ISSN Number: 2454-2024(Online)

International Journal of Technical Research & Science

EMERGING THREATS IN CYBER SECURITY

Anukriti Raj, Arti vaish
E-Mail Id: anukriti.mhs20@sushantuniversity.edu.in, artivaish@sushantuniversity.edu.in
Sushant University, Gurugram, Haryana, India

Abstract-The growth of the Internet in the connections has led to a significant growth of cyber attack cases often with heavy outcome towards the globe. Malware is the primary choice of weapon to carry out malicious intent in the cyberspace, either by exploitation in to existing vulnerabilities or utilization of unique characteristics of emerging techniques. The development of more innovative and effective malware defense mechanisms has been regarded as an urgent requirement in the cyber security community. To assist in achieving this goal, we first present an over view of the most exploited vulnerabilities in existing hardware, software, and network layers.
Keywords: Cyber security Emerging technology trends, Emerging cyber threats, Cyber attacks and counter measure.

1. INTRODUCTION

Our society, economy, and important infrastructures have emerge as largely independent on computer networks and statistics era answers Cyber attacks grow to be greater appealing and doubtlessly more disastrousas our dependence on information technology will increase. Victims of cyber assaults also are substantially developing (11). Based at the survey performed by using Symantec which involved interviewing 20,000 human beings throughout 24 nations ,69 %. Symantec calculated that 14 adults come to be the sufferer of a cyber assault each 2,or extra than a million attacks normal. (5)

1.1 Cyberattacks flourish

It is because cyber attack search paper, convenient and less risky than physical attacks. The people who are into cyber crimes only require a few expenses beyond a computer and an internet connection. They are unconstrained by geography and distance. (2)They are difficult to identity and process due to an environment of the Internet. Given that action against information technique system are very attracting ,it is expected that the number and sophistication of cyber attacks will keep growing:

- Confidentiality is the term used to prevent the disclosure of statistics to unauthorized people or systems.
- Integrity is the time period used to prevent any change/deletion in an unauthorized manner.
- Availability is the time period used to guarantee that the structures responsible for delivering, storing and processing statistics are handy while wished and by individuals who want them. (3)

Many cyber protection professionals believe that ware is the important thing choice of weapon to carry out malicious in tends to breach cyber security efforts in the cyberspace. (4) Malware refers to overseas magnificence of assaults that is loaded on a machine, typically without the know-how of the valid owner, to compromise the systemt the gain of an adversary. Some exemplary classes of malware encompass viruses, worms, Trojan horses, adware, and botexecu tables. Malware infects structures in a spread of ways for examples propagation from infected machines, tricking person to open tainted files, or captivating customers to visit malware propagating (13)
Websites. In greater concrete examples of, malware might also load itself on to a USB power inserted into an infected device after which infect each other device into which that tool is subsequently inserted. Malware might also propagate from devices and equipments that containe embedded systems and computation allogic. In Malware evolves thru time capital in gonne approaches and exploiting the failings inside the rising technology to avoid detection. We describe more than a few of recent patterns of malware attacks gift in the emerging technologies. In choosing emerging technology for illustration, we cognizance some that have changed the manner we stay our daily life. (6) These include social media,cloud computing, clever cell phone generation, and critical infrastructure. We discuss precise traits of each of the seem erging technology and the way malware utilizes the unique traits to seasoned life price itself.
For instance, social media, such associal networkings it esand blogs, are now an fundamental a part of our way of life as many people are journaling approximately their existence activities, sharing news, as well as making pals. Realizing its ability to attach hundreds of thousands humans at on ego,adversaries use social media money owed to befriend unsuspecting users to cars for sending unsolicited mail to the victim's friends while the victim's gadget is repurposedin to a part of botnet. brief, malware can be inserted at any point within the gadget existence cycle. (7)
Finally, we provide our speculative observations as where destiny studies course proportion heading.The encompass:

- Privateness concerns to safe shield increasing volumes of character all in formation entered inside the Internet.

- Requirement to have an era of at ease Internet from scratch with careful consideration of the subjected boom and usage patterns which changed into no longer the case with the net we use nowadays,
- Trust worth device whose fundamental architecture isn't the same as their inception to with stand from involving malware.
- Being capable of identify and trace the source of attack assisted via the development of global scale identity management gadget and hint returned strategies, and
- A strong emphasison usable protection to offer individuals security controls they are able to recognize and manage.

The the rest of the article is prepared as follows.

- Section 2 provides an in sigh of the malware.
- Section 3 gives an over view on how malware penetrates in exiting systems and efforts to mitigate any present vulnerabilities exploited by using adversaries.
- Section 4 evaluations emerging techniques to malware infiltration and discusses the overall assault styles and methods.

2. EXPLOITING EXISTING VULNERABILITIES

Once malware is carried out to the victim's system, cyber criminals could utilize many different aspect so existing vulnerabilities in the victim's system further to use the in their criminal activities.We examine most commonly exploited existing vulnerabilities in hardware, software program, and network systems. (11)

3. EMERGING THREATS

Cyber attack on cyber space evolve through time capitalizing on new approaches. Most times, cyber criminals might alter the prevailing malware signatures to take advantage of the flaws exist inside the new technology. In other many cases ,they simply explore unique characteristics of the new techniques to find loop holes to inject malware. (15). Taking benefits of new Internet technologies with millions and billions active users around ,cyber criminals utilize these new technologies to reach out to a vast number of victims quickly and efficiently. We select four such up and coming technology advancements which include: social media, cloud computing,smart phone technology,and critical infrastructure, as illustrative examples to explore the threats in these technologies. (11)

Table-4.1 Emerging technologies: there common characteristics and common attack pattern

Common Characterstics	Common Attack patterns
Millions and billions of active users	Increased attack through web browser
Became part of our daily life	Increased attacks thrpugh social engineering websites
No geographical boundaries	Increasing attacks coming from non PC based devices (e.g. mobiles, tablets, Volp)
Accessed 24/7 from anywhere at anytime	Increasing number of more organized attacks through botnet
Services are available via internet connection using web browsers	Increasing number of attacks through the attackers with internal knowledge (i.e. inside threats)
Services offered by many different devices such as mobiles and tablets	

CONCLUSION

This survey cognizance on elements of facts machine:know-how vulnerabilities in exiting technologies and emerging threats in up and coming development inside the telecommunication and information technology around the globe . Growing threats were found in emerging technologies, which includes social media,cloud computing, smart telephone technology and vital infrastructure, frequently taking gain of the particular traits. We defined characteristics of each of emerging technology and diverse manner small ware being spread within the new technology.Then,we discuss commonplace set of preferred assault styles observed within the rising technology.

REFERENCES

[1] http://www.maawg.org/,lastaccessed:June2013.
[2] http://www.antiphishing.org/,lastaccessed:June2013.
[3] http://www.ostermanresearch.com/downloads.htm,lastaccessed:June2013.
[4] http://en.wikipedia.org/wiki/Mebroot,lastaccessed:June2013.
[5] http://www.emailtrackerpro.com,lastaccessed:June2013.
[6] http://www.tamos.com,lastaccessed:June2013.
[7] https://www.mandiant.com/resources/download/web-historian,lastaccessed:June2013.
[8] http://www.majorgeeks.com/index.dat_analyzer_d5259.html,lastaccessed:June2013.

[9] http://www.winpcap.org/,lastaccessed:June2013.
[10] http://www.riverbed.com/products-solutions/products/performance-management/wireshark-enhancement-products/Wireless-Traffic-Packet-Capture.html,lastaccessed:June2013
[11] http://shibboleth.internet2.edu/
[12] Australian Parliament the report of the inquiry into Cyber Crime
[13] http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf
[14] www.it2trust.com/pdf/Aladdin.SafeWord_PO_SafeWord.pdf