Malware

- Malware-এর পূর্ণরূপ: **Malicious Software** ম্যালওয়্যার এক ধরনের সফটওয়্যার যা তৈরি/ডিজাইন করা হ ব্যবহারকারীর অজান্তে কোনো কম্পিউ অবৈধ অনুপ্রবেশ করে উক্ত কম্পিউটা সিস্টেমের ক্ষতিসাধনের উদ্দেশ্যে।

ণওয়্যারের অন্তর্গত জনপ্রিয় কয়েকটি সফটওয়্যা

:US (ভাইরাস)

ware (অ্যাডওয়্যার)

rm (ওয়ার্ম)

ware (স্পাইওয়্যার)

jan Horse (ট্রোজান হর্স)

- Rootkit (রুটকিট)
- Browser Hijackers
- Ransomware (র‍্যানসমওয়্যার)
- Overwrite Virus

VIRUS (ভাইরাস)

রূপ: Vital Information Resources Under Seize. অর্থ: গুরুত্বপূর্ণ উৎসগু
জয়াপ্ত করা হয়েছে।

পউটারের একটি ক্ষতিকর প্রোগ্রাম (সফটওয়্যার) যা ব্যবহারকারীর অনুমতি বা
াই নিজে নিজেই কপি হতে পারে বা নিজের প্রতিরূপ সৃষ্টি করতে পারে।

রাসের মূল কাজ: কম্পিউটার সিস্টেমে ঢুকে অন্য প্রোগ্রাম বা ফাইলগুলোকে মে
odify) করে নিজের কিছু ক্ষতিকারক কোড প্রোগ্রামে লিখে দেয়।

পউটার ভাইরাসের নামকরণ করেন: ফ্রেডরিক কোহেন। প্রথম কম্পিউটার ভাইর
eper Virus.

ম্পিউটার ভাইরাসের ক্রমভিত্তিক ইতিহাস:

	তথ্যপ্রবাহ
	কম্পিউটার ভাইরাস আবিষ্কার করে: বব থমাস ক্রিপার।
	'মাইকেল অ্যাঞ্জেলা' নামক ভাইরাস কম্পিউটার সিস্টেমে প্রবেশ করে লক্ষাধিক কম্পি অচল করে।
প্রল ১৯৯৯	বাংলাদেশসহ বিশ্বের লক্ষাধিক কম্পিউটারে 'CIH বা চেরনোবিল' ভাইরাস প্রবেশ কর ভাইরাসের রচিয়তা: চেন ইং হাও)।
	•'Koobface' নামক কম্পিউটার ভাইরাস ছাড়া হয় ফেইসবুক এবং মাইস্পেসকে টা •'Conficker' নামক ভাইরাস মাইক্রোসফট সার্ভার সিস্টেমে প্রবেশ করে।
	'শ্যাডো ব্রোকারস' নামের হ্যাকাররা 'র‍্যানসমওয়্যার' নামক এক ধরনের ম্যালওয়ার ব ছড়িয়ে দেয়, যার সাহায্যে কম্পিউটারের নিয়ন্ত্রণ নিয়ে হার্ডডিস্কের অংশ বা ফাইল পা দিয়ে অবোধ্য করে ফেলে।

পউটার সিস্টেমে ভাইরাস যেভাবে প্রবেশ করে ও প্রতিরোধের উ

	যেভাবে প্রবেশ করে অন্য	প্রতিরোধের উপায়
mory)	অন্য কম্পিউটারে ব্যবহৃত USB Device (যেমন: Pen Drive), Hard Disk, CD, DVD ইত্যাদি নিজের কম্পিউটারে ব্যবহারের মাধ্যমে।	USB Device (যেমন: Pen Drive), Hard DVD ইত্যাদি থেকে ফাইল কপি করার পূর্বে হবে।
Software)	অন্য কম্পিউটার থেকে কপিকৃত সফটওয়্যার নিজের কম্পিউটারে ব্যবহারের মাধ্যমে।	অন্য কম্পিউটার থেকে কপিকৃত সফটওয়্যার আগে সফটওয়্যার ভাইরাস মুক্ত করতে হবে।
	পুরাতন ভার্সনের এন্টি-ভাইরাস সফটওয়্যারের মাধ্যমে।	Update এন্টি-ভাইরাস সফটওয়্যার ব্যবহার
nternet)	সংক্রমিত (Infected) ওয়েবসাইটের মাধ্যমে ৭০% ভাইরাস কম্পিউটার সিস্টেমে প্রবেশ করে।	ইন্টারনেট ব্যবহারের সময় Internet Secur Antivirus ব্যবহার করা।
chment	ইমেইল থেকে File Attachment (যেমন: WordFile, Picture, Power Point file, Audio, Video)-এর মাধ্যমে।	সন্দেহজনক সোর্সের ই-মেইল রিসিভ না কর করতেই হয় তাহলে ভাইরাস মুক্ত করা।

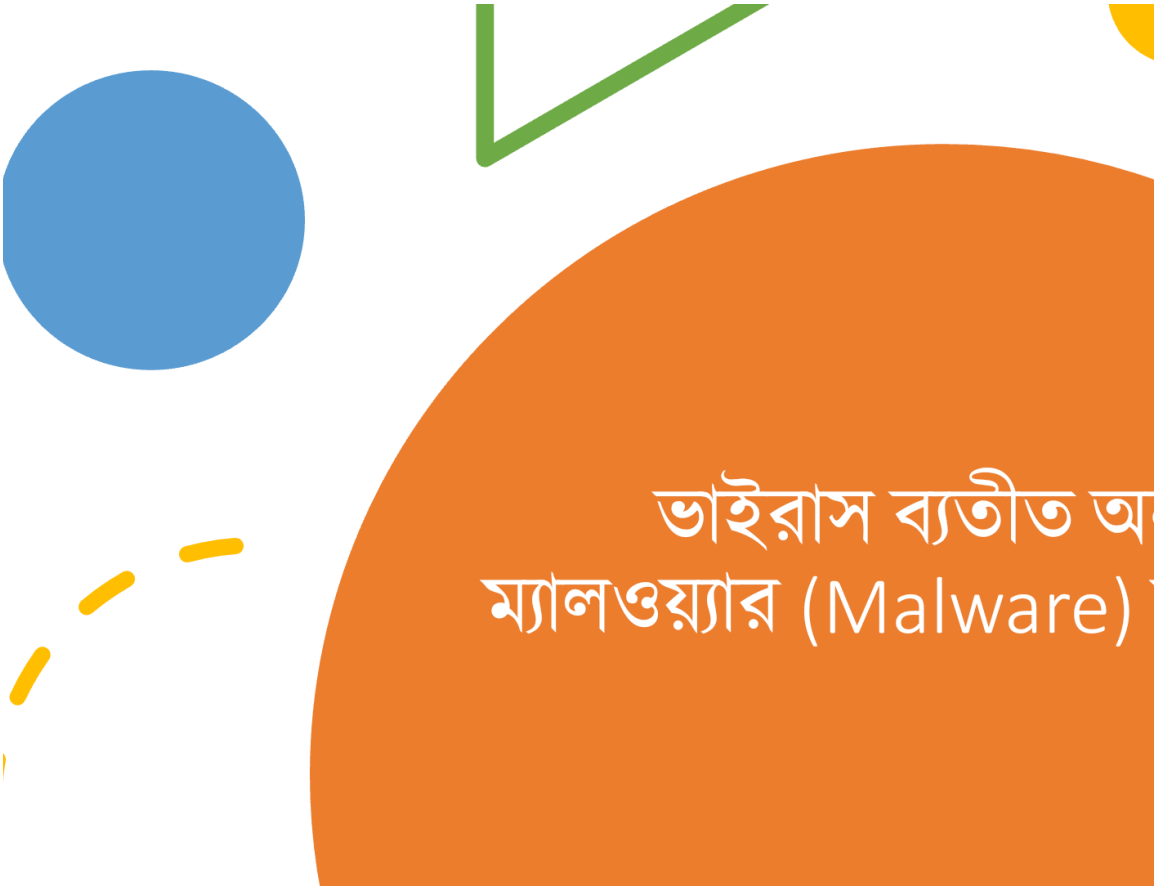
অ্যান্টিভাইরাস (AntiVirus)

ন্টিভাইরাস: একটি Utility Software যা কম্পিউটার সিস্টেমকে ভাইরাস
ক সার্বিক নিরাপত্তা, বিভিন্ন তথ্য, ফাইল রক্ষার জন্য প্রতিরোধক হিসেবে ব
। অর্থাৎ, কম্পিউটার ভাইরাসের প্রতিষেধক প্রোগ্রামকে অ্যান্টিভাইরাস বে

: বিভিন্ন ম্যালওয়্যার (যেমন: Trojan Horse, Worm, BHO (Browser
per Object)-এর বিরুদ্ধে কাজ করে।

মানে আলোচিত ও জনপ্রিয় Anti-Virus:

- Kaspersky
- Symantec
- Virusafe
- NetQin
- Cobra
- Bitdefender
- Thunder Byte
- AVG
- E-scan
- Norton
- Panda
- Norman
- PC Cillin
- Avast
- REVE
- McAfee
- IBM Anti Virus
- Vigilant
- Avira
- Dr. Soloman toolkit



Worms (ওয়ার্ম)

Virus → install

ম্পিউটার প্রোগ্রাম ইন্টারনেটের মাধ্যমে নিজে নিজেই কম্পিউটার সিস্টেমে কপি
ওয়ার্ম বলে।

নাম: Self-Replicating (নিজেই নিজের প্রতিরূপ তৈরি করতে পারে)। একটি
য়্যার কম্পিউটার প্রোগ্রাম যারা নিজেদের কোড এমনভাবে বদলে নেয় যে, খুঁজে
কষ্টসাধ্য।

ব কম্পিউটার সিস্টেমে প্রবেশ করে: কম্পিউটার নেটওয়ার্ক ব্যবহার করে এবং
উটারের নিরাপত্তার ব্যর্থতার সুযোগে কম্পিউটার সিস্টেমে প্রবেশ করে।

বনের ক্ষতি করে: সবসময় নেটওয়ার্কের ক্ষতি করে, ইন্টারনেট ব্যান্ডউইথ খরচ

এবং ভাইরাসের মধ্যকার মূল পার্থক্য: ওয়ার্ম ব্যবহারকারীর সহায়তা ছাড়াই নি
া দিতে পারে, কিন্তু ভাইরাসের সচল হতে ব্যবহারকারীর স্বদিচ্ছা (নিজের ভুলে
াসকে অনুমতি দেয়া) থাকতে হয়।

Ransomware (র‍্যানসমওয়্যার)

রনের ম্যালওয়্যার যা কম্পিউটার ডিভাইসকে আক্রান্ত করার পর ব্যবহারকারীকে তার মেশিনে থকে বিরত রাখে এবং ব্যবহারকারীর প্রবেশগম্যতা সীমাবদ্ধ করে দেয়। এই সীমাবদ্ধতা দূর ক রকারীর কাছ থেকে মুক্তিপণ দাবি করে।

র সিস্টেমে প্রবেশ করে: স্পাম/ফিশিং মেইল বা মেসেজের লিংকে প্রবেশের মাধ্যমে, সাইবার া, দুর্বল পাসওয়ার্ডের কারণে, বিভিন্ন ওয়েব এডের মাধ্যমে।

য় বেশি আক্রমণ করা র‍্যানসমওয়্যার: CryptoLocker, WannaCry (২০১৭ সালে র‍্যানসমও য় বড় সাইবার অ্যাটাক), Crypto Wall, Locky, Petya, CryptXXX, notPetya etc.

য় বেশি র‍্যানসমওয়্যার অ্যাটাক করে Windows OS এ;

nger - MacOS এ অ্যাটাক করা সাইবার অ্যাটাক।

Trojan Horse (ট্রোজান হর্স) অর্থ ট্রয়ের ঘোড়

টি ক্ষতিকারক কম্পিউটার প্রোগ্রাম যা কম্পিউটার সিস্টেমে সাধারণত বৈধ বা স্বাভাবি টওয়্যার হিসেবে আচরণ করে এবং ব্যবহারকারীর কাছে নিজেকে অত্যন্ত কার্যকরী, সু কর্ষণীয় রূপে প্রতীয়মান করে, যাতে ব্যবহারকারী মোহিত হয়ে সফটওয়্যারটি ইন্সটল ক

জান হর্স নিজের প্রতিরূপ তৈরি করতে পারে না; কিন্তু এর মাধ্যমে হ্যাকাররা কম্পিউট স্টমের নিয়ন্ত্রণ নিয়ে নেয়।

গাবে কম্পিউটার সিস্টেমে প্রবেশ করে: সামাজিক প্রযুক্তি ব্যবহার করে, কোনো আকর্ষ ডনলোড করার মাধ্যমে বা কোনো সাধারণ ফর্ম পূরণ করার মাধ্যমে।

ধরনের ক্ষতি করে: কম্পিউটার সিস্টেমে ইন্টারনেট, নেটওয়ার্কের মাধ্যমে প্রবেশ করে াসোনাল ডেটা চুরি বা নেটওয়ার্কের পারফরম্যান্স দুর্বল করে দেয়

Spyware (স্পাইওয়্যার)

ারকারীর অজান্তে ডিভাইসে প্রবেশ করে ডিভাইসের ডেটা সংগ্রহ এবং সংগ্রহকৃত ডেট
কের বিনা সম্মতিতে অন্য আরেক ডিভাইসে সরবরাহ করার উদ্দেশ্যে বিশেষভাবে ডিজ
ধরনের ক্ষতিকর সফটওয়্যার।

াবে প্রবেশ করে: মূলত ইন্টারনেটের মাধ্যমে। ই-মেইল, ফ্রি সফটওয়্যারের মাধ্যমে, অ
বসাইট থেকে ফাইল ডাউনলোড করার সময়, পপ আপ উইন্ডো এবং সোশ্যাল মিডিয়া
রর মাধ্যমে কম্পিউটারে ইন্সটল হয়।

রনের ক্ষতি করতে পারে: আক্রান্ত ডিভাইসের যাবতীয় ইমেইল অ্যাক্টিভিটি, পাসওয়ার্ড
য়া অ্যাকাউন্ট, ক্রেডিট কার্ডের তথ্যসহ সকল তথ্য চুরি করতে পারে। অপারেটিং সিস্টে
ফিগারেশন পরিবর্তন করে ফেলতে পারে। এক কথায়, ব্যবহারকারীর কম্পিউটার সিস্টে
ন্ত্রণ নিয়ে নিতে পারে।

Adware (অ্যাডওয়্যার)

ধরনের ক্ষতিকারক সফটওয়্যার যা ব্যবহারকারীর অনুমতি ছাড়াই অযাচিত বিজ্ঞ
র্শন করে এবং গোপনে তথ্য সংগ্রহ করে। অ্যাডওয়্যার ব্যবহারকারীর অনিচ্ছাসত্ত্বে
া অ্যাড দেখতে বাধ্য করে।

াবে সিস্টেমে প্রবেশ করে: ইন্টারনেট থেকে নিরাপত্তাহীন ওয়েবসাইটে কিছু ফাই
up ডাউনলোড করার মাধ্যমে।

কারণে ব্যবহার করা হয়: পপ-আপ অ্যাড ও স্পাম ছড়ানোর লক্ষ্যে অ্যাডওয়্যার ব্য

ওয়্যার ব্রাউজারের মাধ্যমে অতিরিক্ত বিজ্ঞাপন দেখায়। সেজন্য এটি অন্যান্য
াওয়্যারের মতো এতোটা ক্ষতিকর নয়।

Rootkit (রুটকিট)

ধরনের ম্যালওয়্যার যা হ্যাকারদের টার্গেট ডিভাইসে অ্যাক্সেস এবং নিয়ন্ত্রণ করার জন্য ডিজাই
ছ।

RAT

বে কম্পিউটার সিস্টেমে প্রবেশ করে: ফিশিং বা social engineering attack, অপারেটিং সি
ম।

রেটিং সিস্টেমের মাধ্যমে কম্পিউটার সিস্টেমে প্রবেশে করে এমনভাবে লুকিয়ে থাকে যে অ্যান্টি
সহজে শনাক্ত করা যায় না। রুটকিট দ্বারা সফটওয়্যার, অপারেটিং সিস্টেম, হার্ডওয়্যার, ফার্মও
গ্রস্ত হয় এবং হ্যাকাররা কম্পিউটার ব্যবহাকারীর পারসোনাল ইনফরমেশন জানতে পারে এবং
ত পারে।

্যার কম্পিউটার সিস্টেমে প্রবেশ করতে পারলে যেকোনো ধরনের ম্যালওয়্যার ইনস্টল করতে
tributed Denial of Service) attacks করতে পারে।

Browser Hijacking (ব্রাউজার হাইজ্যাকিং)

ধরনের ম্যালওয়্যার যা ব্যবহারকারীর অনুমতি ব্যতীত ব্যবহারকারীর ব্রাউজারে অযাচিত বিজ্ঞাপ
য়ার জন্য কোনো ওয়েব ব্রাউজারের সেটিংসকে পরিবর্তিত করে। একটি ব্রাউজার হাইজ্যাকার ি
পৃষ্ঠা, ত্রুটি পৃষ্ঠা বা সার্চ ইঞ্জিনটিতে নিজে নিজে প্রতিস্থাপন করতে পারে।

ারণে ব্যবহৃত হয়: কোনো নির্দিষ্ট ওয়েবসাইটকে হিট করার জন্য ব্যবহৃত হয়, এতে করে বিজ্ঞ
ম আয় বাড়ায়।

বে প্রবেশ করে: কম্পিউটার সিস্টেমে ইন্টারনেট থেকে 'Plugin' বা 'Extension' হিসেবে ডা
র মাধ্যমে।

page বা Browser-এ ক্ষতিকারক popup বিজ্ঞাপন দেখায় এবং ইচ্ছার বিরুদ্ধে অন্য Webs

Overwrite Virus (ওভাররাইট ভাইরাস)

স্টম সংক্রমিত হওয়ার পর, ওভাররাইট ভাইরাস তার নিজস্ব কোড দ্বারা য
টেন্টকে ওভাররাইট করা শুরু করে। এই ভাইরাস নির্দিষ্ট ফাইল বা
প্লিকেশনকে টার্গেট করে সংক্রমিত করতে সক্ষম। উদাহরণ: TRj.reboot

াবে কম্পিউটার সিস্টেমে প্রবেশ করে: কম্পিউটারে সিস্টেমের ফাইল এব
কানো ডিলিটকৃত ফাইলের মাধ্যমে।

ল এডিট করে সিস্টেমের ক্ষতি সাধন করে, সিস্টেমের মেমোরিতে ডেটা
ারাইট করে মূল প্রোগ্রামের কোড ধ্বংস করে।

ফায়ারওয়াল (Firewall)

রওয়াল শব্দের অর্থ: নিরাপত্তা ব্যবস্থার অদৃশ্য দেয়াল।

রওয়াল: এক সেট নিয়ম-নীতি বা Rules যা অনুসরণ করে এবং হার্ডওয়্যার ও
ওয়্যারের মিলিত প্রয়াসে কম্পিউটার সিস্টেমকে বাইরের আক্রমণ থেকে রক্ষা ব
, ফায়ারওয়াল হার্ডওয়্যার বা সফটওয়্যার উভয়ই হতে পারে।

মের অভ্যন্তরীণ এবং বাহ্যিক নিরাপত্তার একটি Protection System (নিরাপ
)।

ডিভাইস যা প্যাকেট ফিল্টার (Packet filters অপর নাম: Static Filtering
rs-এর কাজে ব্যবহার করা হয়।

কার্যপ্রক্রিয়া

রের নেটওয়ার্ক থেকে প্রেরিত ডেটা পরীক্ষা-নিরীক্ষা করে যদি কাঙ্ক্ষিত গ
য়ার অনুমতি থাকে তাহলে সেটিকে যেতে দেয়, অন্যথায় ব্লক করে।
াকাঙ্ক্ষিত এবং ক্ষতিকর যেকোনো কিছু আসলে ফায়ারওয়াল সেটিকে আস
া দেয় কিংবা ব্যবহারকারীকে সতর্ক করে।

ারওয়াল ব্যবহারের কারণ:

নুমোদিত (Unauthorized) রিমোট অ্যাক্সেস থেকে কম্পিউটারকে রক্ষা
াঞ্ছিত বিষয়বস্তুর সাথে সংযোগ স্থাপন করে Content-কে ব্লক করে।
লাইন গেমিং নিরাপদ করে। নেটওয়ার্কের ডেটা প্রবাহ নিয়ন্ত্রণ করে।

বচেয়ে গ্রহণযোগ্য ফায়ারওয়াল: অভ্যন্তরীণ
টওয়ার্ক ও ইন্টারনেটের মাঝে একটি কম্পিউটা
রাউটার ব্যবহার করে সমস্ত ট্রাফিক পর্যবেক্ষণ
রে বা নিয়ন্ত্রণ করে।

কারভেদ: ফায়ারওয়াল ২ প্রকার।

হার্ডওয়্যারনির্ভর ফায়ারওয়াল,

সফটওয়্যারনির্ভর ফায়ারওয়াল।

জনপ্রিয় Software Firewall:

ɔrton Internet Security

spersky Internet Security

:afee Internet Security

modo Internet Security

Tools Firewall Plus Free Edition

ıeAlarm Free Firewall

ıampoo FireWall Free

line Armor Free

ıitum Outpost Firewall Free

ɜeclab Personal Firewall Professional Edition

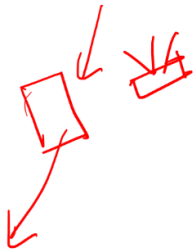
জনপ্রিয় Hardware Firewall:

co PIX

eck Point

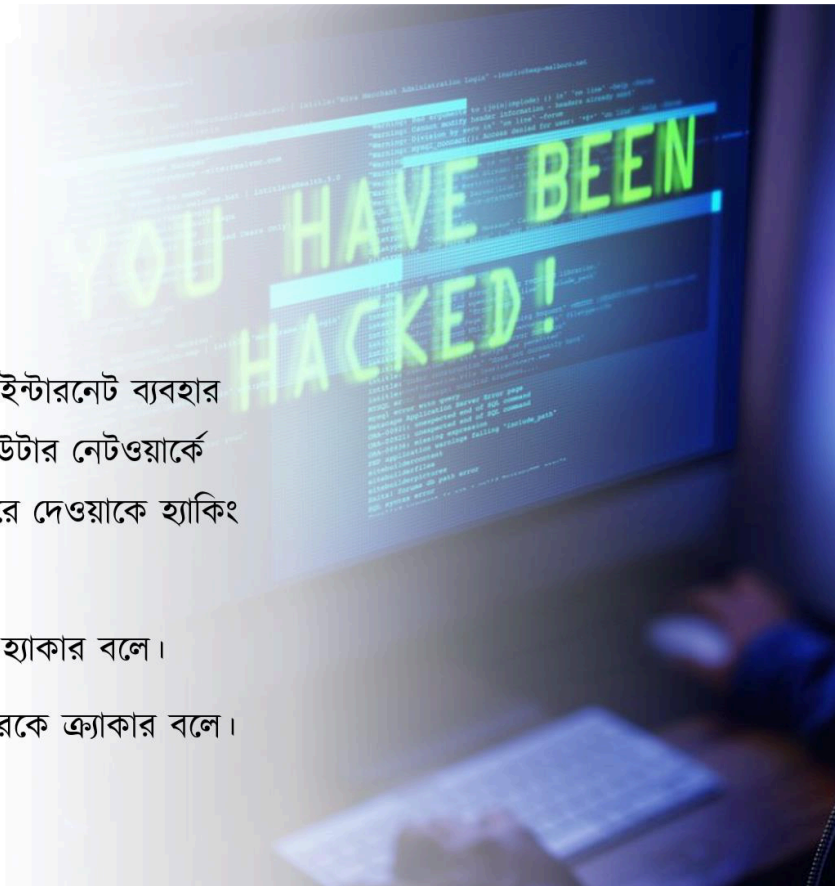
Γ screen

tchGuard



াইবার অপরাধ

- ইন্টারনেটের মাধ্যমে যেকোনো অপরাধ (যেমন: তথ্য চুরি, তথ্য বিকৃতি, ব্ল্যাক মেইল, মানি লন্ডারিং) কে সাইবার ক্রাইম বলে।



ং (Hacking)

চনা ও প্রয়োগের মাধ্যমে ইন্টারনেট ব্যবহার
মতি ব্যতীত কোনো কম্পিউটার নেটওয়ার্কে
রে ডেটা চুরি বা ধ্বংস করে দেওয়াকে হ্যাকিং

র সাথে জড়িত তাদেরকে হ্যাকার বলে।

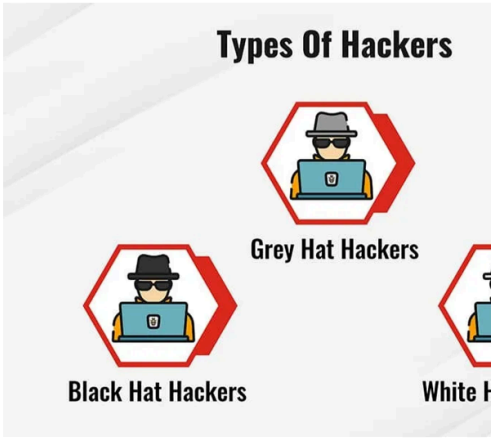
ধভাবে হ্যাকিং করে তাদেরকে ক্র্যাকার বলে।

হ্যাকার প্রধানত ৩ ধরনের-

হ্যাট হ্যাকার: যারা অ্যাডমিনিস্ট্রেটরের অনুমতি নিয়ে
হ্যাক করে দুর্বলতা খুঁজে বের করে এবং তা সমাধানে
রে। এদের কে ইথিকাল হ্যাকারও বলা হয়

ট হ্যাকার: তথ্য হাতিয়ে নেয়, আর্থিক ক্ষতিসাধন

হ্যাকার: অ্যাডমিনিস্ট্রেটরের অনুমতি না নিয়ে সিস্টেম
র নেটওয়ার্কের দুর্বলতা খুঁজে বের করে, দুর্বল
াকে ঠিক করার মাধ্যমে অর্থ উপার্জন করে।

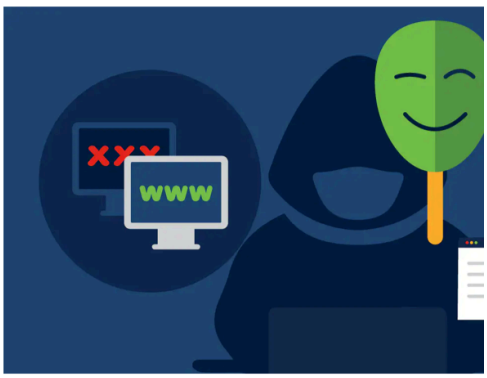


কিং (Phreaking)

টেলিকমিউনিকেশন
ম হ্যাক করে অসৎ
্য ব্যবহার করার
াকে ফ্রেকিং বলে। ফোন
াদের 'Phreaker' বলে।

স্পুফিং (Spoofing)

য়েবসাইটের মাধ্যমে আর্থিক তথ্যাদি
নেয়ার একটি সাধারণ পদ্ধতি।
র্ত মুহূর্তে ব্যবহারকারীরা গুরুত্বপূর্ণ
ত ও আর্থিক তথ্য দিয়ে স্পুফিং-এর
জড়িয়ে পড়ে।



ফিং (Sniffing)

- ট্রান্সমিশন লাইন দিয়ে তথ্য যাবার সময় তথ্যকে তুলে নে জনপ্রিয় পদ্ধতি। তার বা তারবিহীন ব্যবস্থাতে স্নিফিং কর স্নিফিং প্রতিরোধের একমাত্র উপায়: ডেটা এনক্রিপশন।

ফিশিং (Phishing)

াট ব্যবস্থায় কোন সুপ্রতিষ্ঠিত াইট হুবহু নকল করে এর নতুন ওয়েবসাইট তৈরি করে ্যক্তিগত তথ্য (যেমন: User Password) হাতিয়ে নেওয়াকে বলে।

ভিশিং (Vishing)

, টেলিফোন, ইন্টারনেটভিত্তিক
ফান বা অডিও ব্যবহার করে
রা। ফোনে লটারি বিজয়ের
া, টাকা পাঠানোর কথা বলে
ঠয়ে ব্যক্তিগত তথ্য হাতিয়ে
চেষ্টা করা।

ইবারথেফট (Cybertheft)

দ্দেশ্যে ব্যবহারের জন্য কিংবা
অবৈধ ব্যবহারের জন্য কম্পিউটার
করে ব্যবসায়িক অথবা ব্যক্তিগত
ুরি করা।

সফটওয়্যার পাইরেসি

ারীর বিনা অনুমতিতে কোনো
য়্যার কপি করা, আংশিক
ন করে নিজের নামে চালিয়ে
ত্যাদি কার্যক্রমকে বুঝায়।

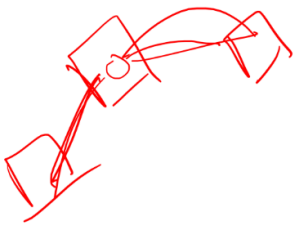
রিজম (Plagiarism)

ক্তি বা প্রতিষ্ঠানের কোন সাহিত্য,
া সম্পাদনা কর্ম হুবহু নকল বা
ারিবর্তন করে নিজের নামে প্রকাশ
ভিত্তিক অন্যের তথ্যকে নিজের নামে
ওয়া। সাইবার প্লেগারিজম
ual Property এর জন্য হুমকিস্বরূপ

ম্যান ইন দ্য মিডল

্মান কথোপকথন বা ডেটা স্থানান্তরকে বাধা দেয়

া স্থানান্তরের মাঝখানে নিজেদেরকে ঢোকানোর পরে আক্রমণকারীরা বৈধ
ণগ্রহণকারীর ভান করে।

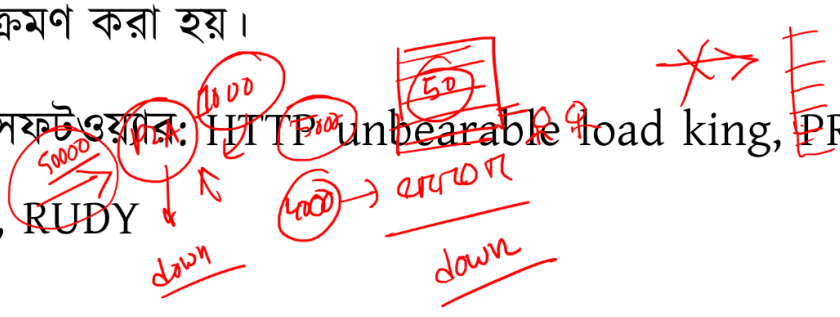


Denial of Service (DoS) Attack

নো কম্পিউটার, সিস্টেম বা ওয়েবসাইটে এই আক্রমণ সংঘটিত হলে
কের বৈধ অনুরোধসমূহ একটি ওয়েব সার্ভার সম্পূর্ণ করতে ব্যর্থ হয়

সিকিউর ওয়েবসাইটকে কিছু সময়ের জন্য ডাউন করে ফেলার জন্য
S আক্রমণ করা হয়।

প্রিয় সফটওয়্যার: HTTP unbearable load king, PRTG, LOIC,
Loris, RUDY



আলোচিত হ্যাকারগোষ্ঠী

ilored Access Operation, NPA: USA'র সরকারি
কার।

zy Bear : APT29 আইডেনটিটিধারী রাশিয়ান হ্যাকার গ্র
য়কটি হ্যাকার/হ্যাকারগোষ্ঠীর নাম: তুরলা (রাশিয়ান), গ্যাি
কিনন, লুলজসিক, কেভিন পলসেন, আদ্রিয়ান লামো,
ানাথন জেমস।