CYBER CRIME & CYBER SECURITY-LATEST TRENDS

DR.V.GUNASEKHAR REDDY,
Ph.D, PG.DBA, CE,,CNA, ETE, SMIEEE, MBESI, MISCA, MISOI,MISTE, MIIPA, MCSI, MPRCI
Professor, ECE Department,
MIST, Hyderabad
gelered@gmail.com, gelered1@rediffmail.com

Abstract

Cyber Crime & Cyber Security underwent several transformations leading to steep increase in crimes related to Cyber space across the World. The Counter measures to tackle the crime related to cyber space and developing security for cyber space is becoming a challenging task . Cyber space crime is increasingly dominant in the present scenario of highest usage of Internet, Computers, Mobiles and digital platforms. In this paper the developments in crime and attacks on Cyber space are dealt .The increasing damages towards Social security, financial frauds, Banking frauds, Data thefts are covered. Cyber security aspects covering Internet Security, Social crimes, Fraudulent Apps., Banking digital Transactions, Data Security are detailed. The legal aspects towards securing Cyber Space from various crimes are detailed. Social awareness strategies are also outlined.

I- Crimes of Cyber Space

Cyber Space crimes are crimes related to the internet using a computer as a weapon to attack a computer or a mobile of a victim. In general, crimes related to cyber space have the following categories.

II- Cyber Crime Types

1. Hacking

In this, an intruder succeeds in accessing to the designated computer without permission. This is Hacking act and they are advanced level experts on computer skills of software and programming. They use several techniques to access the computer when it is accessing the internet. Two most common are: SQL Injections, and FTP Passwords theft and scripting-cross site.

2. Dissemination of Virus

These are programs related to the computers, which gets attached or infect computer operating system or important files, and may spread to many computers which are connected in the network for computer malfunction and affects data storage. Another type are worms which replicate to occupy empty memory of the system. It is also referred as self replicating malicious malware

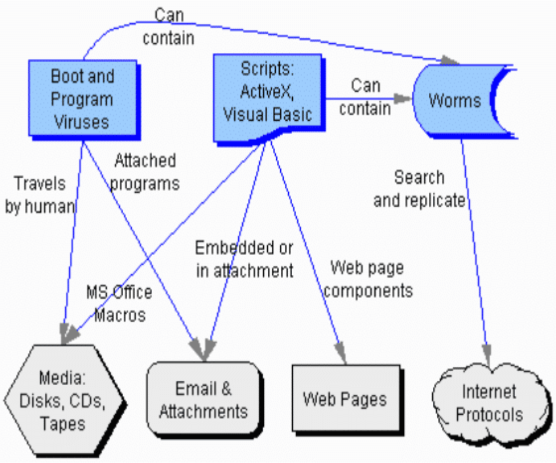


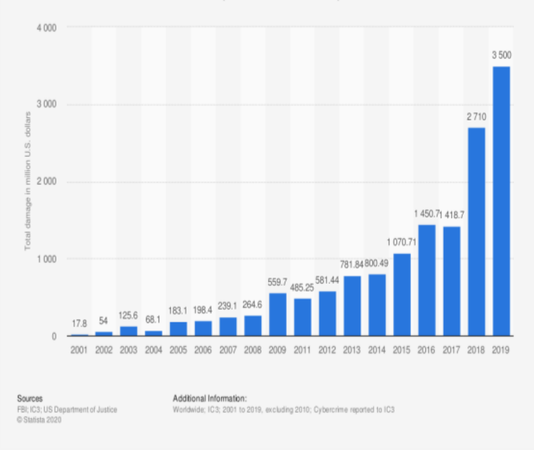
Fig.1 Malware propagation

3. Logical bombs

A logical bomb, or slag code, is a malicious code. It is deliberately transmitted to the computer system soft ware to remain dominantly, for malicious task execution.

4. Denial-of-Service attack

It is an planned approach by attackers to block services to the targeted users related to the service. In this case, the computer resources are flooded with several requests in turn occupying more memory space and resulting in overlading of the servers.



Sources
FBI; IC3; US Department of Justice
© Statista 2020

Additional Information:
Worldwide; IC3; 2001 to 2019, excluding 2010; Cybercrime reported to IC3

Fig:2 Monetary damage caused by reported cyber crime from 2001 t0 2019 (In million US dollars)

5. Phishing

This is used for collecting confidential data related to debit and credit cards information, card numbers, username and password. Phishing is basically performed by email spoofing.

6.Email bombarding and spam

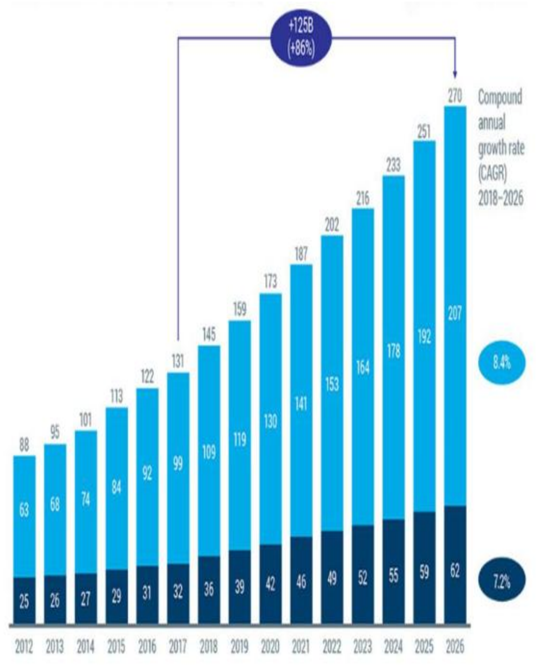
The offender sends emails more in number, to a targeted address resulting in crashing of victim's email services

7. Hijacking of Web services in more number

The hacker manages for controlling targeted web site by fraudulent means. The contents may be altered from the targeted site or may be redirected to some other page which is fake. This site is controlled by the kicker. The original web site owner, looses his access and the offender may use the targeted web site for fraudulent acts.

8. Cyber stalking

It is a type of crime related to internet where in, the targeted individual is followed online affecting piracy and the attacker follows with malicious interest.



* 2012–2016 data based on Gartner data as at 3Q16; 2017 and beyond based on Gartner data

† External spend based on forecasts to 2023 provided by Gartner, extrapolated to 2026 using the average growth rates. Growth rates applied at the product segment level

§ Internal spend refers to the compensation of in-house full-time equivalent employees. Estimated based on Gartner data on global internal spending. Internal spend grows more slowly than external spend, linked to the increasing adoption of external managed security services

SOURCE: Gartner; Australian Bureau of Statistics; Burning Glass; expert interviews; AlphaBeta and McKinsey analysis

Fig.3 Global Security Spending.

9.Data diddling

A type of unauthorised data altercation of a computer system. With this method, the attacker may change/modify the data output and tracing this fraud is difficult..

10. Debit, Credit Cards Frauds & Identity Theft

For accessing to resources like debit, credit cards, bank accounts of any individual, the crime of personal information theft is done.

11. Salami slicing attack

In this type of fraud, the offender indulges in financial fraud in slow systematic steps which are unnoticeable.

12. Software Piracy

Piracy of this nature is predominant. It is noticed in all walks of life starting from duplicating/copying movies, videos, songs, data etc., despite several laws of software piracy which results in huge losses to the original producers.

III. Indian Laws on Cyber Crime

IT Act, 2000 and IT (Amendment) Act, 2008 (Ref.i)

The Information Technology (IT) Act, 2000 was formulated by the Parliament of India during May 2000 and was enforced during October 2000. It is intended to provide legal infrastructure for Indian e-commerce. It is the first act to provide legal sanctity to electronic data records and contracts by electronic communications. This act was later amended in December 2008 through the IT (Amendment) Act, 2008.

IV-Cyber Security or Information Technology Security:

These are the techniques for safe guarding computers, networks, programs and data against unauthorized access or attacks that are aimed for exploitation. Important areas covered in cyber security are:

1) Application Security. 2)Scale of cyber threat information

The cyber threat continues to raise Globally, very fast, with huge number of data breaches each year. The report of Risk Based Security revealed that shockingly 7.9 billion records were exposed by data breaches during the year 2019, which is more than double (112%) the number of records exposed during the year 2018.

The cyber threat scale is set to continuously rise, and the International Data Corporation predicted that the worldwide spending on cyber-security solutions may reach $133.7 billions by the year 2022.(Figs2&3)

V-Cyber Security

It is the method of defending servers, computers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also referred as security of information technology. This term applies to various applications ranging from business to mobile computing, and can be categorized as :

a) Network security is the method of securing a computer network from intruders, planned attackers or malware protection.
b) Application security deals on keeping software and devices free of threats. Security features are incorporated in the design stage, before deployment of a program or device.
c) Information security protects the integrity and privacy of data, both in storage and in transit.
d) Operational security deals with the processes and decisions for handling and protecting data. The user permissions for accessing a network and the procedures for storing or sharing data are under this purview.
e) Disaster recovery measures are developed by the devise manufacturers to restore its operations and information to original configuration.
f) User Awareness is important to ensure that users get into minimum knowledge and awareness to protect their devises related to software privacy and cyber attacks.

VI-New Trends in Cyber Security

1.GDPR(General Data Protection Regulation) Spread around the World. Personal data has to be on top priority for online for the businesses users. With the steep-rising in data breaches, it is getting difficult to address data privacy concerns.

2.Data Breaches and Phishing

Protection from data breaches and phishing attacks is the developing trend in cyber space security.

3.Gap in Cyber security Skills: As per the MIT Technology Review report, (Ref.iii), about 5 million cyber security experts are needed in 2021. and this requirement may grow by 350% in future.

4.Security of Cloud:

The present trend is to upload more user data to the cloud. The protection for cloud data is a vital area in cyber security industry as the cloud- data security threats are on the rise every year.

5.Security of Mobile Devices:

Due to the steep increase in mobile users across the World, the data applications usage for financial transactions are increasing. Security threats of Mobiles are on the increasing levels due to this. In banking sector malware, it was noticed

50% rise in 2019 compared to 2018 as per Check Point's report.(Ref.vii).

6. Cyber Attacks on Vital Government Computer infrastructure:

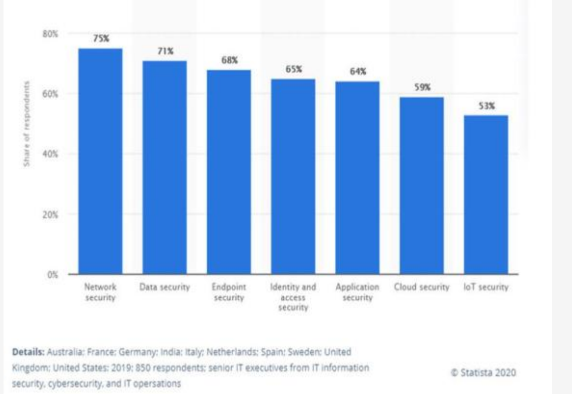
Cybercriminals with political backing from hostile Countries indulging in cyber attacks, stealing vital governmental data, misguiding and involving in the act of potential threat perception to the National security.

7.Security risks of IOT Devises:

The advancement of Internet of Things and IOT enabled devises usage created vulnerability for security threats. In accordance to the F-Secure report (Ref.ii), there is three-times increase in cyber attacks during 2019 with 2.9 billion events.

9. AI and ML roles:

Artificial Intelligence & Machine language play vital role in threats detection, face detection, human tacking etc., A.I. is deployed in cyber security Networks and for data and endpoint security. The COVID-19 pandemic, further accelerated the use of internet services resulting in the increase of security threats. (Fig.4).



Details: Australia; France; Germany; India; Italy; Netherlands; Spain; Sweden; United Kingdom; United States; 2019; 850 respondents; senior IT executives from IT information security, cybersecurity, and IT opersations

© Statista 2020

Fig.4 Artificial Intelligence (AI) usage for Cyber Security (In select Countries,2019)

10. IOT Devises in Transport Infrastructure:

The transport sector deploying IOT devises in cars, transport vehicles, Aircrafts, and trains are increasing, resulting in vulnerable security threats.

11.Network of Fifth-Generation Technology (5G):

In the future with 5G technology, various security features are developed for security threats and by the time the technology roles out, the cyber threats may also undertake various trends and there is a continuous attempt to develop cyber security measures.,

12.Internal security threats/Attacks:

It was pointed out by Verizon's report(Ref.vi) that 34% of cyber attacks in the year 2019 were involved with internal malpractices.

13. Sandboxing of Malicious Software :

This is a type of technology deployed by antivirus software for detecting the malware and securing form the malware attack.

14 Insurance Policy for Cyber Risks

Insurance policy for Cyber Risk is provided for industries/organizations which are contemplating financial risks from cyber attacks. As per the report by PWC, (Ref.iv), few US based companies have cyber risk insurance. Policies.

VII-Methods for Staying Protected

There are various methods for protecting data related to personal and business information and important data from cyber threats.

1.Back-Ups

The important data related to the website , personal or business to be backed up for recovery in case of cyber attack.

2. Devices and Network Protection

The following steps to be adapted:

i)Software Update: Regular updates to be done to keep the latest version of the soft ware..

ii)Installation of anti-virus software to protect and secure business and personal computers from viruses, malware, spyware, and spam.

iii)Firewall configuration: It is a software or hard ware which acts as a protective layer between the computers and the internet. It filters all traffic to provide network security at home or office.

3. Data Encryption

The data which is important, need to be encrypted before sending and for storing online.

4.Two- level authentification

The authentication of this type is more secure. After a password is entered to log on to an account and for any transaction to complete, an authentication code is sent to the user mobile and after entering the code of authentication, then only the transaction gets completed.

5.Passwords

It is proposed for the use of strong passwords to keep the passwords complex. Use letters with mix of upper and lower case, symbols and numbers.

6. Employees Training

For data breaches, employees play a major role. The organisations must enforce restrictions and frame rules for internet usage in networked computers to avoid security breaches..

VIII-Conclusion

Recently, various tends in Cyber crime is steeply increasing with the high use of internet and digital financial transactions across the world. In order to effectively counter increasing cyber attacks, several new trends in cyber space security are also evolving.

IX-References:

i) *Indian Information Technology (IT) Act, 2000*

ii) *F Security Report*

iii) *Review report of MIT Technology*

iv) *PWC(Price Water Coupers) Report*

v) *FBI,IC3,US Department of Justice, Statica 2020*

vi) *Verizon's report https://www.verizon.com/business/resources/reports/cyber-espionage-report*

vii) *Report of Check Point https://ciso.economictimes.indiatimes.com/news/complex-cyber-crime.*

Author

Professor ECE, Director, R&D, Mahaveer Institute of Science &Technology, Hyderabad, Deputy Inspector General of Police, Rtd. AP Police. Council Member ,IETE (2019-22)
Vice-President(2018,2019), IETE, New Delhi .
Secure Communications Consultant TTD, Tirupati (2013-16) and for National & Multi National Organisations .
Teaching & Industry experience-43 years, while working with MIST, Hyderabad, A.P. Police Communications, Uptron India Ltd, Bharath Electronics Ltd. & Videsh Sanchar Nigam Ltd.