zvelo
We categorize the Web

Definitions of the Malicious Web

MALICIOUS SOFTWARE

Denial of Service tools
The prevention of authorized access to a system resource or the delaying of system operations and functions.

Phishing
The use of emails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the email and website look like they are from a bank with which the user is doing business.

Worm
A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Polymorphic Malware
Malicious software that changes its underlying code to avoid detection.

Metamorphic Malware
Malicious software that is capable of changing its code and signature patterns with each iteration.

Spam
Electronic junk mail or junk newsgroup postings.

Trojans & Backdoors
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus
A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Logic bomb
Programming code, inserted surreptitiously or intentionally, that is designed to execute (explode) under circumstances such as the lapse of a certain amount of time or the failure of a user to respond to a program – a delayed-action computer virus or Trojan.

Man in the browser malware
A security attack where the perpetrator installs a Trojan on a victim's computer that's capable of modifying that user's Web transactions as they occur in real time. MITB takes advantage of vulnerabilities in browser security.

RAT
A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer.

Password crackers
Applications programs used to identify an unknown or forgotten password to a computer or network resources. It can be used to help a human cracker obtain unauthorized access to resources.

Bitcoin Miners
User systems mine for Bitcoin without the owners' knowledge and funds are channeled to the botnet master.

Adware
Software that automatically displays or downloads advertising material (often unwanted) when a user is online.

Exploit Kits
A type of malicious toolkit used to exploit security holes found in software applications for the purpose of spreading malware.

(continued)

Drive-by Downloads
A program that is automatically installed on your computer when you're visiting a booby-trapped website. The malicious program is downloaded to your computer without your consent or knowledge, without you having to click on a link on the page or in the email. Drive-by's are typically carried out by exploiting browser vulnerabilities.

Bot
A program that operates as an agent for a user or another program or simulates human activity.

Rootkit
A type of Trojan that keeps itself, other files, registry keys and network connections hidden from detection. It enables an attacker to have "root" access to the computer, which means it runs at the lowest level of the machine.

Ransomware
A type of malicious software designed to block access to a computer system until a sum of money is paid.

Spyware
Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Advanced Persistent Threat
A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.

FRAUD

Online Pump and dump/stock market manipulation
A form of microcap stock fraud that involves artificially inflating the price of an owned stock through false and misleading positive statements, in order to sell the cheaply purchased stock at a higher price.

Credit card fraud
A form of identity theft that involves an unauthorized taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it.

Online banking fraud
A form of activity wherein a malicious party steals banking related information via the use of various types of malware (e.g. MITB) to subvert a victim's bank account.

Dating fraud or "catfish"
Scammers post profiles, using stolen photographs of attractive persons, asking for others to contact them. Correspondence is exchanged; after the scammer feels they have groomed the victim enough, they ask them for money for airline tickets to visit them, medical expenses, education expenses, etc.

Advertising Fraud
Registered clicks or impressions that cannot be viewed by a human. This may mean the activity was generated by non human traffic, or that the ads were stacked on top of each other, served into 1x1 pixels or are generated in other methods that makes them non-viewable by humans.

Donation and Disaster Relief Fraud (Charity Fraud)
Fraudsters take advantage of highly publicized emergencies and bogus charities pop up under the guise of helping victims. Disaster relief fraud is a cyclical problem because the success of fraudsters who run such schemes encourages them to repeat the crime over and over for different disasters.

Other scams
Fraudsters use any topic to which they can get a response – lottery scams (you've won!), inheritance scams (you've been left money!); tax scams (your identity is used to fraudulently file taxes and claim a refund) and 419 scams (you are promised a significant share of a large sum of money, it takes a small up-front payment to obtain)