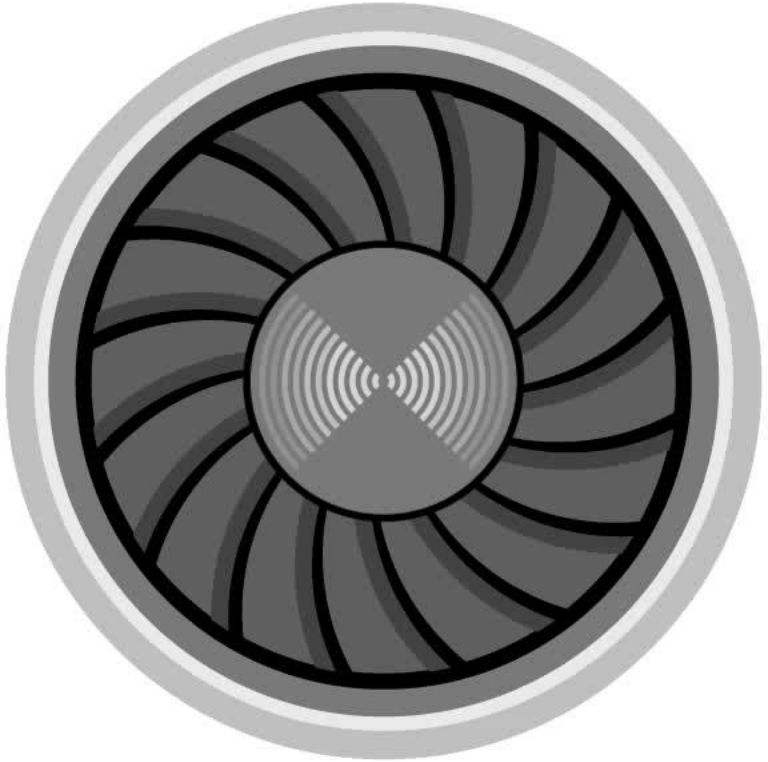
Deloitte.

cyber 101



Anatomy of a Cyber Attacker
Supplementary Reading

August 2017

Examples of Cyber Crime

Let's briefly go through the types of cyber crimes before understanding the types of cyber attackers.

Here are the most common types:

Hacking: an individual's computer is accessed without their knowledge and personal or sensitive information is stolen

IP Piracy: when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the authorities

Identity Theft: the use of an individual's personal credentials to impersonate the victim for unlawful personal gain. This can lead to financial losses for the individual and reputational damage for organisations.

Malicious Software: Software or programs that are used for a variety of criminal purposes. These software can be used to gain access to a system to steal sensitive information or data or cripple systems or networks.

Identity fraud reaching epidemic levels, new figures show

Fraud prevention service Cifas says there were a record 89,000 cases of identity theft in the first half of this year

Identities are being stolen at a rate of almost 500 a day, according to Cifas. Photograph: Tek Image/Getty Images/Science Photo Library RF

Identity theft has reached epidemic levels in the UK, with incidents of this type of fraud running at almost 500 a day, according to the latest figures.

http://www.crossdomainsolutions.com/cyber-crime/
https://www.theguardian.com/money/2017/aug/23/identity-fraud-figures-cifas-theft

One of the best ways to avoid being a victim of cyber crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet.

White Hats

Who are they?

White hat hackers use their powers for good and are also known as "ethical hackers," **white hat hackers can sometimes be paid employees or contractors working for companies as security specialists that attempt to find security holes via hacking.**

White hat hackers employ the same methods of hacking as black hats, with one exception- **they do it with permission from owners of the system, which makes the process completely legal.** White hat hackers perform penetration testing to validate security controls within the organisation. Ethical hacking skills can be acquired through various training and certifications.

Here are some known White Hat Hackers:

Steve Wozniak

Linus Torvalds

Tim Berners-Lee

Singapore

Ethical hackers on the frontline, keeping your home safe from cyber-attacks

The challenge of cyber security, in an age of growing digital connectivity, is explored on the programme Challenge Tomorrow.

SINGAPORE: It is not just computer systems and national infrastructure that are vulnerable to cyber-attacks. The emerging Internet of Things (IOT) - where devices such as smart watches, handphones and even kitchen appliances can connect to the Internet - means even your household is not safe.

http://www.channelnewsasia.com/news/singapore/ethical-hackers-on-the-frontline-keeping-your-home-safe-from-cyb-8577866
http://www.makeuseof.com/tag/5-worlds-famous-influential-white-hat-hackers/

"The smart watch is a very good example," said Mr Toh Jing Hui , Research Assistant from Singapore University of Technology, who would be considered a white hat or ethical computer hacker. "What the attacker can do is to infect your smartwatch with a malicious software that makes it run like a printer."

Black Hats

Who are they?

A black hat hacker is a person who **attempts to find security weaknesses and exploit them for personal financial gain or other malicious reasons**.

Black hat hackers can inflict major damage on both individuals and large organizations by stealing personal financial information, compromising the security of major systems, or shutting down or altering the function of websites and networks.

Here are some known Black Hat Hackers:

Lizard squad

Vladimir Levin

George Hotz

http://www.express.co.uk/life-style/science-technology/602157/Lizard-Squad-Hacking-Group-Ddos-Attack-PS4-Xbox-NCA
https://www.technotification.com/2014/12/top-10-best-black-hat-hackers-in-the-world.html
https://www.theguardian.com/technology/2016/aug/08/cyber-security-black-hat-defcon-hacking
http://thementalclub.com/top-5-black-hat-hackers-world-572

The state of cyber security: we're all screwed

Sophisticated cybercrime, privacy fears and ongoing confusion about security have soured the internet for many, and doing something about it won't be easy

An attendee at Black Hat, a hacking and cyber security conference in Las Vegas, watches a virtual reality video. Photograph: David Becker/Reuters

When cybersecurity professionals converged in Las Vegas last week to expose vulnerabilities and swap hacking techniques at Black Hat and Defcon, a consistent theme emerged: the internet is broken, and if we don't do something soon, we risk permanent damage to our economy.

A ransomware attack is relatively easy to overcome if you have a current and complete copy of your data; you can simply restore the untainted files to your machine, says Beyer. (Before you do, though, be sure to install security software that will remove the ransomware, or you may find yourself being jacked all over again, he warns.)

Grey Hats

Who are they?

A Grey Hat in the IT community refers to a **skilled hacker who toe the line of ethical boundaries.** Grey Hats usually do not hack for personal gain nor have malicious intentions.

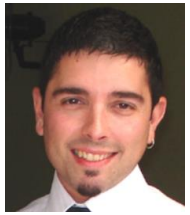
However, Grey Hats may occasionally commit crimes during the course of his/her technological exploits. **A grey hat will not necessarily notify the system admin of a successful compromise.** Such a hacker prefers anonymity at almost all cost, carrying out their activities undetected with as little forensic traces as possible.

Here are some common Grey Hat Hackers:

Kevin Mitnick

Robert T. Morris, Jr

Mark Abene



IT WORKPLACE

Experts divided on `grey hat' hackers

brian bloom @itworldca
Published: January 3rd, 2012

As criminal hackers become more sophisticated and ruthless, security-conscious companies are increasingly recruiting people to help fight a covert war.

On the front lines of the fight stand many "grey hat" hackers — security experts who have online street smarts but aren't mixed up in the racket themselves. A small number may have dabbled in "black hat," or underground hacking, in the past, but most just know how to communicate with the other side.

http://www.toptenz.net/top-10-infamous-hackers.php
http://www.itworldcanada.com/article/experts-divided-on-grey-hat-hackers/45669

"In order to get access to that information, at a minimum you need to turn to a grey hat hacker, who may have access to that side of the fence." says Dave Millier, CEO of Sentry Metrics, a Toronto-based security consulting firm

Hacktivism

What does Hacktivism mean?

Hacktivism is the act of hacking a website or computer network in an effort to convey a social or political message. The person who carries out the act of hacktivism is known as a hacktivist.

In contrast to a malicious hacker who hacks with the intent to steal private information or cause others harm, hacktivists engage in similar forms of disruptive activities to highlight political or social causes. For the hacktivist, hacktivism is an Internet-enabled strategy to exercise civil disobedience. Acts of hacktivism may include website defacement, denial-of-service(DoS) attacks, redirects, website parodies, information theft, virtual sabotage and virtual sit-ins.

What motivates them?

Hacktivism and hacktivists are motivated by an active desire to cripple government control and censorship of electronic and Web technologies and content. It is also their attempt at effecting change according to the beliefs they subscribe to.

As such, hacktivism may be employed by those opposing rigorous copyright regulations or fervently interested in circumventing restricted electronic data.

'This is just the beginning' Anonymous hackers take down nine banks in 30-day cyber attack

HACKING group Anonymous claim they have taken down central banks in Germany, Greece and Cyprus as they carry out a 30-day worldwide cyber attack.

By KATIE MANSFIELD
PUBLISHED: 17:45, Wed, May 11, 2016 | UPDATED: 17:52, Wed, May 11, 2016

SHARE TWEET 1K

Anonymous claim to have taken down nine national banks during a worldwide cyber attack

The activist hacking group, who have joined forces with fellow hackers Ghost Squad Attackers, are targeting bank websites across the world.

https://www.techopedia.com/definition/2410/hacktivism
http://www.express.co.uk/news/world/669346/Anonymous-hackers-take-down-nine-banks-in-30-day-cyber-attack

Digital Economy Minister Ed Vaizey said: "The UK is a world-leading digital economy and this Government has made cyber security a top priority. Too many firms are losing money, data and consumer confidence with the vast number of cyber attacks. It's absolutely crucial businesses are secure and can protect data."

4 Easy Ways to protect your organisation from cyber attackers

- **Know the risks**
  Properly protecting your company from a cyber-attack starts **with a comprehensive understanding of the internal and external threat exposure your organisation**. You will want to have an understanding of your assets and potential areas where hackers may gain entry to your organisation.

- **Encrypt your data**
  Keep your information safe by turning to encryption tools which come standard with most operating systems on.

- **Practise cyber hygiene**
  Cyber-attacks are not limited to networked systems. Practising good cyber hygiene and culture can dramatically raise your security posture. Activities like shredding your documents and physically locking your computer while you are away from your desk is a good place to start.

- **Be vigilant**
  Help employees understand the role they play in contributing to your organisation's security posture. Organise regular awareness campaigns to detect and report **potential threats and as well as awareness on how to keep information safe.**

https://www.entrepreneur.com/article/289680

cyber 101

As a business owner, you rarely think about the threat of cyber-attacks day-to-day, but when one happens to your businesses the result can be catastrophic. By making sure you have these basic security tips in place now, you can save yourself from a lot of preventable headaches down the line

Deloitte.