishing attacks are carried out to steal sensitive or confidential information such as login credentials, bank account details, etc. Attackers send malicious links duping legitimate trusted entities. When the user clicks on the link either malicious links are installed, or the user is duped to give out sensitive information.
- Spear Phishing Attack - A phishing attack is done on a targeted audience after research on the vulnerabilities of the targeted group or organization.
- Whaling Phishing Attack - A phishing attack targeting powerful, wealthy, prominent individuals for monetary gain.
- Vishing - The attacker dupes the victim into giving out sensitive information over the phone, often harnessing human emotions such as fear.
- Smishing - The attack is like phishing, where an attacker uses SMS to dupe their victims.

Cross-Site Scripting Attacks

Also commonly known as XSS Attacks, these attacks make use of a third-party website to install malicious code on victims' systems. The code is scripted as part of the payload of the website header. When the user opens the website malicious code is infected within the victims' system. XSS attacks could have serious consequences which would allow an attacker to capture a screenshot, virtually control the machine, or log user activity.

Salami Attacks

These kinds of attacks normally target financial institutions and online financial transitioning platforms. Such attacks are initiated by engineering a piece of code or altering software in an attempt to steal small chunks of money from an ongoing transaction and swerving them to a different credential. Money that will be transferred can be so minimal that it can go unnoticed. For instance, 2 cents can be deducted from many transactions and hidden in a different account.

COMMON REASONS FOR CYBER ATTACK

Cybercrime and cyber-attacks have been increasing over the years. There are many motives behind these crimes and attacks, but the most common include information theft and manipulating data, asking for ransom, disrupting business activity, creating financial loss to companies, achieving state military objectives, and propagating religious or political beliefs. While the motives can be many it is important to analyze the reasons for system vulnerability for such attacks. Some of these reasons are discussed below:

- **System Vulnerabilities** - Cyber-attacks often make use of system vulnerabilities to plant the attack.
- **Negligence** - Attackers exploit system users' careless behavior and negligence in protecting the system or sensitive information.

- **Security Gaps in Code** - Operating Systems and present-day software are composed of millions of codes and any gap in security in these codes can be used to attack the system.
- **Malicious Insiders** - those from an organization who might have access to sensitive information and credentials.

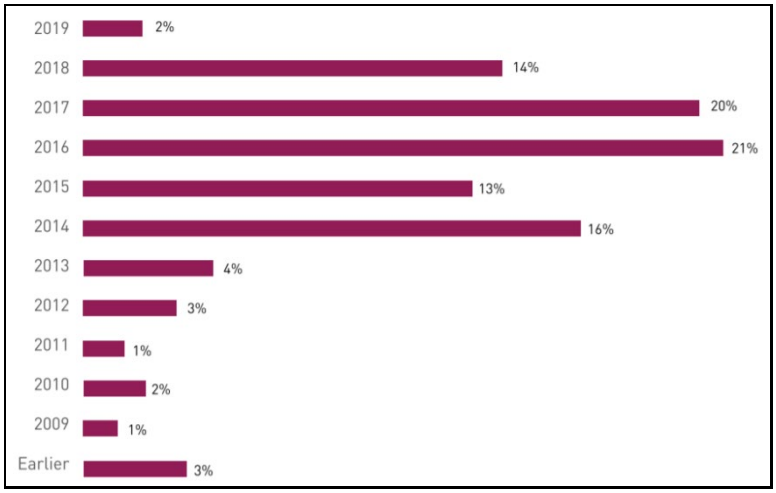


Fig 3: Exploited CVEs by Year [Courtesy: ntsc.org]

CURRENT STATE OF ART

Over the years various technologies have been developed to counter cyber threats. These include Intrusion Prevention Systems (IPS), Endpoint Detection and Response (EDR), etc. A firewall is the most common solution employed to offer protection and security, but they only apply to application-level threats. Hence, advances were made to improve firewalls and Next Generation Firewalls were built. All these solutions are explained in brief.

Vulnerability Scanners

Vulnerability Scanners are automated software on a system that can regularly run and scan for any vulnerability in the system or network that the attacker might exploit. Vulnerability Scanners scan for previously identified vulnerabilities. These Scanners provide users with information such as the vulnerability that is present, the risk associated, and the extent of damage that can be caused, and how to mitigate the vulnerability.

There are 5 Types of vulnerability scanners based on the asset type they will be assessing:
- Network-based scanners - Identify possible network security attacks and vulnerabilities
- Host-based scanners - Identify vulnerabilities in workstation, network hosts
- Wireless scanners - Validate company's network security configuration
- Application scanners - Web application scanners that identify known vulnerabilities
- Database scanners - Identify vulnerabilities or weak points in the database

Apart from this, they are also classified into external or internal scanners and authorized and unauthorized scanners depending on the kind of authorization done.

Web Application Firewall

Web Application Firewalls are installed to protect web applications and constantly monitor the traffic between the Internet and web applications. They protect systems from attacks such as SQL injection and XSS attacks. WAF is an application layer defense system in an OSI network model. WAF does not protect against all kinds of attacks.

Next Generation Firewall (NGFW)

NGFW is a recent development in the field of cybersecurity. Traditional Firewalls analyze traffic based on IP addresses and fail to consider previous traffic that might have already passed through the firewall. NGFW allows dynamic packet filtering, monitoring of all active connections, and state of connection. Another advantage of NGFW over WAF is that it can block malware, which is impossible to achieve in a traditional firewall.

Endpoint Detection and Response (EDR)

The endpoint in an organization's network is communication entry and exit. These are generally laptops, workstations, servers, tablets, and other human-machine interface devices. Endpoints have operating system software and application software. This software is vulnerable to attack. Endpoint Detection and Response is an additional security that is provided at the endpoint. EDR can detect malicious attacks and provide a graphical view of how the attack took place, which endpoint was targeted, and the files that have been corrupted.

Spam Filters and Anti-Malware on Mail Gateway

Social Engineering Attacks make use of the mailing system to deliver and deploy malware in the victim's system. Spam Filters and Anti Malware on Mail gateway can reduce such attacks.

Cryptographic Techniques

These techniques are used to protect sensitive information from attackers by employing various encryption methods.

- Secret Key Encryption - A common key is shared by two users - sender and receiver. The problem with such encryption is the number of keys each user will have to hold.
- Public Key Encryption - In this type of encryption two keys are shared, one public key and one secret key.
- End-to-End Encryption - Exchange of information between two parties without the intervention of the central server.

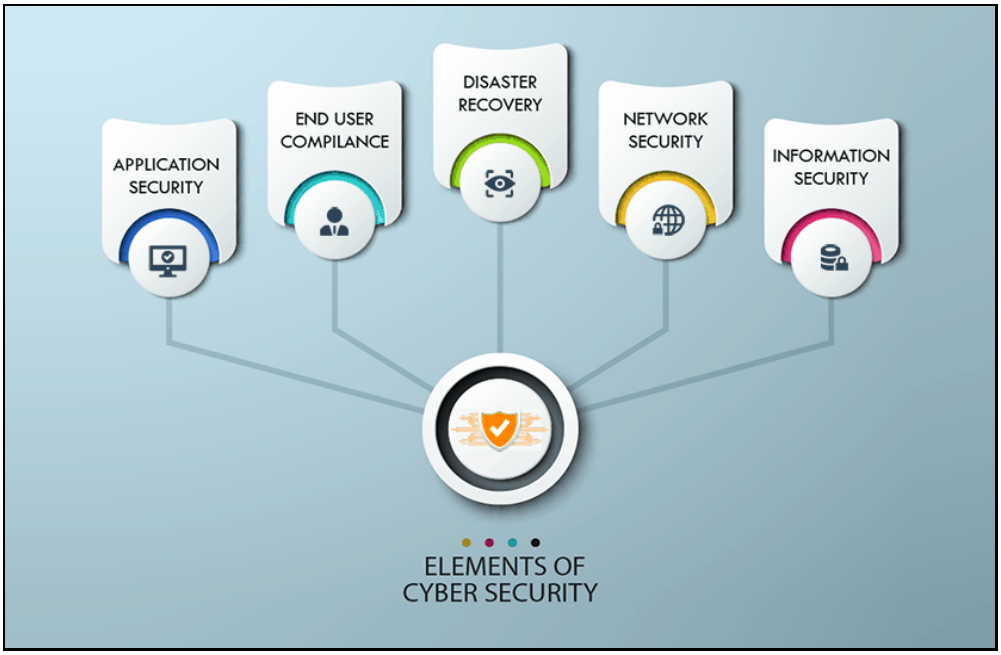


Fig 4: Different Elements of Cyber Security [Courtesy: phoenixnap.com]

CHALLENGES TO EXISTING SOLUTION

- Lack of awareness regarding cyber security and the possible threat it poses. Organizations should ensure they take the necessary steps to educate their employees regarding best practices to avoid cyber-attacks.
- Techniques mostly being used currently are based on signatures that carry a representation of the attack which is syntactic [2].
- Fast-evolving technologies such as the Internet of Things, Cloud Computing, and Machine Learning might have new kinds of vulnerabilities that can be exploited. The R & D community should investigate developing cybersecurity standards for these technologies.
- Lack of Low-Cost solutions and Self-Assessment options for cyber threats. With the increase in self-assessment and low-cost solutions, many SMEs will be able to deploy the solutions.

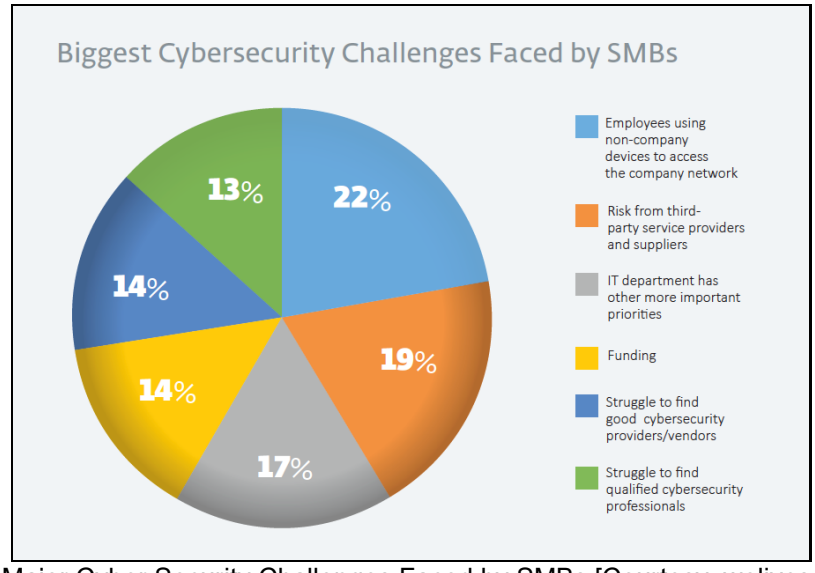


Fig 5: Major Cyber Security Challenges Faced by SMBs [Courtesy: welivesecurity.com]

CASE STUDIES

Canva Data Breach - May

Case Scenario: A massive data breach took place in May 2019. Canva, a graphic design company based in Sydney with over a multimillion user base, was the prey of this attack. Because of the attack, users' critical data was purloined and sold on the dark web. The event was reported on 24th May, followed by a verification test conducted with the help of personal data for 17,000 users.

This had a huge toll on their data. The following lists of data lost:

- The database of 139 million users comprising critical pieces of information such as real names, usernames, email addresses, and other sensitive personal information.
- Encrypted passwords were secured using the crypt hashing algorithm, which is one of the best.
- OAuth tokens of Google based users, some limited banking, and transactional details of users.

To overcome the scenario, the team at Canva decided to send out an email immediately to all its users informing them about the attack and how they were already working on the situation. Users were advised to immediately change the passwords of their respective accounts [9].

Canva was able to identify the situation during the breach, and as an immediate first aid the company shut down its servers, preventing more than 50 percent of the breach.

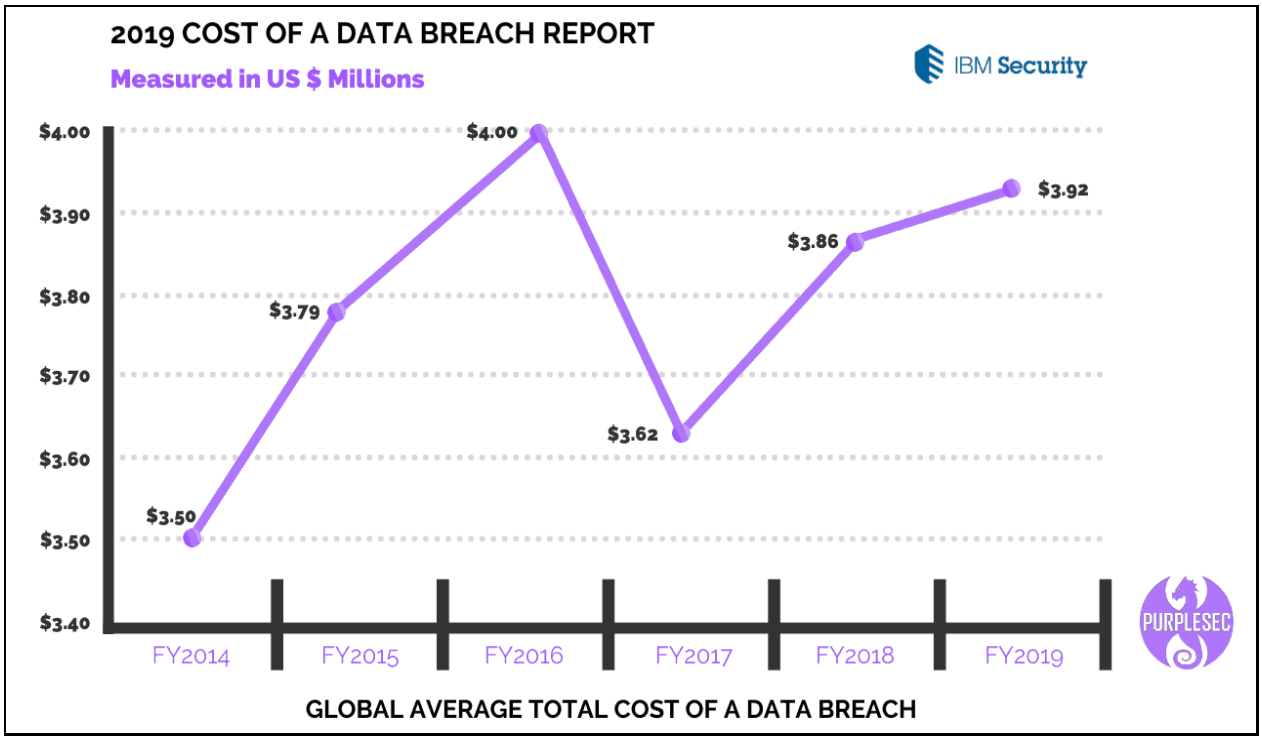


Fig 6: Graph indicating cost of data breach in the year 2019 [Courtesy: purplesec.us]

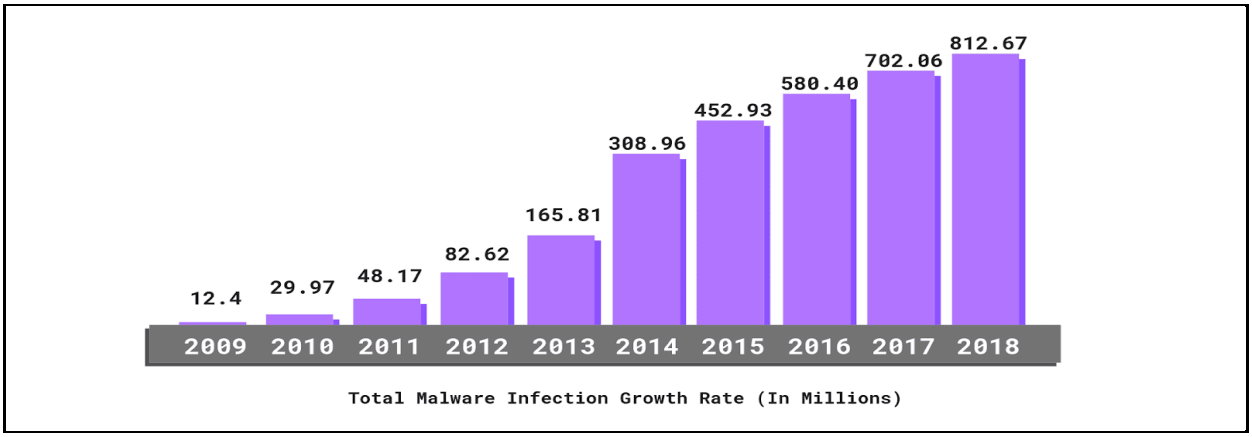


Fig 7: Graph indicating total malware infection growth rate over the decade [Courtesy: purplesec.us]

GitHub DDoS Attack

Case scenario: GitHub.com, one of the most widely used platforms by companies and individuals in the world for maintaining and running projects and codes, became inaccessible from 17:20 to 17:26 UTC and 17:26 to 17:30 UTC on February 28th, 2018. The company was pushed into such a condition due to a DDoS attack that was carried out on its server. It is noted that the attack originated from more than 1,000 varied ASNs, which were laid out over a hundred thousand distinctive endpoints. It was an amplification attack that was carried out using a Memcached-based approach which had a peak of 1.35 Tbsp. through hundred and twenty-six point nine (126.9) million packets per second. The GitHub network administrative system spotted an incongruity in the ingress-by-egress traffic ratio and warned the on-duty engineers and the GitHub chat system.

To overcome the scenario, GitHub took certain strategic steps. Since there was a huge increase in the inbound transit exceeding more than 100Gbps in one of GitHub's facilities, they decided that transferring the traffic to another server that could offer ancillary edge capability services, the best viable option being Akamai, which had these features.

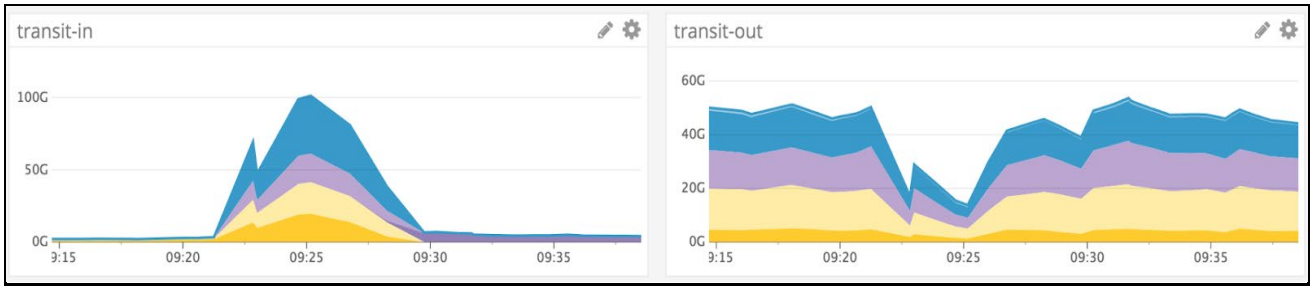


Fig 8: Inbound and Outbound data traffic during the attack [Courtesy: GitHub]

Following the shift to Akamai, at 17:26 the command to withdraw Border Gateway Protocol announcements over transit gateway providers and announce new protocols exclusively over the new routes to Akamai was initiated. The attack was diminished at the border by the access control lists as soon as the new route lines to Akamai were established. Based on the analyzed bandwidth volume and the codes used for load balancing, a full recovery happened at 17:30 UTC. Two major peaks were observed during the attacks - during the first portion the attack hit a peak of 1.35Tbps and during the second it was at a 400Gbps spike [10].

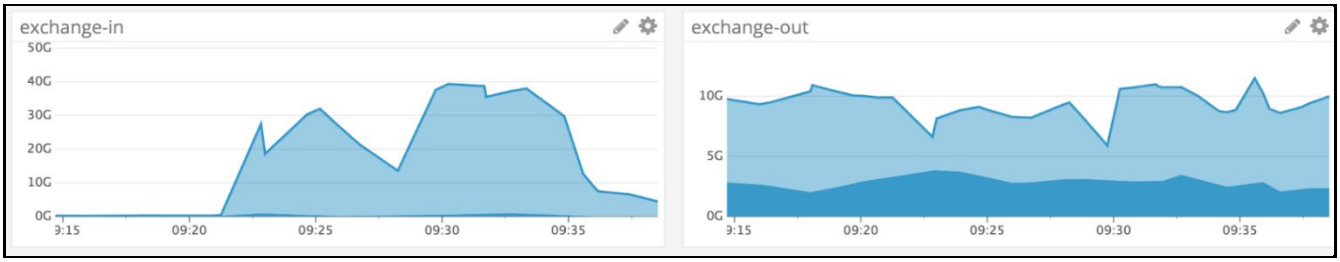


Fig 9: Exchange in and Exchange out traffic after shifting to Akamai server [Courtesy: GitHub]

Amplification attack functions by misemploying Memcached instances which are unwittingly accessible via the Internet in a public domain space, supported by UDP enabling. Enabling IP Spoofing allows the transfer of Memcached responses to a different address that is targeted and then sends excess data toward the prey server than what is normally transferred by the spoofed source. The vulnerable damages inflicted via this type of misconfiguration are considered one of the most peculiar among the class of attacks due to the amplification factor being up to 51,000 in these cases. So, the conclusion is that for every byte that is transferred by the hacker, more than Fifty-One Kilo Bytes are transferred towards the targeted system.

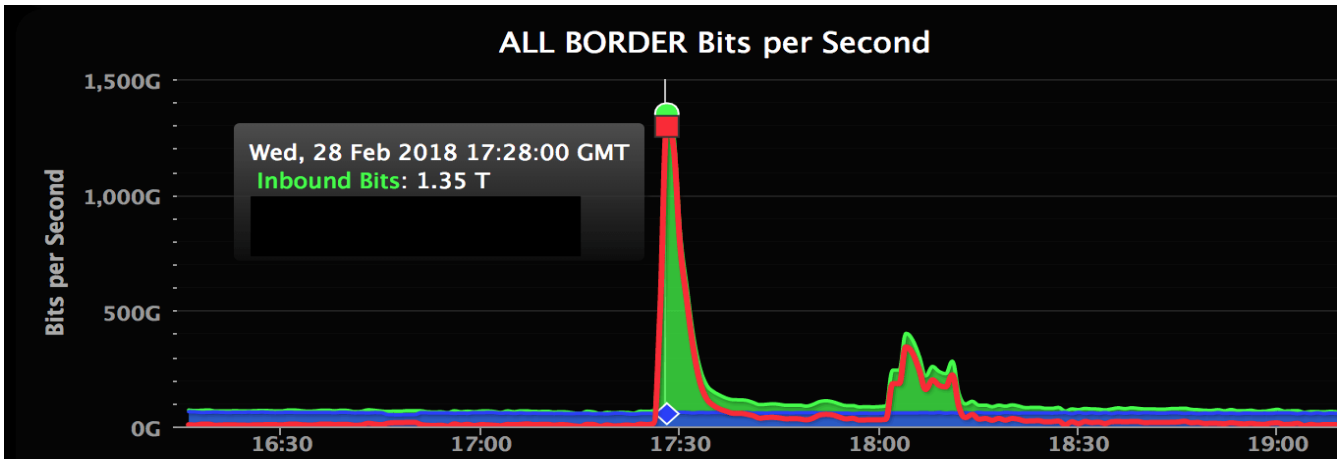


Fig 10: Graph indicating top inbound traffic peaks reached during the arrack [Courtesy: github]

GitHub has promised its users that there are more serious investigations being carried out for enabling the usage of monitoring-based infrastructure that can automate a security protocol that enables mitigation of DDoS attacks. They will continue measuring the response time in such critical cases with a vision to reduce mean time to recovery (MTTR). The company promises its users to build a platform with better detection systems and streamlined processes during emergencies, ensuring the availability and security of the platform.

Zynga Hack

Case Scenario: Zynga, a multimillion-dollar social gaming company, known for its most attractive online games such as ‘Villa’ on Facebook, recently underwent a cyberattack.

In September of 2019, a Pakistani hacker by the name of Gnostic players succeeded in hacking into Zynga’s database of apps, namely Draw Something and Words with Friends. The hacker claimed that he had gained access to the data of 218 million users who had registered for those games. Later, the company confirmed that many critical data items such as email addresses, phone

numbers, user IDs for Zynga, and corresponding Facebook accounts, along with salted SHA-1 hashed passwords were stolen [11].

Most effects of the threat had fallen upon Android and iOS users. Since Zynga does not store Facebook passwords, just the email IDs were compromised. The password protection mechanism used by Zynga,SHA-1, was considered outdated even before the establishment of the company in 2007. Due to this reason, a class-action lawsuit was filed against Zynga on behalf of the players affected by the data breach. The 41-page complaint brings to light that Zynga knew about its vulnerabilities as early as 2012, and still failed to implement the required security measures.

Conclusion

As this paper demonstrates, the threat of cyber-attacks is enormous. This entitles all governments and corporations to pay more attention to cybersecurity. Organizations need to adopt a proactive plan of action to stay a step ahead of cyber criminals and prevent attacks, rather than countering the attack after the attack has been planted. Relying on damage control can have devastating consequences for any organization, as, in many instances, once the malware penetrates an IT infrastructure, this implies an infection that will spread in mere seconds and will be nearly impossible to get rid of. Organizations today must be aware that cyber-attacks are imminent; and even with state-of-the-art security features, the risk of cyber-attack is always there. Detection and automated blocking of an attack at an early stage can prevent damage.

To win the cyber security battle, companies need to implement layered threat prevention technology, solid threat intelligence, and security architecture that protects against a range of cyber-attacks.

Bibliography

[1] Muhammad Altaf Mukati and Syed Muzammil Ali, “The Vulnerability of cyber security and strategy to conquer the potential threats on business applications”, Journal of Independent Studies and Research, Jan 2014, vol 12, pp 56-62

[2] Abdul Razzaq et al., “Cyber Security: Threats, Reasons, Challenges, Methodologies, and State of the Art Solutions for Industrial Applications”, In Autonomous Decentralized Systems ISADS, Mar 2013.

[3] Forbes article on New Orleans Cyber Attack, “https://www.forbes.com/sites/daveywinder/2019/12/14/new-orleans-declares-state-of-emergency-following-cyber-attack/,” Dec 2019.

[4] Cyber Security Report 2020, “https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf”, 2020.

[5] IBM article on IoT Devices being used in DDoS attacks, “https://www.ibm.com/blogs/internet-of-things/ddos-iot-platform-security/”, Dec 2016.

[6] Article on Famous DDoS Attacks, “https://www.a10networks.com/blog/5-most-famous-ddos-attacks/”, July 2020.

[7] Norton Article on Malware Attacks, “https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html”, Jul 2019

[8] Cisco article on Common Cyber Attacks, https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html.

[9] Canva's Status Update on their Data breach,"https://www.canva.com/help/article/incident-may24", Aug 2020.

[10] The GitHub Blog - Article on the DDoS attack, "https://github.blog/2018-03-01-ddos-incident-report/", Mar 2018.

[11] Biggest Data Breaches of all time, "https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html", Jan 2021.

[12] A. Rae and A. Patel, "Developing a security behavioral assessment approach for cyber rating UK MSBs," 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2020, pp. 1-8, DOI: 10.1109/CyberSecurity49315.2020.9138893.

[13] K. N. Sevis and E. Seker, "Cyber warfare: terms, issues, laws, and controversies," 2016 International Conference On Cyber Security and Protection of Digital Services (Cyber Security), 2016, pp. 1-9, DOI: 10.1109/CyberSecPODS.2016.7502348.

[14] Anitha A., and Vaidehi, V.: "Context based Application-Level Intrusion Detection". Proceedings of International conference on Networking and Services (ICNS06) (2006), IEEE.

[15] Razzaq, A. et al., "Foundation of Semantic Rule Engine to Protect Web Application Attacks". In Autonomous Decentralized Systems (ISADS), 2011 10th International Symposium on, IEEE, pp. 95–102.

[16] M. Eckhart et al., "Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins," 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1222-1225, DOI: 10.1109/ETFA.2019.8869197.

[17] S Huang, et al."A multi-channel cybersecurity news and threat intelligent engine – Sec Buzzer, 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2019, pp. 691-695, DOI: 10.1145/3341161.3345309.

[18] Ryutov, T. et al, "Integrated access control and intrusion detection for web servers", IEEE transactions on parallel and distributed systems (2003), 841–850.