Volume-4, Issue-5, May-2015 • ISSN No 2277 - 8160

Research Paper computer Science

A Case study on cyber threats and solution (with special reference to Cisco)

Ms. Komal Saxena Phd scholar(Computer science), Singhania university.

Dr. Anurag Awasthi Research Guide(Computer science), Singhania university

ABSTRACT

There is a buzz these days about cyber threats. Why not! As security is of prime concern whether it's a small or a big organization. Network and services can be damaged due to numerous attacks against physical integrity, as a result of which it destroys or modify the information. There is also a chance of unauthorized use of essential information. Hence use various methods and solution to shield threats.

KEYWORDS : cyberattack, cyber security, cyber business challenges, cyber solutions, cisco

1. Introduction:

cyber Attack:-A cyberattack is purposeful abuse of PC frameworks, innovation ward ventures and systems. Cyberattacks use malignant code to change PC code, rationale or information, bringing about problematic outcomes that can trade off information and lead to cybercrimes, for example, data identify , theft, frauds.

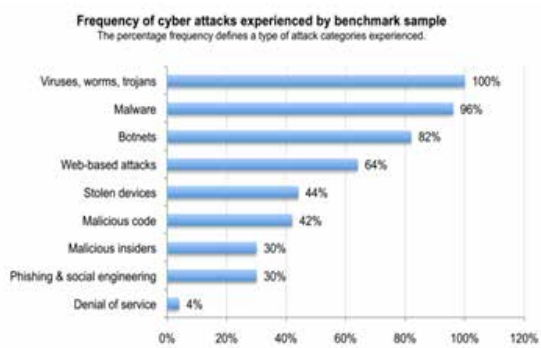

Figure:- 1 graph shows frequency of cyber attacks according to the percentage wise[6]

2. Types of attacks

There are various types of attacks such as-

2.1.Passive and Active attacks

2.1.a. Passive attacks

The intruder quietly observes the information passing through communication medium but do not interfere with the flow of information.

2.1.b. Active attacks

In this type of attack the intruder can modify or insert false messages or Trojans in to the flow of messages.

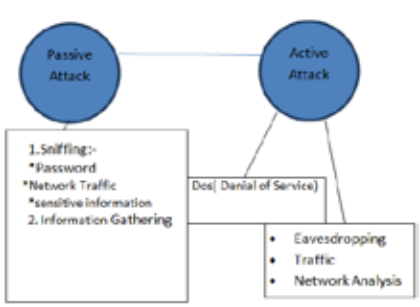

Fig:2 Active passive

2. Denial of service attacks

The attack overloads the system capacity by preventing authorized

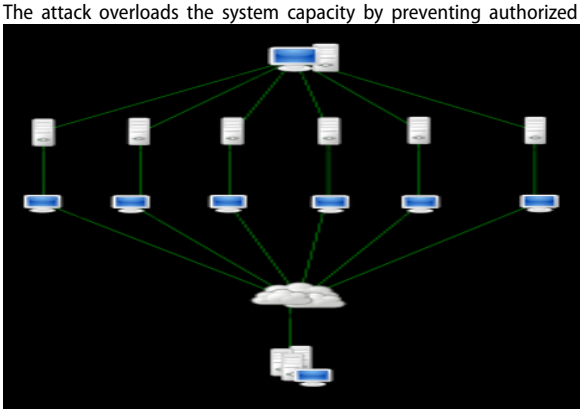

Fig:2 Denial of service[9]

Fig:-3 Malware Attack [8]

It is a malicious code that when interfered with your system infects various operations.

4. Cyber intrusion

An intruder attacks the system using Trojan horses, deception, spying or cracking the encrypted password.

Figure 4. cyber intrusion[7]

5. Spam and Phishing

Spam is very common these days sending unsolicited emails in bulk, whereas Phishing is to persuade web users into revealing their personal information using for criminal offense.

3. Security criteria

- The capability of the system to prevent unauthorized access to data depends on data confidentiality and integrity. They are being access control by authentication, identification and authorization. An integrity criterion is necessary only for authorized individuals. Cyber and proactive cyber defence could be one of the measures to take. Also, SEM (Security Event Manger), SIEM, IPS/IDS systems and Firewalls contribute to analyze cyber attacks.

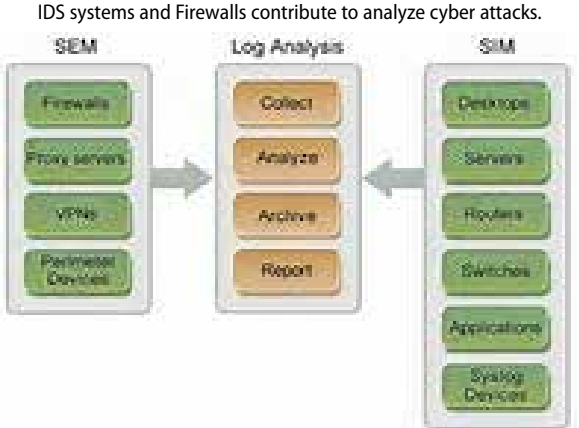

Figure:3security criteria[10]

4. Case study: CISCO cyber threat solution

The case study deals in the cyber security threat solutions. Also, it focuses on

- Business challenges to customized threats.
- A threat defence solution identifying suspicious network traffic patterns and analyzing it to overcome the situation.

Business challenge

Tough it is seen that various businesses use high functional antivirus, firewall, content security and intrusion prevention but custom written threats break all your security codes. This is a serious challenge to security protocols and businesses. The threats can flow under the radar to specific targets very quietly without disturbing the network. Many a time these threads can spread through social engineering or external devices like pen drive.

Some key figures-

- 63% of cyber threats are customized to attack specific targets- a three-fold increment since 2006.[1]
- It is found that from 2006 to 2009 five times increase in the cyber threats against the U.S. government.[2]
- 59% of associations in the United States believe that they are been targeted by various cyber threats.[3]

Where to identify these threats once reached network perimeter-

Look for fingerprints of the cyber threats by analyzing various traffic patterns across routers and switches which forms the network interior. Analyze traffic patterns of internal peer-to-peer connections and subnets of other clients.

CISCO cyber threat solution

The Cisco Cyber Threat Defense Solution unitesthe following elements providing a complete visibility into the dangerous cyber threats:

4.1 Aninterior network traffic telemetry with the capacities of Cisco switches, Cisco Catalyst switches and Cisco ASA 5500 Series Adaptive Security Appliances.

4.2 Network traffic investigation capabilities given by the Lancope StealthWatch System. Cisco has join hands with Lancope to offer the Cisco Cyber Threat Solution.

Application type contextual information, reputation and identity for discerning the severity of a threat. Thecontext points are conveyed by the Cisco switches, Cisco Security Intelligence Operations (SIO), and Cisco Identity Services Engine individually.

Utilizing this contextual information and telemetry a system security examiner can monitor suspicious action, assemble relevant client data, recognize the application, and can monitor host. This empowers evaluation of the potential threat of suspicious activities. With this data, an analyst can decode the advanced cyber threats by:

4.3 Network surveillance - The demonstration of testing the system searching for assault vectors that can be used by specially created cyber threats.

4.4 Network inside malware proliferation - Spreading malware crosswise over hosts with the end goal of get-together security observation information, exfiltrating information, or making secondary passages to the system

4.5 Control and commandtraffic - Communications between internal hosts and attacker.

4.6 Data theft - Exporting data back to the intruder, by control and command communications

Benefits

- It offers theft defense in network interior.
- It detects threats and minimizes attack.
- A Cost effective telemetry solution.
- It simplifies error-prone and manual threat investigation processes.

Conclusion

To tackle Cyber attacks like Trojans, Network sniffers, session hijacking, packet spoofing, industrial espionage, automated probes and various others, perfect network security solutions are required like CISCO cyber threat solution. There are many such solutions that need to be implemented in order to protect your organization.

REFERENCES

[1] Data Breach Investigations Report, Verizon & U.S. Secret Service; April 2011. | [2] U.S. Federal Cybersecurity Market Forecast 2010-2015, Market Research Media; December 2010. | [3] U.S. Advanced Persistent Threat Analysis, Enterprise Strategy Group; October 2011. | -Cyber Security, Environment, Solutions and Case study. | [4]www.zeepedi.com | [5]www.efgonline/blog/cyber-security | [6]http://www.intellectualtakeout.org/library/chart-graph/frequency-cyber-attacks-experienced-benchmark-sample | [7]www.cibis.com.au | [8]/www.intego.com/mac-security-blog/learn-about-mac-malware/ | [9]http://en.wikipedia.org/wiki/Denial-of-service_attack | [10]http:SEM+(Security+Event+Manger),+&go=Submit&qs=bs&form=QBIR | [11]-Special thanks & Acknowledgment to Cisco Cyber Threat Defense Solution: Delivering Visibility into Stealthy, Advanced Network Threats