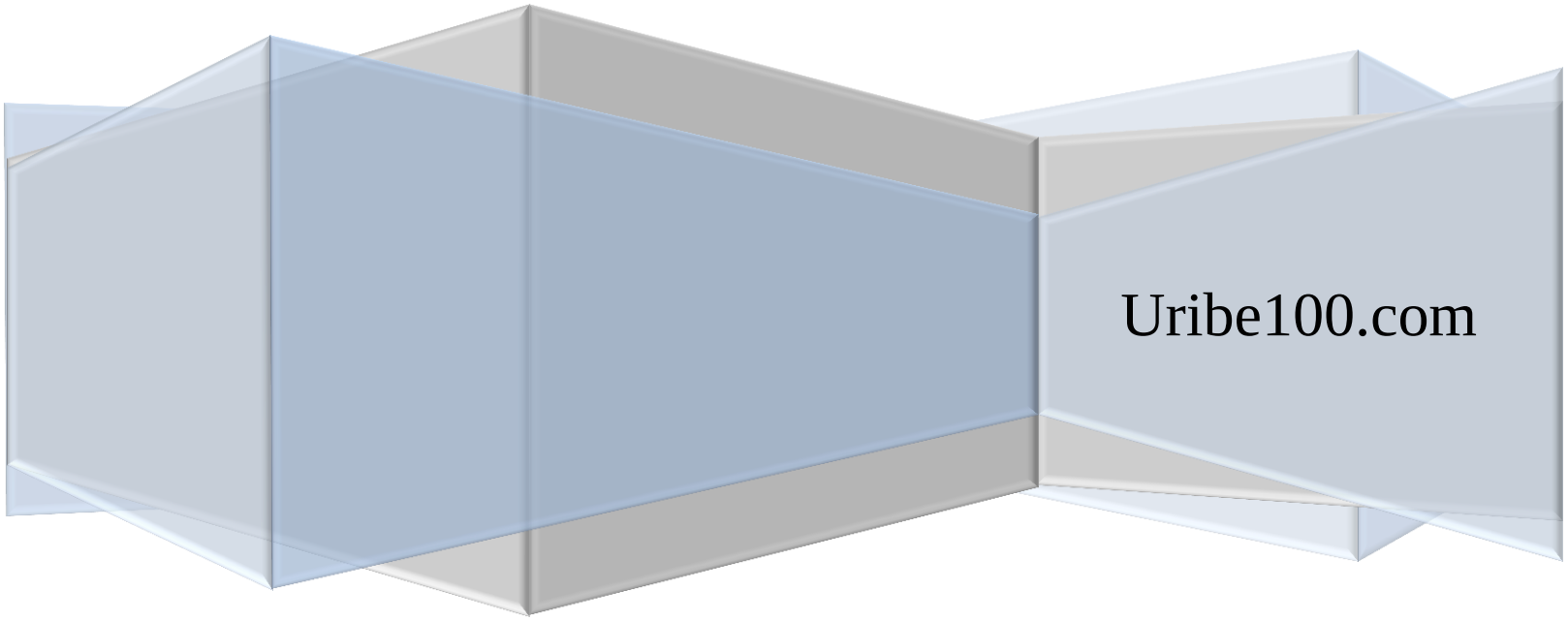
Malsubjects and Malware

The Malicious Combination

By Felix Uribe



"Malsubject" (**Mal**icious **Subject)** is an unauthorized individual or subject whose activities are intended to break into an Information System (IS) with malicious intent to compromise the information's confidentiality, integrity, or availability of organizations and individuals. Malsubjects include hackers, cyber-thieves, spammers, hacktivist, and nation states among many others.[1]

It is easier to identify these individuals in the cyber security space by one common name instead of several, such as bad actors, threat actors, bad guys, cybercriminals, and others. The term malsubject defines these individuals regardless of their intended actions. After all, their intentions are always malicious in nature, no matter who they are or what we label them.

The term "malware", or Malicious Software, is defined by the National Institute of Standards and Technology's (NIST) Glossary of Key Information Security Terms[2] as *"a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim."* Malware by this definition include viruses, worms, trojan horses, or other code-based malicious entity that successfully infects a computer system.

Because malsubject provides an opportunity to identify all types of "cyber bad guys" with a single term, the term "malware" ought to include, in addition to malicious programs, malicious hardware (e.g. ATM and gas pump skimmers) or malicious techniques (e.g. social engineering). Malicious hardware gets inserted into a system (physically and covertly) with the intent of compromising the victim's data. Malicious techniques are also used on individuals with the purpose of tricking them into performing actions or divulging information in order to gain access to information system's data. As a result, I use "malware" in general terms to identify malicious software, hardware, and techniques used to perform cyber-attacks.

In the world of cybercrime and cyber warfare, the fight is always aimed to prevent malsubjects and malware from penetrating information systems of public and private organizations as well as individual systems. It is clear that malsubjects using selected malware can identify, target, and attack all types of IS infrastructure. Once an attack is successful, the results and consequences of these malicious actions become a series of unfortunate events played against individuals and organizations.

[1] Felix Uribe (2012). Protecting your Computer Against Malware and Malsubjects. Retrieved from http://www.uribe100.com/protectingyourpcagainstmalwareandmalsubjects.pdf
[2] NISTIR 7298 Revision 2 Glossary of Key Information Security Terms, May 2013.

The latest Verizon's 2013 Data Breach Investigations Report (DBIR)[3] stated that the 2012 combined dataset of security incidents analyzed for the report represented the largest they have ever covered in any single year, spanning more than 47,000 reported security incidents; 621 confirmed data disclosures; and at least 44 million compromised records. Unfortunately, these security incidents will continue to become regular news as malsubjects intensify their efforts using more and more sophisticated malware. For example, the recent malsubject attack on the Target Corporation produced a breach that exposed personal information on millions of its customers[4]. Figure 1 shows some of these malicious actions.

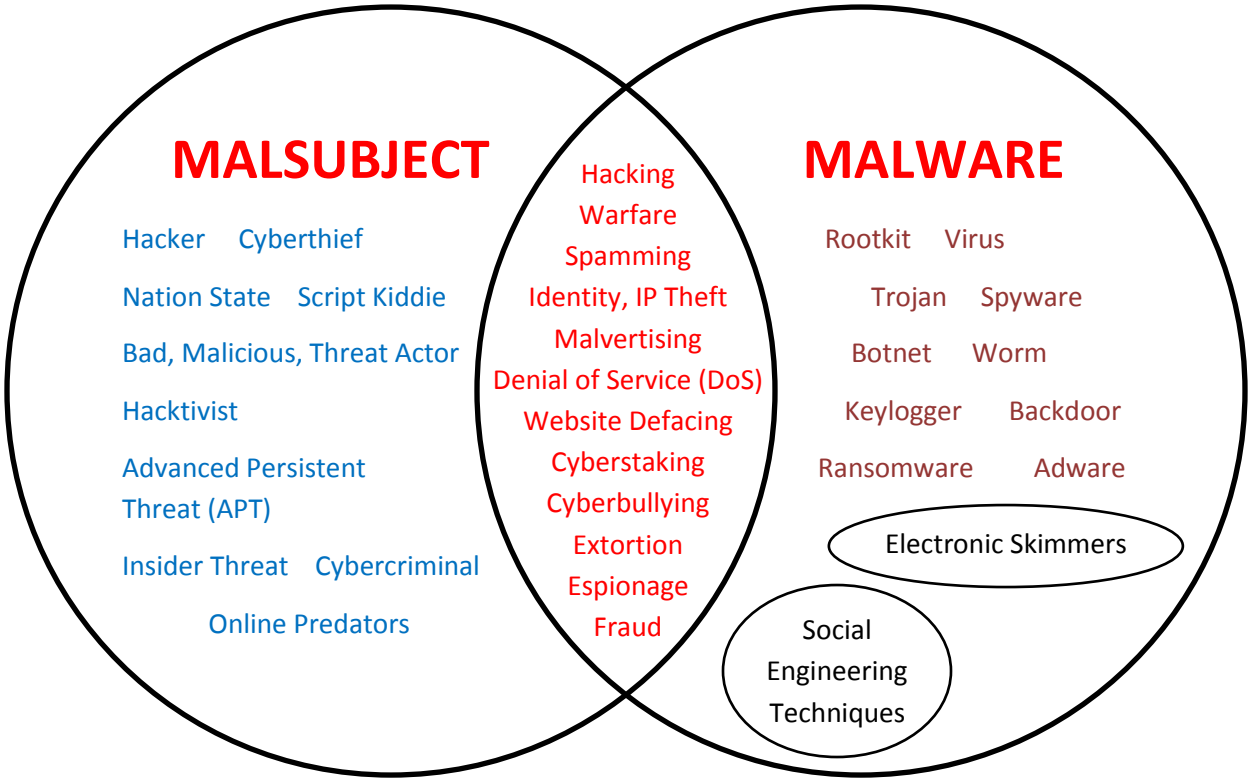


Figure 1: Malicious actions committed by malsubjects using selected malware include hacking, spamming, identity theft, espionage, denial of service and many others.

An effective cyber defense against attacks from malsubjects requires technologies, people, and processes capable of preventing or mitigating the damage caused by their malicious activities. Effective security controls and security awareness training are the best weapons against their intrusions.

[3] The 2013 Verizon's Data Breach Investigations Report was produced based on a collaboration of 19 global organizations that study and combat data breaches all over the world.

[4] Maggie McGrath. (2014, January 10) Target Data Breach Spilled Info On As Many As 70 Million Customers. Retrieved from http://www.forbes.com/sites/wochit/2014/01/10/target-announces-data-breach-for-70-million-customers-video/

According to NIST, *"using the risk management tools and techniques that are available to organizations is essential in developing, implementing, and maintaining the safeguards and countermeasures with the necessary and sufficient strength of mechanism to address the current threats to organizational operations and assets, individuals, other organizations, and the Nation"*[5].

Well implemented security controls based on appropriate risk management tools and techniques increase the odds of preventing many of the cyber-attacks currently affecting information systems and infrastructures all over the world. Figure 2 lists some of the safeguards and countermeasures that are implemented in order to maintain the confidentiality, integrity, and availability of the data used by individuals and organizations.

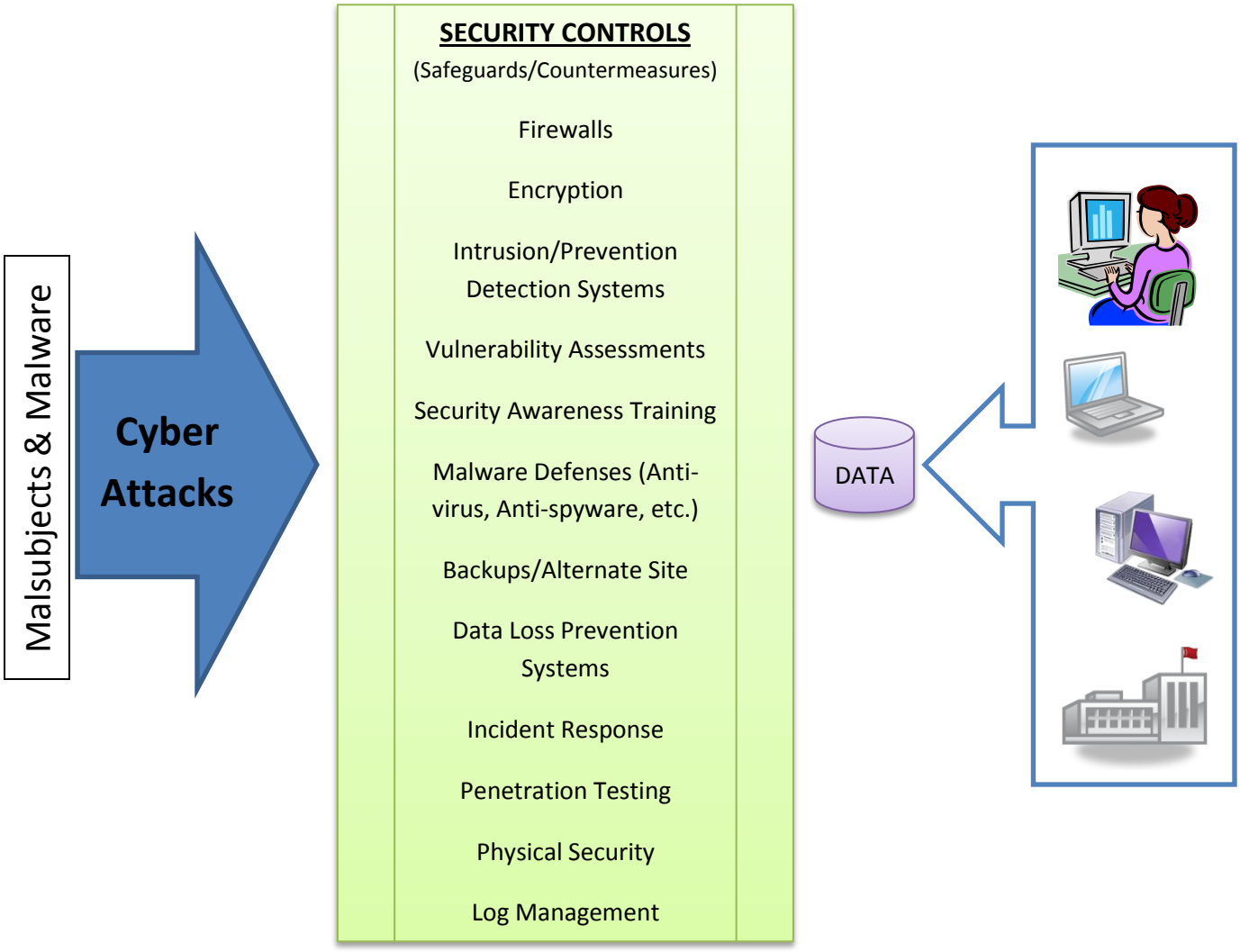


Figure 2: Safeguards/countermeasures used to prevent and stop cyber-attacks.

[5] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

In today's cyber space malsubjects span from one individual to organized crime groups and nation states capable of conducting sophisticated cyber-attacks from the most remote places in the world. All they need is a communication line to the public internet or private networks and the use of well-crafted malware to reach their targets. We might not be able to prevent them from reaching the system boundaries, but with good implementation of security controls; appropriate risk management tools and techniques; and constant security awareness training for organizational staff and the general public, we can slow down and someday we might be able to stop their advances.

