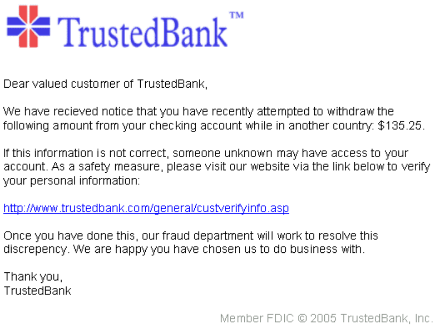
Piotr Rajewicz 23.10.2015

SHORT DESCRIPTION OF MOST COMMON THREATS

Phishing

Kind of a fraud which makes a victim provide a criminal with information such as credit card details or passport details. This kind of threaten is usually distributed by social networks or emails. To be protected from it you should not open links in fake emails, check if a website you enter is based on a HTTPS protocol or keeping your web browser updated.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

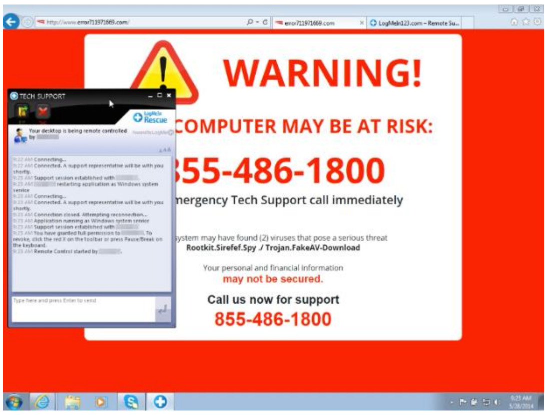
Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Fake Help Desk Calls

The way this threat works is that a victim receives a call from either a known or an unknown number. An answering machine, which sounds familiar and authentic, guide the victim to deliver information such as credit card details or ID details. The answering machines stops responding and the call ends. Having gained those details a criminal is able to do whatever he or she wants. Not only can Internet user protect themselves from these type of scams but also they can report it. By doing so they assure other users and themselves of more efficient security firewalls.



http://www.error711971669.com/

WARNING!

COMPUTER MAY BE AT RISK:

855-486-1800

mergency Tech Support call immediately

ystem may have found (2) viruses that pose a serious threat
Rootkit.Sirefef.Spy ./ Trojan.FakeAV-Download

Your personal and financial information
may not be secured.

Call us now for support
855-486-1800

TECH SUPPORT

Your desktop is being remote controlled by [redacted]

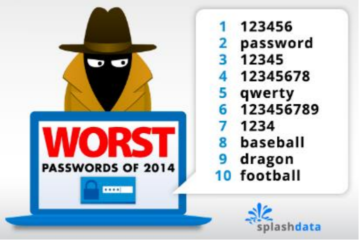
9:22 AM Connecting...
9:22 AM Connected. A support representative will be with you shortly.
9:23 AM Support session established with [redacted]
9:23 AM [redacted] restarting application as Windows system service
9:23 AM Connecting...
9:23 AM Connected. A support representative will be with you shortly.
9:23 AM Connection closed. Attempting reconnection...
9:23 AM Application running as Windows system service
9:23 AM Support session established with [redacted]
9:23 AM You have granted full permission to [redacted]. To revoke, click the red X on the toolbar or press Pause/Break on the keyboard.
9:23 AM Remote Control started by [redacted].

error711971669.com
LogMeIn123.com – Remote Su...
LogMeIn Rescue
Type here and press Enter to send
9:23 AM
5/28/2014

Password Attacks

Easy passwords

Establishing an easy password for a user name makes it very easy to gain an access to an account with some important information. The easy password is said to be the one consisting of three or more digits in the order (1, 2, and 3) or a few letters of which none are captivated. A hacker has no problem with guessing the password especially if a victim is known by the hacker or if the victim left some information in the Internet.



Dictionary

This type of a threat occurs when a hacker tries to type many common word and guess a password. The hacker succeed in hacking the password since vast majority of Internet users pay no particular attention to the strength of their passwords.

Brute-force

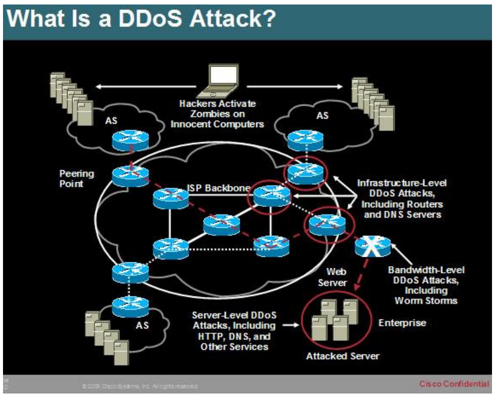
What describes this kind of a threat is it algorithm. It looks up all possible passwords rather than focusing on a detailed analysis.

Denial of Service (DoS)

What overuse an application serving certain data making it unable to sending and receiving more data is called DoS. Not only does it cause the loss of network connectivity but also it can have an effect in the loss of files.

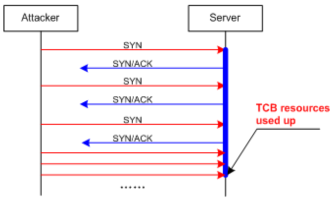
Distributed Denial of Service (DDoS)

A kind of a threat which overtake all resources available through numerous computers (*zombies)* simultaneously is called DDoS. The way it works basis on an interruption of receiving and sending data which causes a loss for a company.


What Is a DDoS Attack?
Hackers Activate Zombies on Innocent Computers
AS
AS
AS
Peering Point
ISP Backbone
Infrastructure-Level DDoS Attacks, Including Routers and DNS Servers
Web Server
Bandwidth-Level DDoS Attacks, Including Worm Storms
Server-Level DDoS Attacks, Including HTTP, DNS, and Other Services
Enterprise
Attacked Server
Cisco Confidential

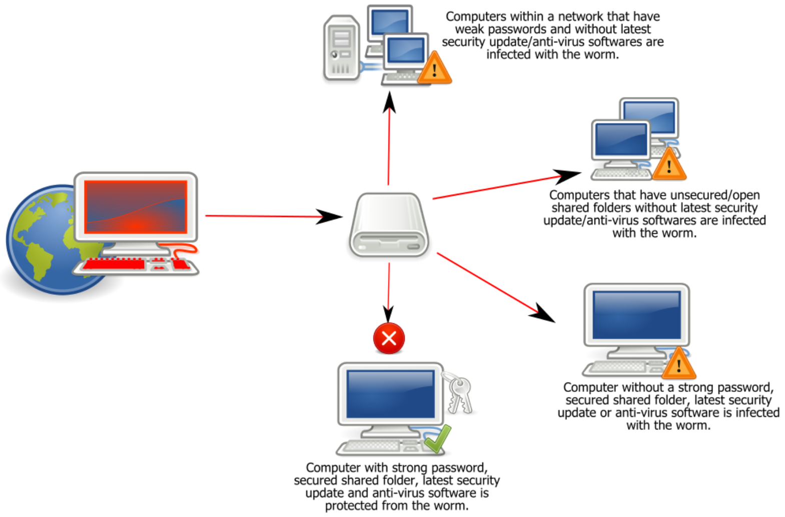
SYN Flood

The name of a threat describes this threat method. Mainly, it sends a succession of SYN request what means it wants to use a server resources in depth in order to make a server unavailable and unresponsive. It uses TCP protocol.



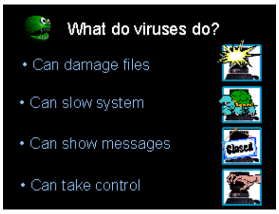
Worms

The next kind of a threat that will be presented uses a computer program which is a standalone malware. The program is used so as worms can be replicated among user's network holding on to their independence. By entering through systems vulnerability worms are said to usually harm a system and damage whole structure of a machine.


Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.
Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.
Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.
Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

Virus

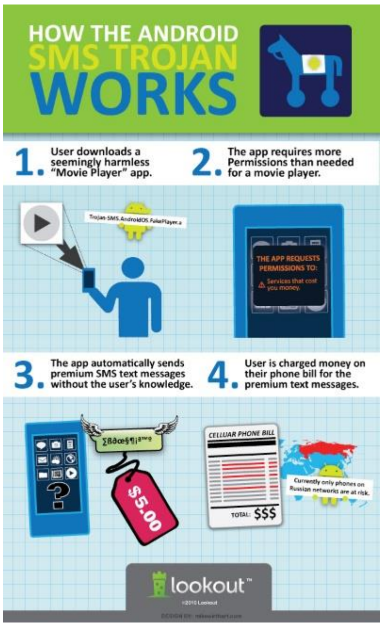
This kind of malicious software works just like human viruses, which means it can be replicated by using copies of itself into structures of a machine. What it does is to make a damage to internal structures of a machine such as for example disk space or CPU time. The reason why it is undesirable is it influence on computer resources, maintenance costs, corrupting data etc.


What do viruses do?

- Can damage files
- Can slow system
- Can show messages
- Can take control

Trojan horse

Trojan horse has its name thanks to its similar strategy as the ancient Trojan horse. It seems for a user that a software he or she is about to download is just an innocent program that actually makes the users life better. The unwitting user goes through the installation process that cause the installation of Trojan. This kind of a threat uses mostly all of the methods available in the IT world that is why users need to be aware of them and protect themselves as much as they can.


HOW THE ANDROID
SMS TROJAN
WORKS

1. User downloads a seemingly harmless "Movie Player" app.

2. The app requires more Permissions than needed for a movie player.

Trojan-SMS.AndroidOS.FakePlayer.a
THE APP REQUESTS PERMISSIONS TO:
⚠ Services that cost you money.

3. The app automatically sends premium SMS text messages without the user's knowledge.

4. User is charged money on their phone bill for the premium text messages.

∑ßðœ§¶¡ª™º
$5.00
CELLUAR PHONE BILL
TOTAL: $$$
Currently only phones on Russian networks are at risk.
lookout™
©2010 Lookout