ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (80-90), Month: October - December 2020, Available at: www.researchpublish.com

Common Cyber Threats to Organizations

[1]Mohamed Asadullah, [2]Jamaludin Bin Ibrahim

[1,2]Kulliyah of Information and Communication Technology, International Islamic University Malaysia Gombak, Malaysia

Abstract: **This paper aims to contribute to the body of knowledge on common cyber threats, methods, and impact among organizations. It is also to create awareness of cyber threats by identifying their definitions, potential targets, boundaries, crime patterns, and effective mitigation strategies. There will be a discussion of relevant literature review on cyber threats in recent years. This paper elaborates on common cyber-attacks, to create social awareness and recommends to apply adequate controls and how they are designed to mitigate the risks to ensure safety.**

Keywords: **Cyber Threats; Cyber Attack, Cyber Security, Organizations, Process, Technologies.**

I. INTRODUCTION

Data is increasingly getting digitized and the internet is being used to save, access, and retrieve vital information. A cyber threat is a malicious act to damage data, steal data, or disrupt the digital life of data. Each malicious act requires various steps and methods to exploit data. Cybersecurity in general refers to get rid of this malicious act by applying business functions and technology tools are used to protect information assets. Cybersecurity has played and would continue to play a very prominent role in the future. This is attributed to the rapid technological and connectivity advancements which is also the same platform used by threat agents to disrupt and exploit important assets. The devastating business effects of cyber-attacks, such as the WannaCry, Petya, and NotPetya attacks which took place in 2017 point to inaction on those charged with the implementation of cybersecurity framework and the lack of adequate board oversight [1]. As such, every organization may struggle to put in place the right level of governance, management, and assurance practices to protect themselves from intentional attacks, breaches, and incidents.

II. LITERATURE REVIEW

The recent records of cyber threats were observed from ENISA and IDC Corporation. ENISA, a European Union Agency for Cybersecurity which is fully operational since September 1, 2005, and located in Athens, Greece. IDC, an International Data Corporation that provides market intelligence, advisory services, and events for the information technology located in the USA.

Malware Attacks

According to ENISA Threat Landscape: Malware, from January 2019 to April 2020 state the findings below:

- 400,000 detections of pre-installed spyware and adware on mobile devices [2].
- 13% increase in Windows malware detections at business endpoints globally [2].
- 71% of organizations found malware spreading from one to another employee [3].
- 46.5% of all malware in e-mail messages found in the '.docx' file type [4].
- 50% increase in malware designed to steal personal data or stalker were [5].
- 67% of malware was delivered via encrypted HTTPS connections [6].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (80-90), Month: October - December 2020, Available at: www.researchpublish.com

Prevalent Malware Types

Emotet is a type of malware that was discovered in early 2014 as a banking trojan. Emotet was identified as the most prevalent type of malware strains in 2019 and is continued to be evolved in 2020 around the globe. Emotet evolved into a botnet to increase its activity and initiated new localized spam campaigns to install ransomware or to steal information.

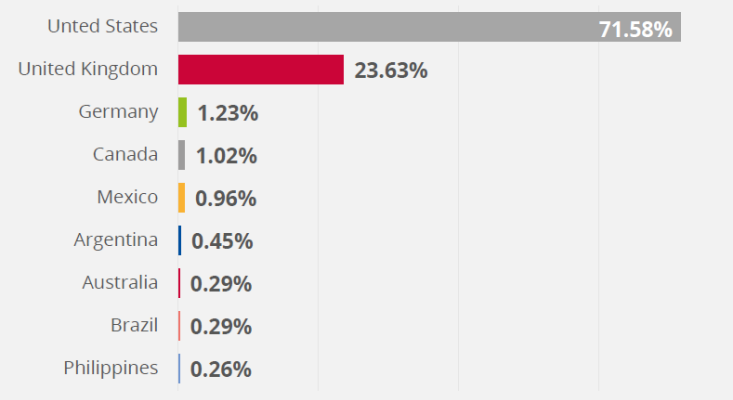

Fig 1: Global Emotet Detections by Country as of Q3 2019.

Source: Malware bytes [2] & ENISA [43]

Malware into Business Targets

Although malware detections globally remained at the same levels as in 2018, a 13% increase in malware targeting businesses was observed in banking, services, education, and retail among the worst affected sectors [2].

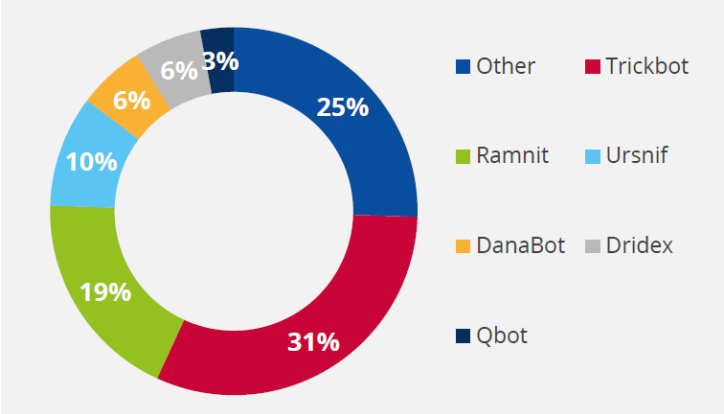

Fig 2: Global Banking Malware Detections as of Q3 2019.

Source: CheckPoint [7] & ENISA [43]

File-less Malware Types

File-less malware does not contain an executable file. It can evade common security filters. For this reason, this malware family can be up to ten times more vigorous to succeed than the others [8]. Instead of an executable file, this type of malware requires the attacker to inject malicious code into already installed and trusted software, either remotely (e.g., in the case of Windows Management Instrumentation or WMI and PowerShell) or by actively downloading document files (i.e., office documents) containing malicious macros [9]. After a successful attack, the malware can gain persistence through the registry, built-in task scheduler, or the WMI. File-less malware attacks increased by 265% during the first half of 2019 [10]. The majority of such attacks were script-based (38%), while others executed an in-memory attack (24%) or abused built-in system tools (20%) [11].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (80-90), Month: October - December 2020, Available at: www.researchpublish.com

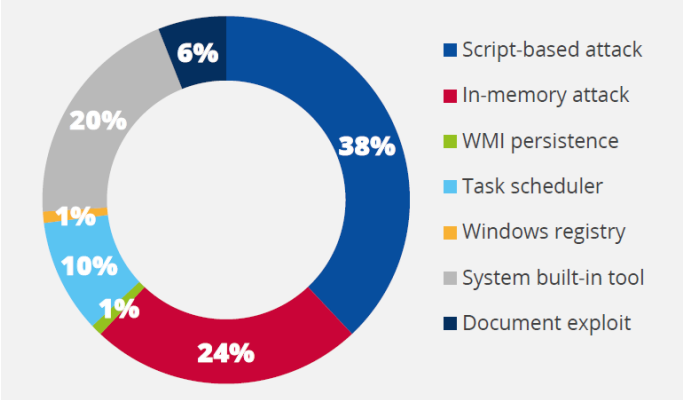

Fig 3: Percentage of File-less Events Detected in the first half of Q3 2019.

Source: Norton [9] & ENISA [43]

Phishing Attack

According to ENISA Threat Landscape: Phishing, from January 2019 to April 2020 state the findings below:

- 26.2 billion of losses in 2019 with Business E-mail Compromise (BEC) attacks [12].
- 42.8% of all malicious attachments were Microsoft Office documents [13].
- 66.7% increase in phishing scams in only 1 month during the COVID-19 pandemic [14].
- 30% of phishing messages were delivered on Mondays [15].
- 32.5% of all the e-mails used the keyword 'payment' in the e-mail subject [16].

The Rise of HTTPS-Based Phishing Attack

More than 2/3 of phishing sites are HTTPS-based and continuously increased over the past few years. In the last quarter of 2019, 74% of phishing sites were using HTTPS [17]. Although technologies such as HTTPS (Hypertext Transfer Protocol Secure) and SSL (Secure Sockets Layer) are designed to secure communications between a web-client and a web-server, the presence of a lock-in icon at the browser's address always create the illusion that a website can be trusted. Hackers might use legitimate sites that they have hacked to host phishing content, therefore it is challenging for the end-user to identify a site as unsafe. Other factors contributing to the increase in HTTPS usage are the plethora of free certificate services such as Let's Encrypt and the fact that modern browsers mark every HTTPS site as secure, without any further checks [18]. Trends of phishing frequently attack into cloud storage, DocuSign, Microsoft cloud services, Microsoft 365 services, BEC (Business Email Compromise), etc.

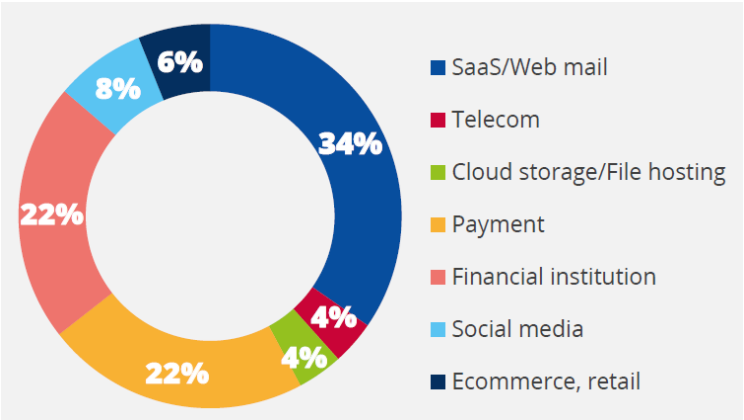

Fig 4: Phishing Target Attacks as of Q3 2019.

Source: Proof Point [19] & ENISA [44]

Distributed Denial-of-Service (DDoS) Attack

According to ENISA Threat Landscape: DDoS, from January 2019 to April 2020 state the findings below:

- 24.1% increase in the total number of attacks during Q3 2019 compared with the same period of 2018 [20].
- 79.7% of all DDoS attacks were SYN-Floods [21].
- 86% of the mitigated attacks during Q3 2019 were using more than two vectors [22].
- 84% of the DDoS attacks lasted less than 10 minutes [23],[24].
- 509 hours was the duration of the longest DDoS attack in Q2 2019 [20].

DDoS Attack Vectors

Based on security researches, UDP (User Datagram Protocol) flood was found to be a popular attack vector in 2019 and it is believed to be related to the dominant adoption of this protocol in high-risk industries such as gaming. DNS (Domain Name System) and TCP (Transmission Control Protocol) based attacks followed by UDP floods are in the list of top attack vectors. There was also an observation of multi-vector throughout this period. However, research shows that some of the multi-vector attacks are an unintended by-product of a DoS attempt [24]. DNS Amplification attacks were identified as the top DDoS attack vector followed by HTTP flood and TCP SYN attacks. The number of attack vectors in Q3 2019 was similar to SYN floods, the top vector was followed by UDP, TCP, and HTTP attacks.

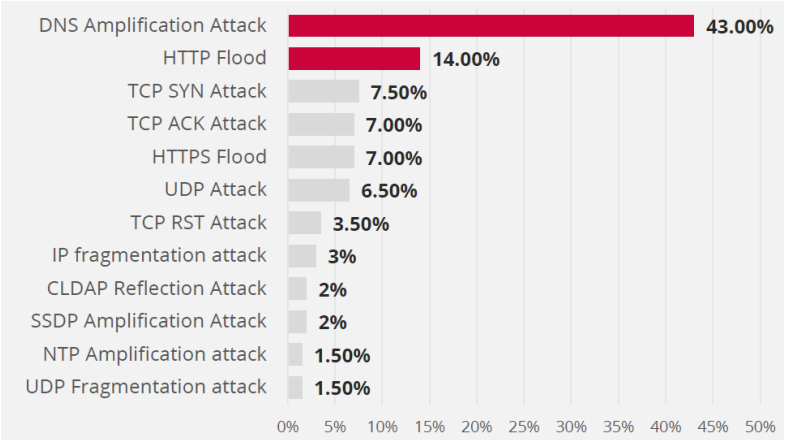

Fig 5: DDoS attack vectors in Q3 2019.

Source: NexusGuard [25] & ENISA [45]

Structured Query Language Injection (SQLi) Attack

According to ENISA Threat Landscape: Web-Application Attacks, from January 2019 to April 2020 state the findings below:

- 20% of companies and organizations reported DDoS attacks on their application services daily. A buffer overflow was the most common technique used (24%). HTTP flood (23%), resource reduction (23%), HTTPS flood (21%) and Low Slow 21% were other commonly used techniques [26].
- 63% of respondents to the CyberEdge survey are using a WAF (Web Application Firewall). 27.5% have plans to deploy this technology and 9.5% do not have any such plans [27].
- 52% increase in the number of web application attacks in 2019 compared with 2018. According to a security researcher, the amount of web application attacks was almost flat compared with 2018 and rose sharply later in the year [28].
- 84% of observed vulnerabilities in web applications were security missed configurations. This was followed by cross-site scripting (53%) and broken authentication interestingly (45%) [29].

Growing trend of SQL injection (SQLi)

Web-based services and web-applications depend mostly on databases to store, retrieve, and to deliver the required information. SQL Injection (SQLi) types of cyberattacks are well-known of these examples and the most common threats against web services. Based on security research identified that two-thirds of web-application attacks include SQLi attacks. Whereas, other web-application-attack vectors were stated to remain or growing continuously. SQLi attacks continued to be growing sharply, and this was notified at its peak during the holiday season of 2019. The SQLi attacks target's finance industry and they face more LF (local-file-inclusion) attacks compared with other sectors. There is always a general perception that web-application attacks are quite diverse. However, data from security research shows that major threats in web-application attacks are limited to SQLi, followed by directory traversal, XSS (Cross-Site Scripting), broken authentication, and session management which are on the top of the attack vectors [30].

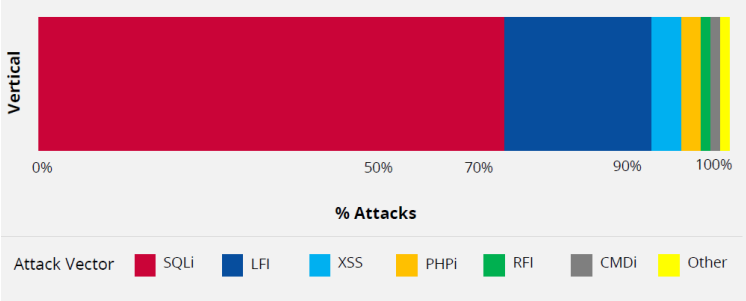

Fig 6: Attack Vectors

Source: Akamai [31] & ENISA [46]

Zero-Day Exploit Attack

The most frequent techniques used to start a cyber-attack include brute force with stolen credentials, configuration errors, exploitation of web applications, and social engineering. Other techniques that are less frequently executed but equally important in cyberattacks are the exploitation of system vulnerabilities from the outdated system patches and zero-day-exploitation where software backdoors are often used in more complex and sophisticated cyber-attacks.

Vulnerabilities of Zero-Day Exploits in Microsoft's Products

Internet Explorer 11 found Scripting Engine Memory Corruption Vulnerability, CVE-2020-1380 considered as zero-day exploitation. This classified by Microsoft as a memory corruption vulnerability turned out to be caused by Exchange Server failing to properly create unique cryptographic keys at the time of installation. The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory [32]. Microsoft released a patch (in the Windows kernel) on June 9, 2020, and the second vulnerability was patched on August 11, 2020.

Microsoft Exchange Server found Microsoft Exchange Validation Key Remote Code Execution Vulnerability, MITRE CVE-2020-0688 considered as zero-day exploitation. This classified by Microsoft as a remote code execution vulnerability exists in Microsoft Exchange Server when the server fails to properly create unique keys at install time. The security update addresses the vulnerability by correcting how Microsoft Exchange creates the keys during install [33]. Microsoft released a patch on November 2, 2020.

Domain Name System (DNS) Attack

Almost all major organizations require DNS to run their business and this was well focused by cybercriminals to conduct DNS-based attacks. DNS protocol will translate a user-friendly domain name, e.g., iium.com, into the computer-friendly IP address 206.19.48.158. When an end-user enters domain name iium.com into a client's browser, the DNS resolver looks up iium.com's numerical IP address. DNS attack can be easily done with the compromised of server administrator in case of an outdated version of DNS software, weaker authentication, and vulnerability in the system.

Impacts of DNS Attack

The migration of the application to the cloud increases from year to year. Downtime on cloud-based services caused by DNS attacks has significantly risen. It has been contributed to the reputational damage of organizations. The cost of DNS

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (80-90), Month: October - December 2020, Available at: www.researchpublish.com

attacks remained extremely high, affecting the brand image, data confidentiality, and the company finances. Instances of application downtime in-house or in the cloud are the most impacting result of DNS attacks. DNS attacks and business outcomes are interlinked and consist of strong measurable business impacts.

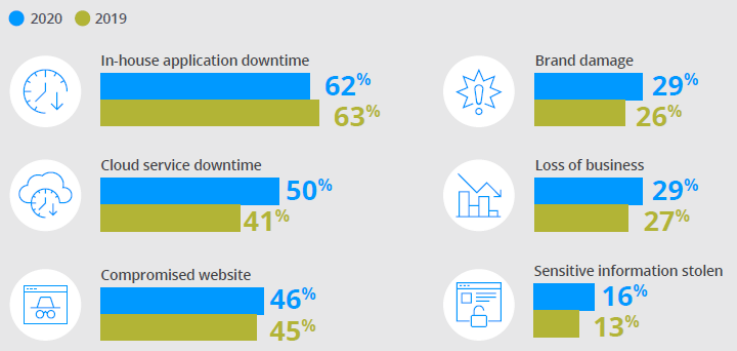

Fig 7: Impact Statistics

Source: International Data Corporation (IDC) [34]

III. CYBER THREATS AND MITIGATION STRATEGIES

Malware

Malware is a common type of cyber-attack which used to describe malicious software. Malware types include spyware, ransomware, viruses, and worms. Malware breaches through a network, especially on web and e-mail protocols. It is vulnerable typically when a user clicks an unidentified e-mail with an attachment or a link then it initiates to install of risky software. Once the transformation of malware into the system, it can block access to key components of the network; installs malware bugs or additional harmful software [35], i.e., ransomware. Then it may covertly obtain information by transmitting data from the end-user hard drives (also known as spyware) to the hacker's location. Disruption of system components may cause the system non-functional and access data. Users should always think before click and run scheduled scans with Malware Bytes, Anti-Malware and Antivirus. Users should undertake to halt arbitrary processes and isolate infected devices. Another effective way to defend against malware attacks is by keeping software up-to-date. Since there are file-less infections that happen with Microsoft applications it is important to keep these applications to the latest version. Microsoft has also upgraded its Windows Defender package specifically to detect abnormal activities in the PowerShell application or other scripting engines.

Phishing

Phishing is the practice of a fraudulent attempt of communication to steal login credentials, credit card information, money, and other valuable assets [36]. The main goal is to steal the user's sensitive data and the hackers install the malware in the victim's machine. Phishing is an increasingly cyber threat in a social network, i.e., social media messaging, WhatsApp. In the future, the most relevant change would be the methods used to send messages where adoption of adversarial Artificial Intelligence (AI). An emotional response from the victim is what hackers looking for. The mitigation strategy development should be practiced such as educate staff, launch simulated phishing campaigns and staff's responsiveness; apply security solutions to identify phishing sites in real-time, enhance the security of e-mail gateway by applying policy-based filtering, avoid clicking download attachments, communicate via secure e-mail communication that uses digital signatures or encryptions for critical financial transactions and sensitive information, apply fraud detection at the network level for both inbound and outbound e-mails; enhance social media awareness, avoid clicking short links or ads, avoid sharing personal information on social media, i.e. personal phone contacts, bookings, hotel reservations, duration of office leave, vehicle registrations and so on where these can be the source of information that could be collected by hackers; strengthen login credentials, enable mechanism of two-factor authentication, applying a strong and unique password.

DDoS

Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks are similar and can be differentiated by their scale. Single DoS attacks come from one source, while Distributed DoS attacks come from multiple locations by

flooding the network. The DDoS attack is non-intrusive internet attacks which flood systems, servers, or networks with traffic to exhaust resources and internet bandwidth. As a result, a targeted system will be a slowdown and unable to fulfil legitimate requests. Sometimes, attackers use multiple compromised devices to launch this attack and even a tiny amount of traffic is enough for the attackers to succeed. Website owners should familiarize themselves with the security landscape of their sites. The challenging part could be to navigate the various types of DDoS and always time-consuming. Certain signs could help us to identify DDoS attacks such as the website is unresponsive or responsive slowly and the user also may face internet connection issues. Users can apply security measurements such as activating WAF (Website Application Firewall) which helps to understand the types of data allowed for each protocol such as SMTP (Simple Mail Transfer Protocol) and HTTP. Attacks from various countries can be overcome by applying country blocking or geo-blocking on the sites. Applying IDS (Intrusion Detection System) prevents DDoS attacks and monitors websites traffics [37].

SQL Injection

Structured Query Language (SQL) is used to communicate with database management systems and applied in major business industries. A Structured Query Language injection (SQLi) occurs when an attacker inserts malicious SQL statements into a server that uses the SQL platform and forces the server to reveal information. The misconstructions on a database command, resulting in unforeseen consequences that include the control on a database server behind a web-application and circumvention of authentication mechanisms by allowing the attack to add, modify, delete, and retrieve records. The first and best line of defence against SQLi attacks is by applying security-driven programming practices and ensuring software developers are aware of the risks, the tools, and the techniques which can mitigate SQL vulnerabilities. Client-side input sanitization and validation should be made available for the end-user and when these validations are be bypassed, then the server-side solutions should be employed. Do not use dynamic SQL when it can be avoided and always use prepared statements and parameterized queries [38]. Proper update and patching process will prevent vulnerabilities in applications and databases.

Zero-Day Exploitation

A zero-day (0 day) exploit hits after a network vulnerability is announced but before a patch or solution provided by a software vendor or to an antivirus vendor. Attackers target vulnerability during this course of time before any parties mitigating it [39]. The zero-day vulnerability is a weakness in a computer system that may undetected by affected parties. Attackers attempt as a threat actor to penetrate or damage by compromising a system. In a Zero-day attack, the victim will don't have any defense in place and attackers may have a high level of chances to succeed. As mitigation, by applying Windows Defender Exploit Guard. This has been introduced by Microsoft in Windows 2010. Attack Surface Reduction (ASR) detects and blocks malicious, obfuscated macro code and scripting engines. Applying Next-Generation Antivirus (NGAV) instead of normal Antivirus, where traditional antivirus solutions only able to detect malware using file signatures and these are ineffective. NGAV solutions leverage threat intelligence and behavioural analytics to identify suspicious anomalous behaviour. NGAV may not detect all zero-day threats, but it can significantly reduce the chances of attacks. Patch management policies and procedures should have clear communications between the development and security team.

DNS Tunneling

DNS (Domain Name System) is a hierarchical and centralized naming system for computers, services, or other resources that are connected to a private network or internet. Almost all business industries apply the Domain Name System. DNS Tunneling is another cyber-attack method that encodes the data from other programs in DNS queries. DNS Tunneling utilizes the DNS protocol to communicate with non-DNS traffic over port 53. DNS tunneling requires the compromised system between the internal DNS server with external network connectivity [40]. DNS tunnel can be used as a full remote-control channel for a compromised internal host. Investigate queries because a compromised device might continuously send DNS queries or ping the Command and conquer servers. Since DNS service is utilized lively and difficult to block, there must IP identifier. A defender program might identify suspicious domains and IP addresses. Internal clients can be configured to send all queries to an internal DNS server only and filter all external clients or block suspicious domains. There should be periodical testing conducted. This will help us to detect suspicious domains where always be short-lived. Reporting suspicious domains to threat intelligence platforms will also help reduce the effectiveness of DNS tunneling attacks.

IV. RECOMMENDATIONS

Cyber security-related investment is like buying an insurance policy, whereby organizations need to seek the best balance between spending on cybersecurity and mitigating cyber risk. Cybersecurity programs have become a common measure prescribed by organizations towards mitigating cyber risks. Cyber risks can be managed by deploying 'off-the-shelf' IT security solutions such as the Advanced Persistent Threats (APT) system and the Security Incident and Event Management (SIEM) system. These 2 key system solutions in cybersecurity have been deployed by major organizations around the globe.

a) Advanced Persistent Threat (APT) Security System

APTs are often aimed at the theft of intellectual property. APT as an adversary that possesses sophisticated levels of expertise and significant resources to achieve its objective by using multiple attack vectors [41] (e.g., cyber, physical, and deception).

Types and the general characteristics of malicious software (malware) commonly being used as APT attack tools are: -

- Spyware - gathers sensitive information without the knowledge
- Adware - present advertisements (generally unwanted) to users
- Ransomware - extortive malware that locks or encrypt data or functions and demand payment to be made, normally by the medium of bitcoins
- Keystroke logger - secretly records user keystrokes and/or screen contents
- Rootkit - modifies the underlying operating system

Common risks associated with APT are: -

- Loss of personal information and intellectual property;
- Reputational damage;
- Financial loss (tangible);
- Contractual breach (due to materialization of abovementioned risks) of legal issues, and
- Loss of availability, i.e., business continuity issues.

Common technical security controls used to protect against APT attacks are: -

- Antivirus, anti-malware, and end-point control;
- Network technologies - firewalls, routers, switches;
- Intrusion prevention/detection system - signature/abnormal event detection and prevention;
- Network segregation - zoning off;
- Remote access technologies;
- Mobile security gateways and anti-malware controls;
- Log monitoring/event correlation; and
- Sandboxes - an environment with limited functionality.

b) Security Incident and Event Management (SIEM) Security System

Cybersecurity monitoring and real-time analysis of centralized log events is an important element of the defense. Security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM) [42]. SIM and SEM provide real-time analysis of security alerts generated by applications and network hardware. SIEM is normally procured as software, as an appliance, or as a managed service, and has been used to log security data and generate reports for compliance purposes. Typically, SIEM control sets and

associated tools are deployed to achieve a largely automated logging, interpretation, and classification of security-related (or suspicious) events. Advanced SIEM will also look for typical correlations of events indicating attack patterns or probing.

V. CONCLUSION

The cyber threats have been all-time in around as well as information systems are around us. Adequate knowledge of cybersecurity will enable effective preventive defenses in countering the threat posed. Adoption of post-breach detection capabilities which is regarded as essential, moving forward. Organizations with the right capabilities have a proactive safety net that should become part and parcel of any well-prepared enterprise. As preventive methods, organizations should ensure the adequacy of cybersecurity management by complying with all the processes, procedures, and international cybersecurity standards. It is important to cultivate everyone regarding cyber issues or cybercrime. More care as more study is important to prevent cybercrime all over the world.

REFERENCES

[1] Alex Hern, 2017, The Guardian, https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

[2] "2020 State of Malware Report", 2020. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

[3] "Most malware in Q1 2020 was delivered via encrypted HTTPS connections". June 25. 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

[4] "Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection". April 16, 2019. Kaspersky. https://www.kaspersky.com/about/pressreleases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-usersdemonstrating-the-need-for-protection

[5] "Mobile banking malware surges in 2019". July 25, 2019. Computer Weekly.https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

[6] "Malware statistics and facts for 2020" July 29, 2020. Comparitech.https://www.comparitech.com/antivirus/malware-statistics-facts/

[7] "Cyber Security Report". 2019. Checkpoint.https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

[8] "What Is Fileless Malware?". McAfee. https://www.mcafee.com/enterprise/en-us/securityawareness/ransomware/what-is-fileless-malware.html

[9] "What is file-less malware and how does it work?". Norton.https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html

[10] "Trend Micro Report Reveals 265% Growth In Fileless Events". August 28, 2019. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html

[11] "Understanding Fileless Threats" July 29, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radarunderstanding-fileless-threats

[12] "Business Email Compromise The $26 Billion Scam" September 10, 2019. FBI.https://www.ic3.gov/media/2019/190910.aspx

[13] "Email: Click with Caution". June 2019. Cisco.https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threatreport.pdf

[14] "Coronavirus phishing emails: How to protect against COVID-19 scams" 2020.https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

[15] "2019 Phishing and fraud report" 2019. F5 Labs. https://www.f5.com/content/dam/f5-labsv2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

[16] "Human Factor Report." 2019. Proof Point.https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

[17] "Phishing Activity Trends Report Q1". 2019. APWG.https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

[18] Let's Encrypt. https://letsencrypt.org/

[19] "Phishing Activity Trends Report". 2019. APWG.https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

[20] "Q4 2019 - The State of DDoS Weapons Report." 2019. A10 Networks.https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

[21] Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q3 2019" November 11, 2019. Kaspersky. https://securelist.com/ddos-report-q3-2019/94958/

[22] "DDoS attacks up 241% in Q3 2019 compared to the same period last year." November 19, 2019.Neustar. https://www.home.neustar/about-us/news-room/press-releases/2019/ddos-attacks-up-241--in-q3-2019-compared-to-same-period-last-year#

[23] "2019 Half-Year DDoS Trends Report." 2019. Corero Security.https://www.corero.com/blog/infographic-2019-mid-year-ddos-trends-report/

[24] Nadav Avital, Avishay Zawoznik, Johnathan Azaria, Kim Lambert. "2019 Global DDoS Threat Landscape Report." 2019. Imperva. https://www.imperva.com/blog/2019-global-ddos-threatlandscape-report/

[25] "DDoS Threat Report 2019 Q1." 2019. NexusGuard. https://blog.nexusguard.com/threatreport/ddos-threat-report-2019-q1

[26] "The State of Web Application Security, Protecting Application in the Microservice Era." 2019. Radware. https://www.radware.com/resources/was-report-2019/

[27] "2019 Cyberthreat Defense Report." 2019. CyberEdge Group. https://cyber-edge.com/wpcontent/ uploads/2019/03/ CyberEdge-2019-CDR-Report.pdf

[28] "Sonicwall Cyber Threat Report". 2020. Sonicwall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

[29] "Web Applications vulnerabilities and threats: statistics for 2019." February 13, 2020. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/#id9

[30] "State of the Internet / Security | Web Attacks and Gaming Abuse (Volume 5, Issue 3)." 2017-2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/sotisecurity-web-attacks-and-gaming-abuse-executive-summary-2019.pdf

[31] "State of the Internet Security | Financial Services – Hostile Takeover Attempts (Volume 6,Issue 1)." 2020. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-theinternet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

[32] Microsoft, https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1380

[33] Microsoft, https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0688

[34] Romain Fouchereau & Konstantin Rychkov, IDC, June 2020, 2020 Global DNS Threat Report

[35] Klein, Tobias, 2011, A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security. No Starch Press. ISBN 978 1-59327-415-3

[36] Van der Merwe, A J, Loock, M, Dabrowski, M., 2005, Characteristics and Responsibilities involved in Phishing Attack, Winter International Symposium on Information and Communication Technologies.

[37] Paganini, Pierluigi, 2013, "Choosing a DDoS mitigation solution…the cloud-based approach". Cyber Defense Magazine.

[38] SQL Injection, 2012, Prevention Cheat Sheet". Open Web Application Security Project.

[39] Kim Zetter, 2014, "Hacker Lexicon: What Is a Zero Day?". Wired.

[40] Son, Shmatikov, Vitaly, 2017, "The Hitchhiker's Guide to DNS Cache Poisoning" Cornell University.

[41] NIST, 2011, NIST Special Publication 800-39, Managing Information Security Risk

[42] Nowcomm, 2020, Security Information and Event Management (SIEM), https://www.nowcomm.com/siem/

[43] ENISA Threat Landscape Report, Jan 2019 - April 2020, Malware.

[44] ENISA Threat Landscape Report, Jan 2019 - April 2020, Phishing.

[45] ENISA Threat Landscape Report, Jan 2019 - April 2020, Distributed Denial of Service.

[46] ENISA Threat Landscape Report, Jan 2019 - April 2020, Web Application Attacks.