Introduction to Cyber Security

Assignment 1

Automation and Integration In Cyber Attack And Defense

Student ID : IT19208268

Name : Poobalan A.V

Year 2 sem 1

weekday

Table of Contents

Abstract

This report mainly is comprised by two main topics automation and integration in cyber-attacks and automation and integration in cyber defense. Automation and integration in cyber-attacks include the history of performing automated cyber-attacks and the future of automated cyber-attacks using machine learning and further with the help of artificial intelligence. As much as cyber-attacks being automated the defense has always needed a generous amount of input from a cyber security specialist to plan, analyse, detect, mitigate and counter-attack or trace down attack source. The idea and measures taken to automate defense which requires immense efforts in machine learning and Artificial Intelligence always has been a hindrance. Despite barriers certain firms have initiated automated defense or systems that could counter automated attacks is further described and elaborated. Cyber-security industry which has so far used human input and human intelligence in its field will be affected due to automation and integration of cyber defense systems is also included in the latter of the report.

Despite the topic going hand in hand it does not translate that automated cyber defense is the only countermeasure for automated cyber-attack, it is one efficient way which still requires human input if otherwise being handled by artificial intelligence.

Introduction

Automated cyber-attacks have been in the field of cyber security almost since inception of attacks. This form of attacks is called worms. Worms can still be found vastly in the field of cyber-security till to date and will still remain the classic form of attack in the future. If attacks were clumped into generations based on their capacity and origin, Worm attack sits on the first generation of cyber-attacks. In the said classification falling into the second generation of automated cyber-attacks will be botnets. Although several countermeasures have been found to detect and mitigate bad bots, botnets are not yet out of the scene. The use of botnets still remains as one of the major forms of attack and there is foreseen significant improvement in the botnet technology in the future. Taking position at third generation automated cyber-attacks would be imitation attacks. This current trend of cyber-attack forces the loss of integrity on people. The future of automated cyber-attacks depends on artificial intelligence. There is no solid evidence that there is existence of AI powered Cyber Attacks.

Although automated attacks have been in the field of cyber-security for quite a while the emergence of automated defense in the field of cyber security was quite recent. The implementation of automation for defense requires a massive support of machine learning since the type of attack differs from attack to attack. The implementation of automation in the field of defense gets rid of the extra effort and time taken incase an organization faces a cyber-attack. However, the automation in defense works in two stages in detection and countermeasures. Machine learning helps the detection system an edge over the attack and trigger the prevention system perform its countermeasures.

Manual combat against attacks against organizations can be tough the requirement of an automated measure is necessity but the necessity will not be functional if the system is not built on correlative data, if the system does not trigger protective measure faster than the attack, if the system does not implement the selected triggered countermeasure faster than the attack or if the system is not capable of detecting existing infections in the system. When detection system satisfies the above conditions technically its capable of tackling automated cyber-attacks.

Why automation is the key to cyber-security

Manual attack prevention requires a cyber security professional handling the situation but this situation in simple words is a man against machine since most of the cyber-attacks are automated. This situation pushes the situation to be high risk because the cyber security professional as a human has a possibility to lose control halfway of preventing from the attack however when a machine counter-preventing this situation against a machine has an edge over the human i.e. the right tool against the right type of attack. This would enhance the process of taking the situation under control. The next downside of using manual attack is that it causes the organization to have less trust on the professional handling the situation. The usage of an automated form of protective measure in the field of cyber defense gives an extra level of confidence to the organization sourcing it. Since the days have changed and there is a significant higher trust on technology than on people.

The process of automation ensures that there is less worry of the development in technology might cause new methodologies of attacking the vulnerabilities of the system. Since machine learning helps learning the entire system and has knowledge on the vulnerabilities of the system if proper counter-attack prevention and protection schemes are implemented there is not much worry on the system since the machine already is fed the knowledge compared to human intelligence on under pressure. Compared to a group of people working during a cyber attack have different levels of capacity of their own and as human beings they tend to break down in situations under pressure, in comparison having a group of systems that work together have a very less probability of a technical breakdown and the capacities of the individual systems doesn't differ from one another, the uniformity in the capacity of the system re-assures to trust automated systems over the use of human intelligence.

With all the added advantages the organizations have higher efficiency financially by saving money from hiring professionals, the expense of setting up an automation defense system is considered a capital expense organizations tend to appreciate the step. Technical efficiency too is comparatively very high using the automated systems. Technical efficiency increases since there is very less errors caused by systems than by individuals. Additionally, machine learning helps in better decision making of the system since cyber attacks immediately causes disrupt in the functions of an organization there is immense pressure on the team working on it. When the attack is on execution or on spread the professionals without any knowledge on the system have very less idea on how to proceed ahead this situation leads to bad decision making by the individuals. On the contrary having a system provided with all the knowledge has very less chance on failing at decision making. for example, if the program senses an attack to the data of the system the automated protective measure could be to trigger an immediate backup of sensitive data and destroy available content from the reach of the attacker. At such situations the system has a slight edge over human decision making.

Down side in using automation in the field of cyber security.

The automation of system requires machine learning a huge chunk of correlating data related to attacks and its countermeasures this system has a high chance in going wrong in the situation of a slight misinformation given to the system while on the build. No system function as a whole package the idea of preventing from all types of attack is too broad to fit in a system since there is uncountable ways of performing attack and each system has its own vulnerabilities and threats. Provided this situation a one size fits it all type of automated defense system is still a dream.

Although systems are efficient and has won the belief in the usage compared to humans there is a higher risk in the technical physical structure of the system. The system has a disadvantage that it at times might not function at all during situations like physical damage. One major disadvantage is that the system itself might have its vulnerabilities to be exploited and make look like a dummy during such situations human intelligence and support is highly required.

Since each system is tailor-made there is high chances that the system has its loopholes while integrating the system in its actual environment such loopholes may cause the data of the organization to be vulnerable than without a system. The system has to have a vast knowledge on the users the environment the type of attacks it most likely will face the counter measures protection schemes etc. this particular reason was the reason behind the lag of creating automated defense systems. It pushed the people to a situation of close to impossibility that such systems cannot exist. With all the advantages the organizations opt for a semi-automatic system where there is cyber security professional handling an automated system.

The implementation of such systems has a huge impact on the people who are in the field since there will be an industrial shift from manual protection to building security systems. This sector is new to the industry and the pros and cons are not yet seen in practice or the consequences or results are not definitive. Despite being not definitive it clearly shows the indication that this is the way forward for the cyber security industry.

What caused the transition to automation

The IT industry has been on an ever growth since its inception. The current trend of machine learning artificial intelligence and quantum computing is being on the rise and such technologies are already taken its stance in being used in cyber-attacks but in the field of defense there is a significant setback in the usage of such technologies that is on the trend. This situation gave an edge to the attackers who were able to utilise such technologies and perform their intended attack. Since now the situation is fight fire with fire the security industry is using the technologies to embed into systems that can counter the attacks in the field of defense.

Additionally, the introduction of IoT (Internet of Things) has completely expanded the domain of attack that the attackers and attack. Since IoT gives internet access and control to its functions to everyday objects that we use this completely expands the zone to attack. This situation raised in the question where do we implement security for this expanded zone? Can the industry afford to provide such high number of professionals to the field of IT?

Being the trend in the field of IT, Cyber Security lacks the ability to fulfill all the security requirement of every individual expecting security with the expansion of attacking domain. The setback in the technical ability and the excessive demand for security and sudden growth of attacking domain the industry is forced to make the move of developing the automation defense system.

The development in the field of IT that gifted the world with internet opened the gate for anybody to reach anyone who is in the web. This significantly increased the number of cyber criminals in this world from cyber bully to cyber fraud to extreme industry targeting attacks such as DDoS attacks worm transfers to network etc. which caused the industry to force security as a compulsory requirement. Over the years the attackers are matured and attacks are grown and mutated and is highly advanced in the current time that uses advanced technology.

It is the industry's responsibility to cater to the need of security since it has turned into a mandatory requirement in the field of IT. As stated previously organizations tend to set their beliefs high on machines and systems than that they have on people. This forces the industry to lessen the number of personnel involvement and allow higher usage of machines and systems to handle the critical task. Although the transition has its benefits the downsides are mentioned the organizations prefer a capital investment than recurring investment so that the expenses can be used elsewhere. In a IT firm for example, it has a significant advantage since there will be less attention to be paid to the security aspect more effort and time will be spent on the development aspect.

The industry's decision now wasn't an option mostly was a decision that evolved to take it position now as autonomous defense system will hit the market to counter combat cyber-attacks from attackers which is believed to be a healthy fight.

Worm as automated Cyber attack

Worm as mentioned earlier falls under the first generation of cyber attacks. Worms are stand alone computer programs that hold a malformed code embedded. Worms have a recursive function that replicates itself and spreads itself within a system infecting all the systems in the network. Worms as attacks is used to spread through the system and is considered to be automated since once transferred the rest of the activities will be completely carried out by the program since it's the beginning of any attack once spread in the network it has the ability use up all bandwidth in the network. Mostly worms carry a payload with it this may cause unexpected trouble in the victim's network.

Some famous worms such as "code red" was a backdoor program containing Trojan horses that was spread through a worm to a network. Another such example is "Nimda" Nimda is admin spelt backwards this was an indication that suggested that it is targeted towards the admin privileges of a system. What the actual worm performed was to exploit vulnerabilities in the system to attack. Some worms which were automated to do more than just deny service was "ExploreZip" worm. The explore zip worm once into the system begun to encrypt files in the system that were important to an organization and used it as the base for the ransomware attack. Demanding ransom in order to remove the encryption from the infected files. The ILOVEYOU worm which was used as a phishing attack to trick user into running a malformed code were all such examples of how automation was a major part of automated attack.

Worm entirely is not faulty. There are worms that are made with good intent. Those worms are called as anti-worm. There were worms such as XSS worms that was used to study how worms spread and to counter Code Red worm in the mode of combat two worms namely Blaster and Santy worms were used. A special worm was used in windows operating system as a security measure that is Welchia. This particular worm gets transferred through the network like any other worm. Once the worm is infected it starts execution and its intention was to automatically download and install certified windows security patches to the device without the consent of the user.

Automation to defend such situation would be the usage of advanced directory control I the switches and routers. Once the advance directory control is active there is rules and regulations on each port number and IP addresses that are available on the system. Other automation techniques might be implementing extra levels of packet filters filtering out what comes in and goes out of the system. One other technique would be nullrouting or black hole networking. Monitoring all the lost traffic and dropped traffic which mostly is used by the attacker to inject the worm in to the system would help trace back at the attacker.

However, such measures only work after the detection and realization of such a worm exists. The automation process should actually begin at detection the system should be able to sense the malformed code at the beginning. But, if the worm was transferred as a message from a device to device the intervention of the system to check for malformed code will break the integrity.

Botnets as Automated Cyber attack

Botnets falls under the second generation of autonomous cyber-attacks. Following the worm and its first introduction in 2003.

Botnet is a number of interconnected devices having bots working under them that as a whole causes distributed denial of service on a specific network and steal data from the systems. Usually there is one commanding computer that has command and control (C&D) over the taken over computers and devices that provides its resources to the commanding computer and the specific devices functions as robots. That's how the name was found. Such technology in attacking now moving into the new domain of attacking such as Internet of things have made it more vulnerable. Such as a distributed denial of service on a person's home that is controlled by internet of things has the possibility that the person is completely locked in or out of his premise or it might increase the possibility of theft and burglary.

Botnets are also one of the major threat to autonomous vehicles and vehicles that has an onboard computer to control its functions. Such systems are more vulnerable since it might cause in worst case scenario death or fatal accidents in traffic.

The process of taking over systems into custody for acting as slaves are of different ways one such way is telnet it forces devices to be connected with the commanding server where a malicious code is executed on the client devices which later turns into a slave of the commanding computer. Another way of doing it was through IRC networks which uses comparatively lower bandwidth to do the communications within the network of bots that together performs distributed denial of service, one such bot that is very well known and well popular is the maxite bot.

Other methods also include peer to peer, since irc networks can be taken down in some time there is less time to function hence the decision of peer to peer, this requires public key cryptographic mechanism which in turn has caused an extra level of effort requirement either to build or break it.

There are some botnets that prefer domains than any other since it comes with an advantage of easily handling all the bots in the network. It gives an extra level of control. Therefore, large botnets such as Rustock and srizbi used the technology.

Such botnets can be mitigated autonomously through anti-bots. Anti-bots must have huge filtration techniques that would allow only approved requests to reach the server. This would significantly reduce the number of requests handled which would help the server from being faced with distributed denial of service.

Imitation attacks as automated cyber-attack.

Imitation attacks fall into the 3rd generation of attacks that imitates the behavioral pattern of certain individual and using his credentials displaying an imposter figure in the internet arena for criminal activities. This is a combination of attacks that steals user details that is mostly used for identification such as using spear phishing techniques to capture credentials and capture biometrics that will be later used as proof.

This practice mostly affects the ecommerce industry since the organization has no proof of the actual person on the other end. Using the credentials online banking activities that leads to financial fraudulent activities and account takeovers and money transfers are worst outcomes of this version of attacks. These automated imitation attacks have reached a new level with the development of technology and field of cinema and art.

One major development in the field of cinema was deep fake. Deep fake is a technology that can graphically mimic an actual user in real-time. This has made famous people more vulnerable to be attacked. Since these are used in the place of verification the source where such forms cannot be easily identified. This is an added advantage for people performing this type of attacks.

Mitigation of such attacks has not yet been found or there is no method of prevention technologically. The only solution to such situation is to follow old school methods to be physically present for verification. Since it cannot be considered an advancement in the field of technology the solution cannot be accepted as a valid solution top such problems.

Maybe once there is artificial intelligence successfully implemented there would be a solution to imitation attacks or deep fake as an attack.

The future of cyber-attacks

The future of the IT industry completely relies on machine learning and artificial intelligence. The entire arena of how security or attack will be functioning is quite unimaginable as its well known that artificial intelligence is possible after quantum supremacy.

One major threat of the future in the field of cyber-attacks would be AI fuzzing. AI fuzzing is a system that is based on machine learning poisoning that helps development companies identify vulnerabilities in the system. Fuzzing is a technique that has been in play for a long time but comparatively a very hard job to do but with the help of machine learning this takes away a significant amount of work load from fuzzing. This is actually a good development step useful for vendors. Since this has the ability to identify vulnerabilities this can be used on the darker side to be used as a tool to detect vulnerabilities in the victim's system with the help of this tool and exploit the entire system.

Machine learning is the way forward in the entire IT industry that fact is considered undeniable. Although being the base of artificial intelligence machine learning is too considered vulnerable with a new threat directed towards it which is called machine learning poisoning. Machine learning depends on the collection of data and gains knowledge by experience and the usage. Once the data is collected the system uses the data to develop or use the existing mathematical algorithm to find a solution to the user's problem. Machine learning poisoning feeds in false data to corrupt and mislead the system. There are 4 different threats in this section that is corruption of logic, manipulation of data, data injection, learning transfer. Out of the logic corruption is considered to be the worst threat that sends malicious code into the system that will change the logic of picking the algorithm that the system would use to pick to solve the problem. This although doesn't change the data, it will force the system to give a wrong output. Data manipulation and data injection goes hand in hand this data once moves into the system will force the system to give a not intended output. Since machine learning makes decisions on the data provided, the system will suffer wrong outputs if injected with false information or false data.

Last but not the least is called the machine transfer. This particular attack doesn't change any output or doesn't feed any false data. Once in the system the program will study how the machine learning functions such as what type of algorithm it picks and what type of data it handles and what output it gives in certain situations. These are valid and resourceful data in the world of IT this translates directly into a similar form of crime in real world called the knowledge theft.

These kind of attacks are completely new in the field of IT. Therefore, there is no proper solution that is available so far to mitigate prevent detect or counter attack In such situations. The only possible answer so far is that with the introduction of complete artificial intelligence there will be a proper solution to all the above mentioned future automated threats.

New technologies battling automated attacks

Automated Incident Response Solution, This system battles the artificial cyber attacks with the help of artificial intelligence that alerts authorities and professionals and the organization if faced with a cyber attack. This significantly decreases the response time. The system also comes with immediate security procedures that would be triggered. This helps prevent the attack from spreading since there is swift action as response acting on the system the security measures spread faster than the attack and prevention schemes works faster than the attack.

Most attackers use the time of reaction to their benefit to take the system under their control since the most significant problem is off the table the response team can work on the progress of the protection and countermeasures of the system or network.

A new emerging field is Integrated adaptive cyber defense. Such systems that has a security procedures and protocols embedded and automation active that helps organization fight back during a cyber attack. This a part of rapid cyber defense operations that improves efficiency of the system and the team.

How to avoid or refrain from automated cyber attacks

The usage of multi factor authentication. Usage of multi factor authentication gets rid of a significant amount of phishing and cyber attacks. Multifactor authentication includes a combination of lot other verification and authentication that could be possible only if the actual user attempts to be verified. Although a preplanned individual attack may surpass this barrier, but in most cases this has always been a good solution

Generally there are five steps to follow in setting up an automated defense system that defends automated cyber attack. Starting off from automated ingestion. This helps in developing machine learning since there is various methods of attacks this part of system will record how the attempt was attempted and how it was performed based on this information this system would not allow similar attack to replicate in the future.

Then the flow moves to stacking this is a system that stacks the information such as ip address, host id etc, to help not replicate any further attempts or deny access to that specific device.

The next obvious step is using enriched technology. As defending systems that echoes security comes at a price the system must use multiple tools and huge amount of resources generously to mitigate and counter attack. If offenders can use the sweet of technology to offend. Defense system must follow the same procedure and fight fire with fire.

The most important two steps would be Decisions and actions. Based on all the data collected through the help of machine learning and decision making ability the system must pick the best form of counter measure for the incident.

Conclusion

Automation is one key development feature in the field of information technology. People prefer manless effortless situations. Although the topic is divided into defense and attack automation in attack has been in existence for a long time but automation in defense is just rising into play but comes with a significant advantage.

With the development of the industry in the field of internet of things and the emergence of fields like quantum computing and artificial intelligence the need for security is highly uprisen. In current days with all the sweet of technology and information being wealth and the field of cyber security not fulfilling the actual demand there is a high need of automation in this field. Once the field is completely taken by automation maybe the professionals in the field of cyber security may suffer from over supply.

Given all that information there is quite a problem in completely automating since there is always a requirement of human intelligence at least to guide the automated system. With all that information still there is all threats coming towards the field from automated systems or automated programs, there is a need to fight fire with fire. Hence, the requirement of automation In the field of cyber defense.

With Artificial intelligence and machine learning in development the future is more likely on the unpredictable side since the its mostly like the 4^{th} dimension—explanations there understanding isn't.

References

"Thingbots: The Future of Botnets in the Internet of Things". Security Intelligence. 20 February 2016. Retrieved 28 July 2017

Barwise, Mike. "What is an internet worm?". BBC. Retrieved 9 September 2010

"Security of the Internet". CERT/CC

"Distributed Denial-Of-Service". www.garykessler.ne

Top 5 best practices to automate security operations - Microsoft Security", *Microsoft Security*, 2020. [Online]. Available: https://www.microsoft.com/security/blog/2017/08/03/top-5-best-practices-to-automate-security-operations/.

"Multi-Factor Authentication Blocks 99.9% of Automated Cyberattacks", *HealthITSecurity*, 2020. [Online]. Available: https://healthitsecurity.com/news/multi-factor-authentication-blocks-99.9-of-automated-cyberattacks. [Accessed: 30- Apr- 2020]