



International Journal of Engineering, Business and Enterprise Applications (IJEBEA)

(Open Access, Double Blind Peer-reviewed, Refereed and Indexed Journal)

www.iasir.net

A Review Paper on Discrete Online Attacks

Aakanksha Chopra

Assistant Professor, Department of Information Technology,
Jagan Institute of Management Studies (JIMS), Rohini, New Delhi-110085, INDIA.
Affiliated to GGSIPU, Dwarka Sector-16C, New Delhi, INDIA

Abstract: Volumes of information which is available today needs to be protected and fostered against distinct categories of attacks such as- deliberate hackers, displeased current or former employees, interested computer neophytes, sneaky vendors. Oodles of online attacks are occurring and this is potentially the massive threat today. Earlier there was the time when Information leakage was speculated to be the largest risk and which could lead to manipulating data; but, still, could be avoided. Today, the scenario has completely changed breach in security and the diverse attack capabilities of infiltrators are increasing which is leading to high-security threats. This paper is a review paper on various types of online attacks, what is cyber crime hierarchy, what are Security insights across 4 key areas namely- Trust, Threat Intelligence, Industry, and Recommendations.

Keywords: security-threat; online attacks; cyber crime; security insight; security breach.

I. Introduction

Back in 2013, Tom Simonite wrote in an article named- "Web ads are used to launch online attacks", that it is very easy to hide code in online ads that can run people into an online attack squad. He explained how online advertising networks could be used to attract millions of innocent web surfers in intrusion on websites [6].

According to an Article written by Illena Armstrong named- "Let's just call it The era of IT Security." Illena stated that frequent and massive data breaches have impacted millions of private citizen's personal information loss by theft. Hacktivists and other cyber vigilant's increasingly have targeted various groups and corporations. It also states 2014 as "The year of Data Breach", with which the impact of cyber attacks are getting personal [7].

In an article "Cyber Security Predictions in 2016," Sidharth Shekhar wrote that with the huge amount of people being online or having access to computers or tablets or connected devices, cybercrime has evolved and is more complex than ever.

According to KPMG cybercrime security report 2015- "India continues to be an attractive option for hackers. Cyber Crime in India has increased immensely in 2015, with 72% companies accepting that they faced online attacks and 94% respondents indicated that cybercrime is a major threat faced by Organizations [8]."

II. A Statistical Report By CISCO

According to CISCO 2014 Annual Security Report- "the biggest problem today is of TRUST." The attackers and malignant users are exploiting the trust of user's in system and people in business they interact with on the day-to-day basis.

Ample proofs are there that these vicious attackers are coming up with new styles of embedding their malware in a network, stealing data or spoil critical systems. They also remain undetected, untracked for the longer period of time.

According to this report, networks are facing two form of trust corruptions-

- a. Firstly, depreciating customer morale in the integrity of products.
- b. Secondly, malicious attackers are defeating trust mechanisms, thus calling into question the effectiveness of network & application assurance, authentication, and authorization architectures.

This report concluded with Security insights across 4 key areas described as follows-

- a. **Trust-** all the organizations should be concerned about finding the right balance of trust, transparency, and privacy because much is at stake. There are three pressures on security practitioners in this area who are helping their organizations to maintain a balance-

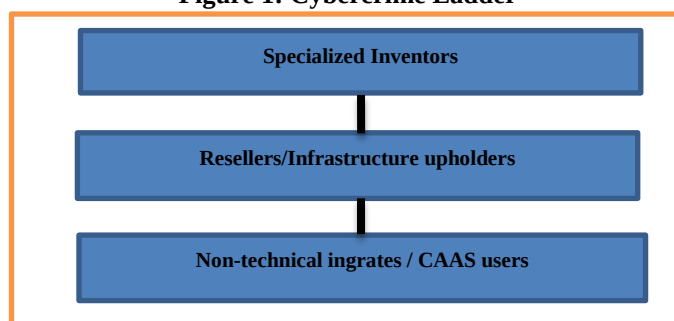
- i. **Greater attack surface area-** The attack surface has increased exponentially and is still expanding. Data is no more a data it has become a currency. If data is a "street value" and if data is most wanted it is definitely at "Risk." If the value of the target is greater than the risk of compromising it, it will be hacked.
- ii. **Proliferation and Sophistication of the attack model-** The simple attacks have given way to modern cyber crime operation that is illusionary, financed, and capable of provoking major damage to the organization.

- iii. **The complexity of threats and solution-** today's network goes beyond traditional boundaries, and constantly evolve and parent new attack vectors like mobile devices, web-enabled & mobile applications, social media, web browsers, home computers, etc. This makes controlling information security even more difficult for security teams.
- b. **Threat Intelligence-** using largest set detection telemetry CISCO and Sourcefire together have analyzed & assembled security insights from the past years-
 - i. Attacks on infrastructure are targeting significant resources across the internet.
 - ii. Malicious actors are using trusted application to exploit gaps in perimeter security.
 - iii. It was observed that network penetrations remain undetected over long periods.
- c. **Industry-** CISCO investigators observed that security is affected by many practices around Industry. Practices like brute-force login attempts, large-scale DDOS activities and ransomware efforts to the growing relevance on the cloud, lack of security & other concerns.
- d. **Recommendations-** This section covered how a threat- centric security model enables defenders to address the full attack continuity. In order to leave the security threats behind the organizations need to examine their security model before the attack, during an attack, and after an attack.

III. Cybercrime Hierarchy

Due to security gaps the cybercrime network is expanding, strengthening & increasingly operating like any legitimate, sophisticated business networks- At the bottom resides the Non- technical ingrates or Crimeware- as-a-Service (CAAS) user. Then in the middle comes the Resellers or Infrastructure upholders. Lastly at the top of the hierarchy resides the Specialized Inventors.

Figure 1: Cybercrime Ladder



Many actors in the so-called "Shadow economy" also now send surveillance malware to collect information about an environment, including what security technology is deployed, so they can target their attacks. Malware is delivered to users accessing the mainstream websites. Spam emails from well- known companies contain malicious sites. Third- party mobile applications laced with malware & insiders using information access privileges to steal intellectual property from employees.

There should be an assumption by all users that nothing in the cyber world can or should be trusted. The need for confidence in security has helped for an advancement of the common criteria for Information Technology Security Evaluation, which is a language and framework that allows govt. agencies and other groups to define the requirements that technology products must meet to assure that they are trustworthy.

IV. Types of Online Attacks

1. **Denial of Service-** "DoS" is an attack that is not targeted at gaining access to a network or system. Instead, it aims at disrupting the service of the network or system under attack by flooding it with more information or service requests than it can handle.

It is difficult to trace as DoS attack can be initiated at one or multiple sources. This happens in Distributed Denial of Service ("DDoS") attack- in which a single attacker consciously introduces DoS attack programs into dozens or even hundreds of other systems by various techniques of online attack. The attacker then simultaneously initiates all those DoS attack programs to bombard the target network or system.

Distributed denial-of-service (DDoS) attack has been one of the most regularly in the works attacks that badly intimidate the stability of the Internet. According to CERT Coordination Center (CERT/CC)[1], there are mainly three categories of DDoS attacks: flood attack, protocol attack and logical attack which needs to be taken care of [1].

2. **Spoofing Identity-** is a method by which user's data is accessed in an unlawful manner and is used against that user for authentication purpose. The information of the user like username, passwords, OTP's is used. Basically, malicious users try to become an authentic user illegally which they are not in reality.

3. **Hijacking-** Hijacking is an attack in which a connection is stolen after a victim has authenticated himself or herself to the system. Once it is done any malicious act could be performed on that connection. The victim may be aware that the connection is hijacked. Hijacking attacks generally take place on a remote computer (e.g., a customer's personal computer), although it is sometimes possible to hijack a connection from a computer on the route between the remote computer and the banks' internal systems.

4. **Random Dialling or War Dialling-** It is a technique where an attacker sequentially or randomly dials every number on a known telephone exchange with the objective of detecting modems that bypass network firewalls and other security measures. By this, an attacker can gain access to the networks through the modems.

5. **Back Doors or Trap Doors-** back doors are basically the programs which are written into operating systems or applications so that programmers gain access to the programs without going through security checks. Back doors may extract some special sequence of inputs or are run from a user ID which is then granted special access rights accordingly. Back doors are used by the Programmers to obtain quick access to expedite debugging or monitoring of the programs that they are developing.

The problem occurs when the programmer forgets to withdraw a back door after debugging. Further, an attacker can create a back door after gaining access to an account for his future access.

6. **Brute Force-** Brute force attack is a process of capturing encrypted messages, and then by the use of a software it decrypts the encrypted message and gains access to it. It may extract user IDs or passwords. If the attacker gains access to a user ID that has sufficient privileges, he can create a back door (see point 5 above) for future access, even if the password of the user ID is subsequently changed.

7. **Exploiting known security vulnerabilities-** Attackers may exploit known security flaws to gain unauthorized access to a particular system. For doing this they make use of automated tools to probe particular systems to identify security weaknesses. The Internet is an important source for such information. Certain security vulnerabilities would allow intruders to modify the content of web pages, mishandling firewall, etc.

8. **Social engineering-** Social engineering is a technique to gain information or access using social techniques. An attacker may claim to be someone authorized to access the system and attempt to reveal victim's user ID or passwords, or even request the set-up of a new account for the attacker himself. Social Engineering is a method of gathering information and performing attacks against Information and Information Systems [2]. A social engineering attack targets this weakness by using various manipulation techniques in order to elicit sensitive information. [3]. An attacker may also call the organization's help desk acting like an authorized user to gain information about the system (e.g. requesting the help desk to change the original system password to one given by the attacker).

9. **Passwords Guessing-** Guessing passwords is a process to test all possible combinations to gain entry into a system or network. This is done using a software. Some attacks speed up this process by trying commonly used combinations first (e.g., words in dictionaries).

10. **Viruses-** Computer viruses are computer programs that may be embedded in other code and can replicate themselves. They may result in destructive outcomes in system or networks once they are active. The virus program may be part of mail attachments, may move internally and destroy data files, or devices on a system and spread through multiple other systems in a network.

11. **Trojan horses-** Trojan horses are programs that contain additional (hidden) functions that usually allow unintended activities such as gathering information or performing furtive acts to gain control of the system, without any disruption to normal transactions. To allow an unrestricted access to a system Trojan horses can be attached to e-mails and may create a back door (see attack 5.) The major drawback is a program may automatically exclude logging and other information that would trace the intruder.

V. Conclusion

With the complexity of threats and corresponding solutions at an all-time high, organizations need to rethink their security strategies. Instead of relying on point solutions they can minimize complexity by continuously integrating security into the network itself so the network can firstly, continuously monitor and analyze files and identify subsequent malicious behavior whenever it may begin. Secondly, help organizations scale enforcement, expanding the surface on which network device can be placed. Thirdly, accelerate the time to detection because it can see more traffic. Fourthly, give organizations ability to aggregate unique context awareness that is not possible to obtain by relying on security-specific devices alone.

References

- [1] Saurabh Ratnaparikhi, Anup Bhangre, "DDOS Attacks on Network; Anomaly Detection using Statistical Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, pp.: 321-326, Volume 2, Issue 12, December 2012, ISSN: 2277 128X, Available online at: www.ijarcsse.com
- [2] Anubhav Chitrey, Dharmendra Singh, Monark Bag, Vrijendra Singh, "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model", International Journal of Information & Network Security (IJINS), pp.: 45-53, Vol.1, No.2, June 2012, ISSN: 2089-3299.

- [3] Francois Mouton, Mercia M. Malan, Louise Leenen, H.S. Venter, "Social Engineering attack framework", Information Security for South Africa (ISSA), 2014, Publisher: IEEE, Electronic ISBN: 978-1-4799-3384-6, CD-ROM ISBN: 978-1-4799-3383-9, DOI: 10.1109/ISSA.2014.6950510
- [4] Zainal Fikri Zamzuri, Mazani Manaf, Adnan Ahmad, Yuzaimi Yunus, Book- "Chapter 30- Computer Security Threats Towards the E-Learning System Assets", Software Engineering and Computer Systems, Publisher- Springer Berlin Heidelberg. Second International Conference, ICSECS 2011, Kuantan, Pahang, Malaysia, June 2011 Proceedings, Part II pp- 335-345, DOI-10.10007/978-3-642-22191-0_30, Print ISBN-978-3-642-22190-3, Online ISBN-978-3-642-22191-0.
- [5] Shah Mahmood, "Chapter 2: Online Social Networks: Privacy Threats and Defences", Security and Privacy Preserving in Social Networks, R. Chbeir and B. Al Bouna (eds.), DOI 10.1007/978-3-7091-0894-9 2, Springer-Verlag Wien 2013
- [6] "Web Ads Used to Launch Online Attacks" by Tom Simonite, August 1, 2013, MIT Technology Review, Online available at: <https://www.technologyreview.com/s/517751/web-ads-used-to-launch-online-attacks/>
- [7] "Lets just call it The era of IT Security" written by *Illena Armstrong*, December 14, 2015 in SC Magazine for IT security Professionals. Online available at: <http://www.scmagazine.com/lets-just-call-it-the-era-of-it-security/article/459493/>
- [8] "Cyber Security predictions for 2016", by Sidharth Shekhar, in DATA QUEST magazine Online available at: <http://www.magzter.com/articles/93/146996/569fc1fb60a9f>