SALT

!@ #

Ethical Hacking

Unit 1

Information Security: Attacks and Vulnerabilities Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Malware, Worms, viruses, Trojans, Spyware, Rootkits, Types of vulnerabilities: Top 10 OWASP.

Types of attacks and their common prevention mechanisms: Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping, Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs

Case-studies: Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit, Media Markt, Kaseya, JBS, Colonial Pipeline, The University of California at San Francisco.

What is Ethical Hacking

Also Called – Attack & Penetration Testing,
White-hat hacking, Red teaming

Hacking

Process of breaking into systems for:
- Personal or Commercial Gains
- Malicious Intent – Causing sever damage to Information & Assets

Ethical

Conforming to accepted professional standards of conduct

Black-hat – Bad guys

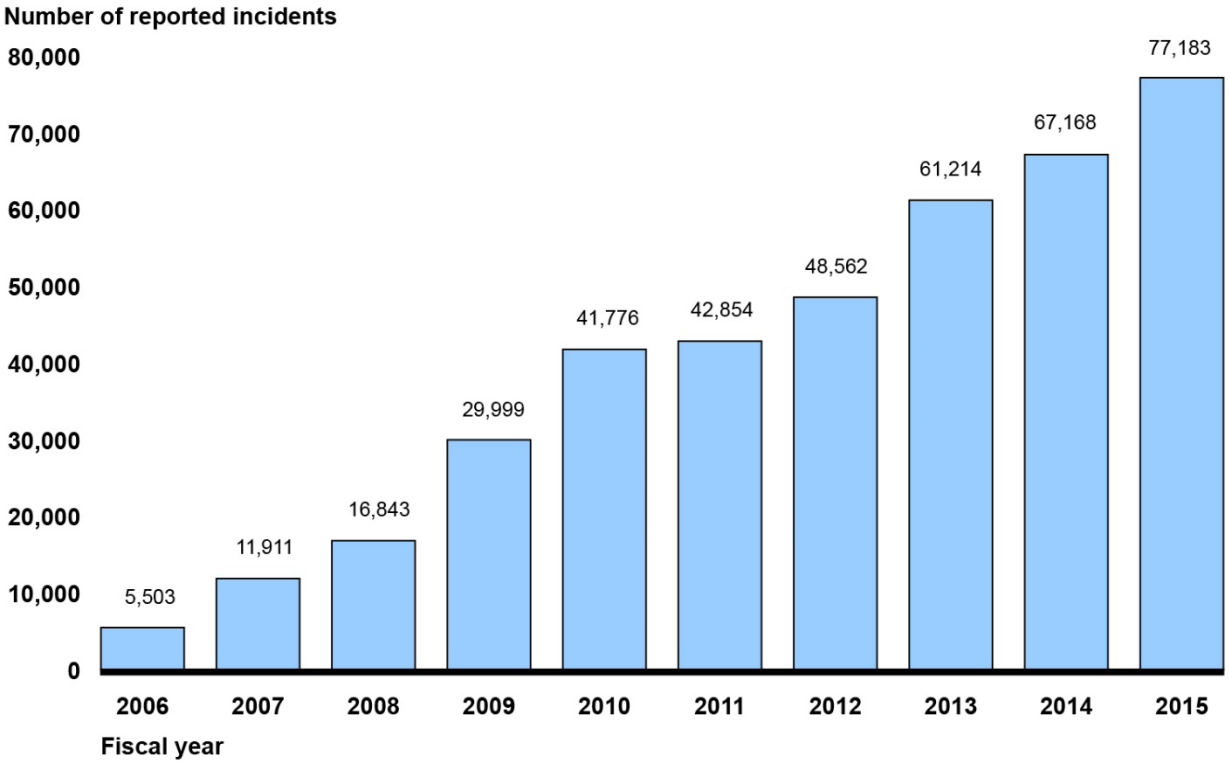
White-hat - Good Guys

What is Ethical Hacking

- It is Legal
- Permission is obtained from the target
- Part of an overall security program
- Identify vulnerabilities visible from Internet at particular point of time
- Ethical hackers possesses same skills, mindset and tools of a hacker but the attacks are done in a non-destructive manner

Why – Ethical Hacking

Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015

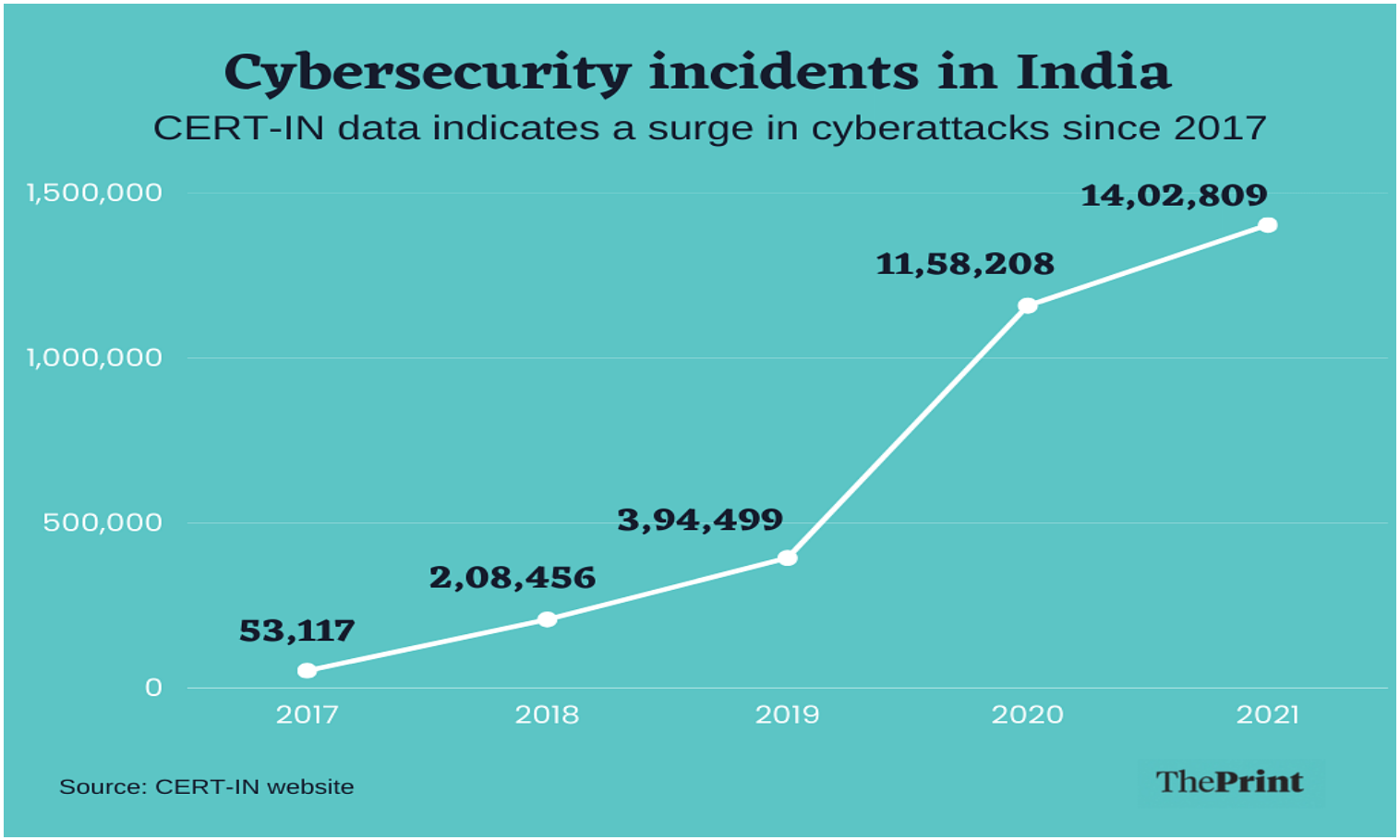


Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Source: CERT-India

I@ #

Why – Ethical Hacking

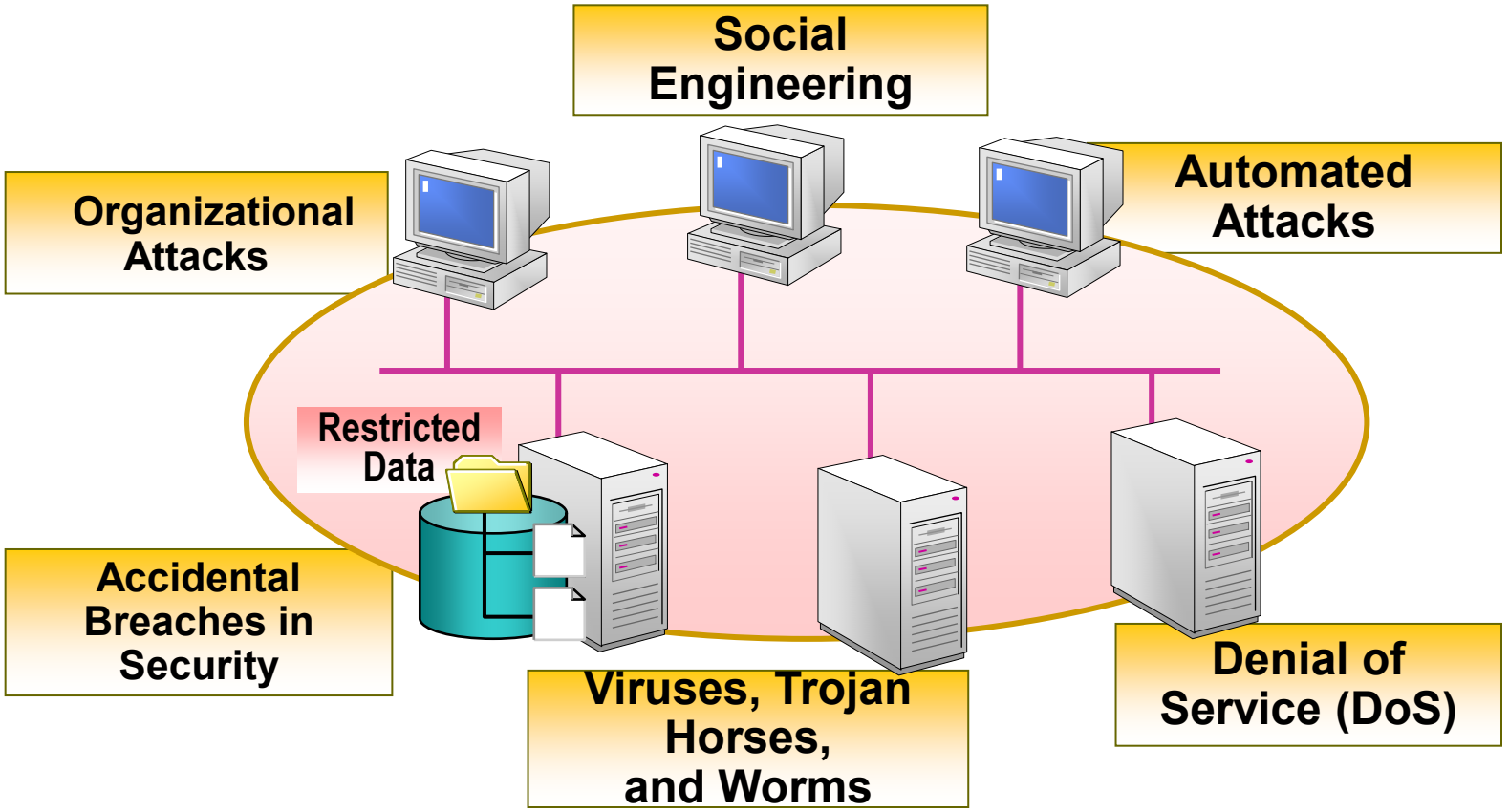


Total Number of Incidents Incidents *Source: CERT/CC*

I@ #

Why – Ethical Hacking

Protection from possible External Attacks



Ethical Hacking - Process

1. Preparation
2. Footprinting
3. Enumeration & Fingerprinting
4. Identification of Vulnerabilities
5. Attack – Exploit the Vulnerabilities

Preparation

- Identification of Targets – company websites, mail servers, extranets, etc.
- Signing of Contract
  - Agreement on protection against any legal issues
  - Contracts to clearly specifies the limits and dangers of the test
  - Specifics on Denial of Service Tests, Social Engineering, etc.
  - Time window for Attacks
  - Total time for the testing
  - Prior Knowledge of the systems
  - Key people who are made aware of the testing

Footprinting

Collecting as much information about the target

- DNS Servers
- IP Ranges
- Administrative Contacts
- Problems revealed by administrators

Information Sources

- Search engines
- Forums
- Databases – whois, ripe, arin, apnic
- Tools – PING, whois, Traceroute, DIG, nslookup, sam spade

Enumeration & Fingerprinting

- Specific targets determined
- Identification of Services / open ports
- Operating System Enumeration

Methods

- Banner grabbing
- Responses to various protocol (ICMP &TCP) commands
- Port / Service Scans – TCP Connect, TCP SYN, TCP FIN, etc.

Tools

- Nmap, FScan, Hping, Firewalk, netcat, tcpdump, ssh, telnet, SNMP Scanner

Identification of Vulnerabilities

Vulnerabilities

- Insecure Configuration
- Weak passwords
- Unpatched vulnerabilities in services, Operating systems, applications
- Possible Vulnerabilities in Services, Operating Systems
- Insecure programming
- Weak Access Control

Identification of Vulnerabilities

Methods

- Unpatched / Possible Vulnerabilities – Tools, Vulnerability information Websites
- Weak Passwords – Default Passwords, Brute force, Social Engineering, Listening to Traffic
- Insecure Programming – SQL Injection, Listening to Traffic
- Weak Access Control – Using the Application Logic, SQL Injection

Identification of Vulnerabilities

Tools

Vulnerability Scanners - Nessus, ISS, SARA, SAINT
Listening to Traffic – Ethercap, tcpdump
Password Crackers – John the ripper, LC4, Pwdump
Intercepting Web Traffic – Achilles, Whisker, Legion

Websites

- Common Vulnerabilities & Exposures – http://cve.mitre.org
- Bugtraq – www.securityfocus.com
- Other Vendor Websites

Attack – Exploit the vulnerabilities

- Obtain as much information (trophies) from the Target Asset
- Gaining Normal Access
- Escalation of privileges
- Obtaining access to other connected systems

Last Ditch Effort – Denial of Service

Attack – Exploit the vulnerabilities

Network Infrastructure Attacks

- Connecting to the network through modem
- Weaknesses in TCP / IP, NetBIOS
- Flooding the network to cause DOS

Operating System Attacks

- Attacking Authentication Systems
- Exploiting Protocol Implementations
- Exploiting Insecure configuration
- Breaking File-System Security

Attack – Exploit the vulnerabilities

Application Specific Attacks

- Exploiting implementations of HTTP, SMTP protocols
- Gaining access to application Databases
- SQL Injection
- Spamming

Attack – Exploit the vulnerabilities

Exploits

- Free exploits from Hacker Websites
- Customised free exploits
- Internally Developed

Tools – Nessus, Metasploit Framework,

Reporting

- Methodology
- Exploited Conditions & Vulnerabilities that could not be exploited
- Proof for Exploits - Trophies
- Practical Security solutions

Ethical Hacking - Commandments

- Working Ethically
  - Trustworthiness
  - Misuse for personal gain
- Respecting Privacy
- Not Crashing the Systems

keystroke logging

- creating records of everything you type on a computer or mobile keyboard
- monitor your computer activity while you use your devices as normal.
- Keyloggers are used for legitimate purposes like feedback for software development but can be misused by criminals to steal your data.

How Keystroke Logging Works

- Length of the keypress
- Time of keypress
- Velocity of keypress
- Name of the key used

Types of keystroke logging

- ***Software keyloggers***

-API-based keyloggers

-Form grabbing-based keylogger

-Kernel-based keyloggers

- ***Hardware keyloggers***

-Keyboard hardware keyloggers

-Hidden camera keyloggers

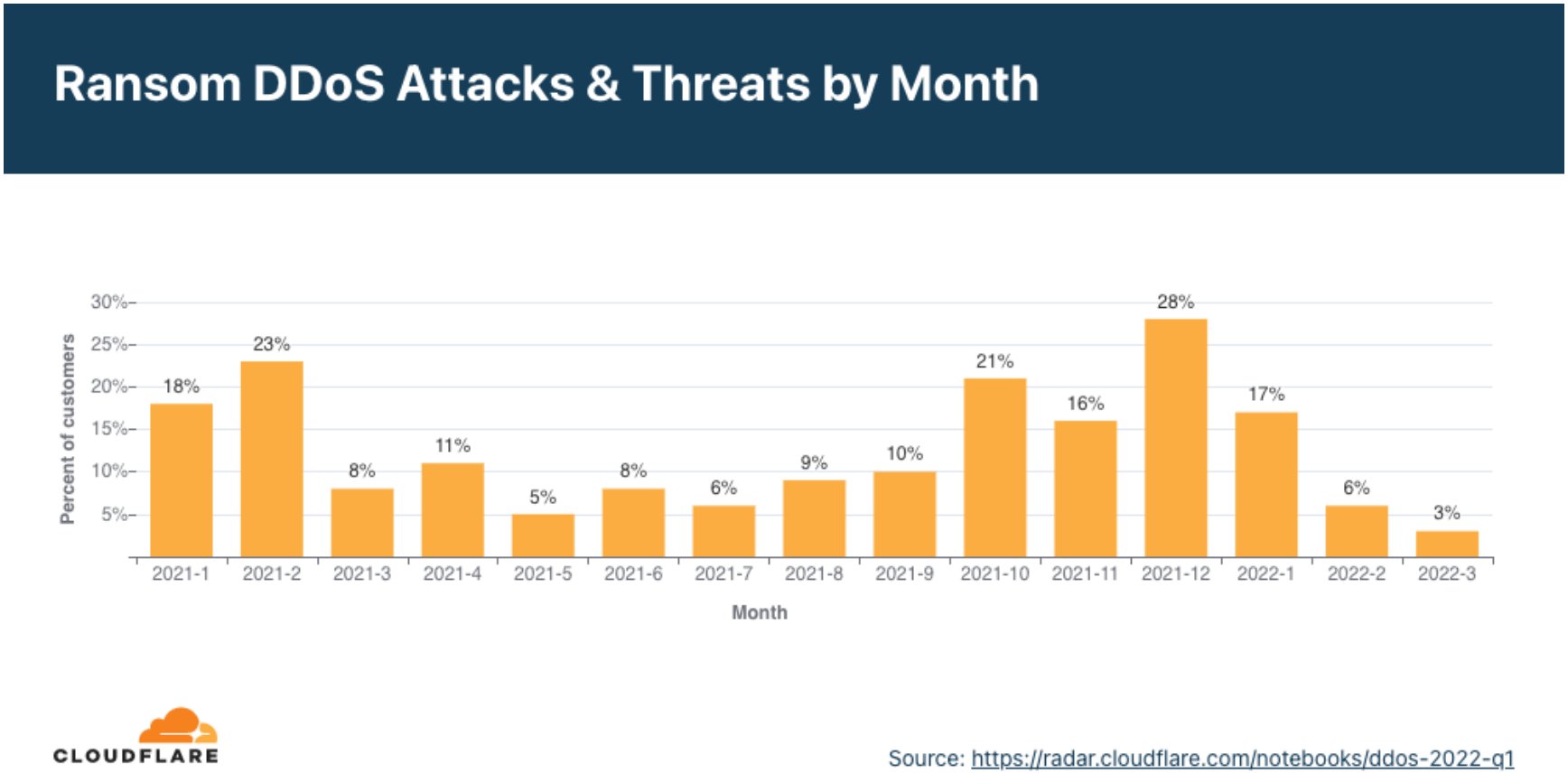
-USB disk-loaded keyloggers

WHAT IS “DOS ATTACK”

Denial-Of-Service Attack= DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to it customers.

- DoS = when a single host attacks
- DDoS = when multiple hosts attack simultaneously

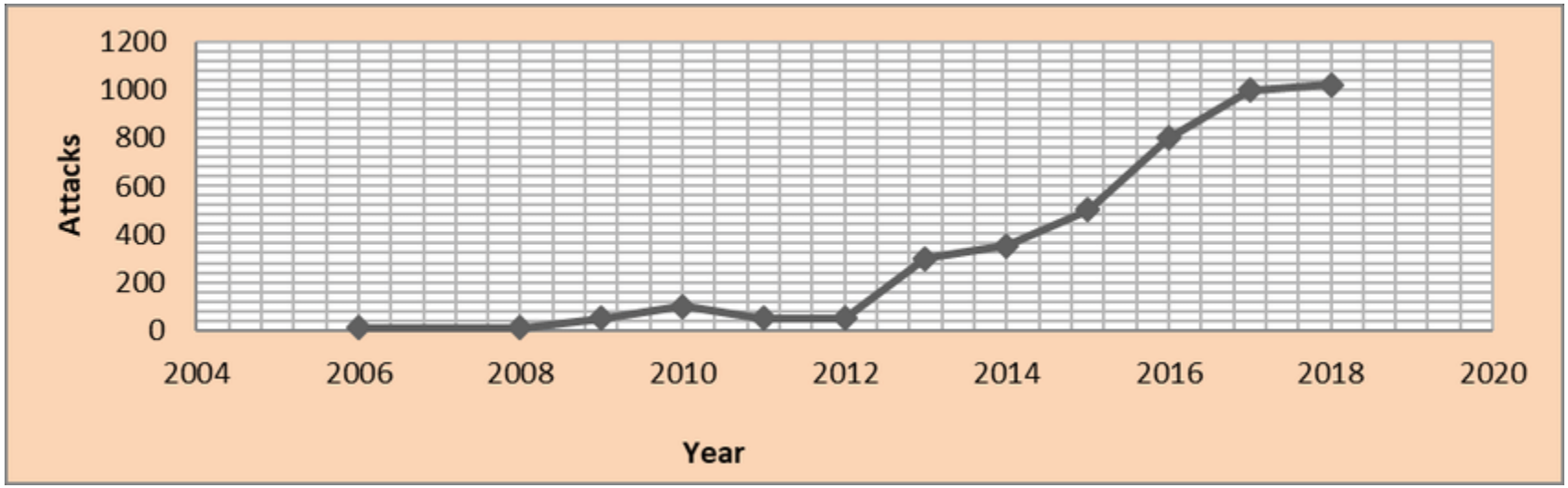
ATTACK SIZE IN GBITS-PER-SECOND



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q1

ATTACK SIZE IN GBITS-PER-SECOND



IDEA OF “DOS ATTACKS”

- Purpose is to shut down a site, not penetrate it.
- Purpose may be vandalism, extortion or social action (including terrorism) (Sports betting sites often extorted)
- Flood a network with traffic, thereby preventing legitimate network traffic.
- Disrupt connections between two machines, thereby preventing access to a service.
- Modification of internal data, change of programs (Includes defacement of web sites)

HISTORY

Morris Worm (November 2, 1988)

- First DDoS attack to cripple large amounts of network infrastructure
- Self-replicating, self-propagating.
- Exploited software commonality (monoculture)

1. Fingerd buffer overflow exploit
2. Sendmail root vulnerability
3. Weak passwords

HISTORY

Morris Worm effect

- Infected systems became "catatonic"
- Took roughly three days to come under control
- Ultimately infected 10% of Internet computers (6,000) and cost $ million to clean up.
- Morris convicted under computer fraud and abuse act, three years probation, fine of $10,000

HISTORY

SQL Slammer (January, 25 2003)

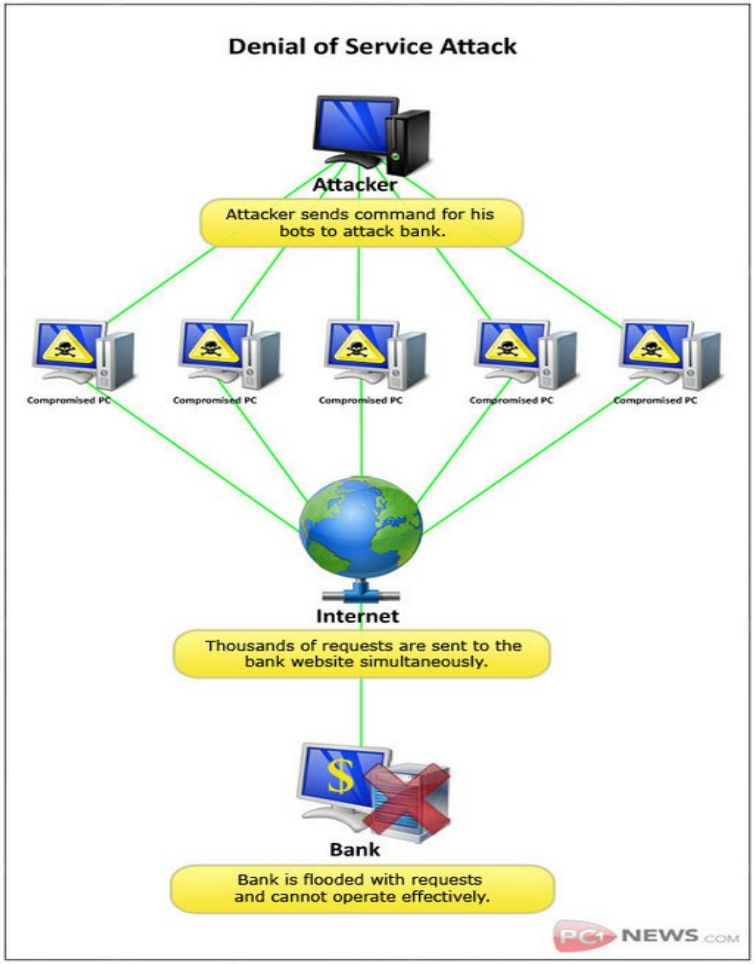
- Exploited common software (Microsoft SQL Server) as well as hardware (Intel x86), spread rapidly in a distinct monoculture.
- Non-destructive. Modified no data on infected system
- Extremely simple in construction (376 bytes)
- Devastating:
  1. 120,000 computers infected at peak (1/26/2003)
  2. Exhausted network bandwidth
  3. Crashed network infrastructure (multicast state creation)
  4. Shut down communication (fire-fighting) capability

HISTORY

SQL Slammer effect

- Extremely Virulent
- Caused economic damage outside of IT infrastructure (multiple ATM outages)
- Original perpetrators have never been identified or brought to justice

TYPES OF DOS ATTACKS



TYPES OF DOS ATTACKS

- Penetration
- Eavesdropping
- Man-In-The-Middle
- Flooding –syn

TYPES OF DOS ATTACKS

Penetration

- Attacker gets inside your machine
- Can take over machine and do whatever he wants
- Achieves entry via software flaw(s), stolen passwords or insider access

TYPES OF DOS ATTACKS

Eavesdropping

- Attacker gains access to same network
- Listens to traffic going in and out of your machine

TYPES OF DOS ATTACKS

Man-in-the-Middle

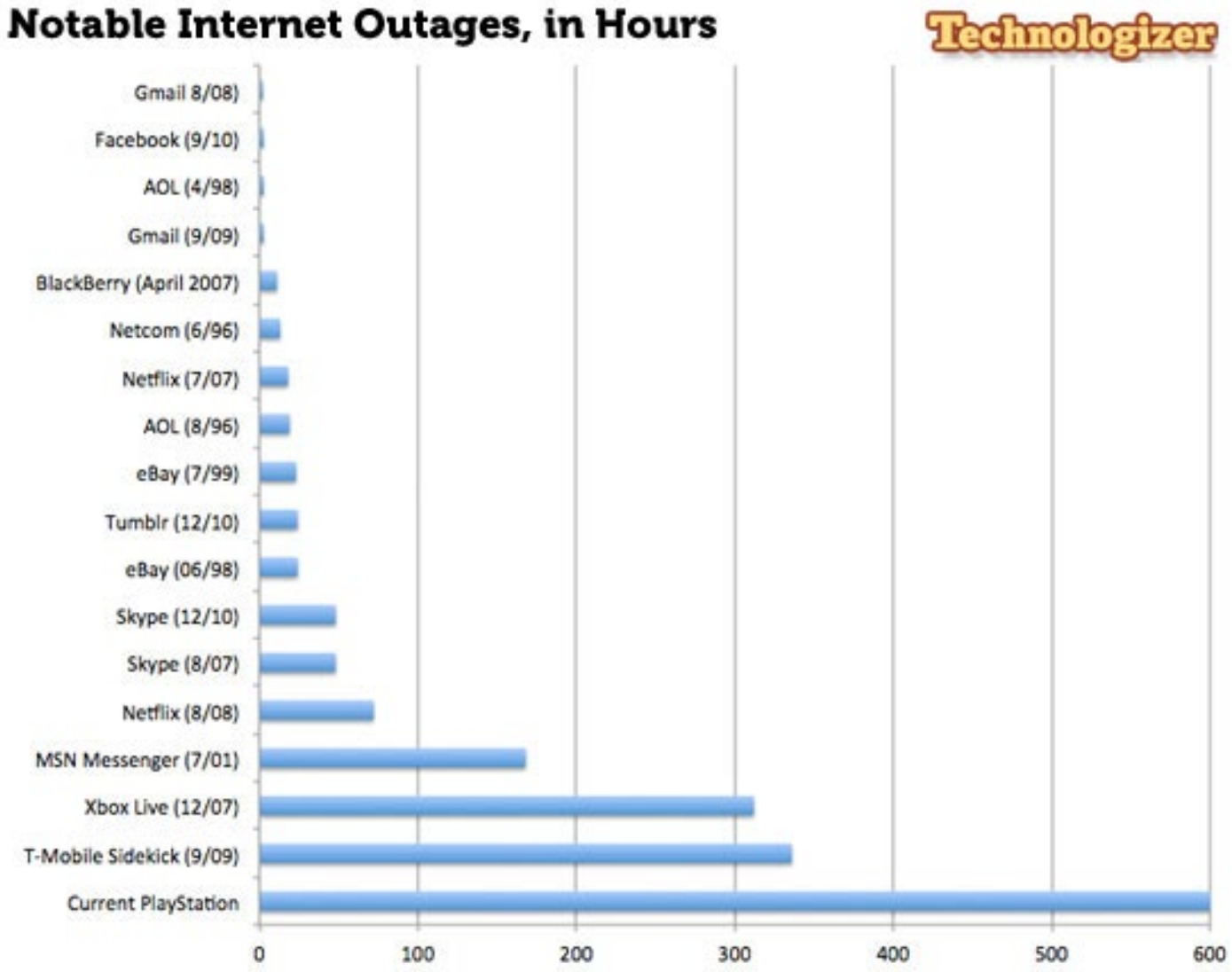
- Attacker listens to output and controls output
- Can substitute messages in both directions

TYPES OF DOS ATTACKS

Flooding

- Attacker sends an overwhelming number of messages at your machine; great congestion
- The congestion may occur in the path before your machine
- Messages from legitimate users are crowded out
- Usually called a Denial of Service (DoS) attack, because that's the effect.
- Usually involves a large number of machines, hence Distributed Denial of Service (DDoS) attack

MAIN TARGETS PG 122 TOOL



#

ESTONIAN CYBERWAR APRIL 27, 2007

- Weeks of cyber attacks followed, targeting government and banks, ministries, newspapers and broadcasters Web sites of Estonia.
- Some attacks took the form of distributed denial of service (DDoS) attacks (using ping floods to expensive rentals of botnets).
- 128 unique DDOS attacks (115 ICMP floods, 4 TCP SYN floods and 9 generic traffic floods).
- Used hundreds or thousands of "zombie" computers and pelted Estonian Web sites with thousands of requests a second, boosting traffic far beyond normal levels.

ESTONIAN CYBERWAR APRIL 27, 2007

- Inoperability of the following state and commercial sites:
  - The Estonian presidency and its parliament.
  - Almost all of the country's government ministries.
  - Political parties.
  - Three news organizations.
  - Two biggest banks and communication's firms.
  - Governmental ISP.
  - Telecom companies.

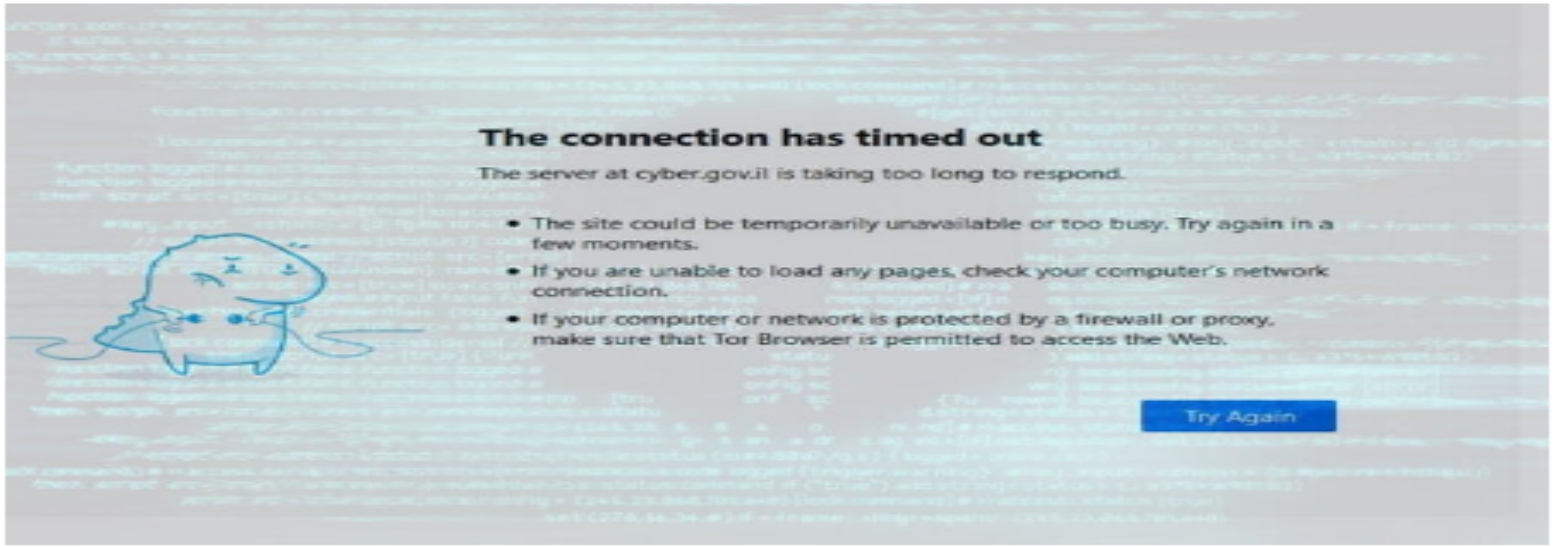
ESTONIAN CYBERWAR APRIL 27, 2007

- The attack heavily affected infrastructures of all network:
  - Routers damaged.
  - Routing tables changed.
  - DNS servers overloaded.
  - Email servers mainframes failure, and etc.

Israeli government websites crash after 'massive' cyberattack, officials say

Users unable to reach sites with gov.il extension for an hour, as National Cyber Directorate reportedly declares state of emergency over incident

By EMANUEL FABIAN
14 March 2022, 10:13 pm | 3



Screenshot of Israeli government website cyber.gov.il unavailable during an apparent cyberattack on March 14, 2022, overlaid with an illustrative image of computer code. (Screenshot; solarseven; iStock by Getty Images)

Israeli government websites were downed for over an hour due to a major cyberattack on Monday evening, officials said.

Communications Minister Yoaz Hendel held an assessment with officials due to the "broad cyberattack" on government websites, a statement from his office said.

Users attempting to enter sites with gov.il extensions were unable to for at least an hour, before the sites slowly began to come back online.

HOW TO DEFEND

- Firewalls - can effectively prevent users from launching simple flooding type attacks from machines behind the firewall.
- Switches - Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding to detect and remediate denial of service attacks
- Routers - If you add rules to take flow statistics out of the router during the DoS attacks, they further slow down and complicate the matter
- DDS based defense
- Clean pipes

PROSECUTION

- Different governmental legislation
- Too expensive
- National interests
- Hard to prove who used the computer