Chapter 29
Lawful Trojan Horse

Bruce L. Mann
Memorial University, Canada

ABSTRACT

News outlets don't usually report on training methods in counter-cyberterrorism, particularly lawful trojan attacks. Instead they describe recent cyberterrorist attacks, or threats, or laws and regulations concerning internet privacy or identity theft. Yet Europe is looking to do just that to head-off the next major cyberattack by creating rules for how member states should react and respond. Several news outlets, for example, reported that Germany's Federal Criminal Police Office (BKA) were using a Trojan Horse to access the smartphone data of suspected individuals before the information was encrypted. Although the urge to strike back may be palpable, hacking-back can put power back into the hands of the suspect. The consensus now is that government action is preferable to hacking-back at attackers.

HACKING THEN AND NOW

Hacking originally implied an extraordinary computer skill to extend the limits of a computer system (Chatterjee, 2019; Merisalo, 2020). Hacking required great proficiency. Today however, code libraries and automated tools available on the Internet make it possible for anyone with the will, to intrude into a computer network. The consensus is that attackers will attack a computer network in five phases (Chatterjee, 2019; Merisalo, 2020):

Phase 1. Reconnaissance

Reconnaissance is the first phase of hacking where the attacker collects information about the target (Chatterjee, 2019). This may include identifying the target, finding out the target's IP Address Range, Network, DNS records. Attackers are often motivated by financial gain, access to sensitive information or damage to brand, so the attacker's first goal is to identify potential targets for their mission (Merisalo, 2020). The attacker's aim is to acquire the names, positions, and email addresses of the target individual or group. The attacker may collect information about the company from LinkedIn and the corporate

DOI: 10.4018/978-1-6684-3698-1.ch029

website, map the supply chain, get building blueprints, information on security systems and available entry points. They may even visit the company building, an event or call the secretary. The attacker might set up a fake company, register domains and create fake profiles for social engineering purposes. Once the attacker determines what defenses are in place, they choose their weapon. The selected vector is often impossible to prevent or detect. It can be a zero-day exploit, a spear-phishing campaign or bribing an employee. Usually there is a minimal business impact. Finally, the attacker is ready to plan an avenue of attack.

Phase 2. Scanning

Scanning is the second phase (Chatterjee, 2019). At this phase the attacker seeks to breach the corporate perimeter and gain a persistent foothold in the environment (Merisalo, 2020). They may have spear-phished the company to gain credentials, used valid credentials to access the corporate infrastructure, and downloaded more tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. This activity is virtually untraceable. The attacker wants details, such as computer names, IP addresses, and user account numbers by which the attacker perpetrates the attack. The initial intrusion is expanded to persistent, long-term, remote access to the company's environment. They begin testing the network for other avenues of attack, using a couple methods, to help map the network. The attacker then needs to contact someone to see which email server is currently in use. They are looking for an automated email if possible, or based on the information gathered so far, email HR with an inquiry about a job posting.

Phase 3. Gaining Access

Gaining access is the third phase of hacking (Chatterjee, 2019). During this phase the attacker, having finished enumerating and scanning the network, now decides to explore options for gaining access to the network. Based on data collected during Phases 1 and 2, the attacker develops a blueprint of the target network. Their goal is to expand the foothold and identify the systems housing the target data (Merisalo, 2020). The attacker searches file servers to locate password files and other sensitive data, and maps the network to identify the target environment. Using any number of options, such as a phone app, website email spoofing, or zmail, the attacker sends-off a email asking users to login to a new Google portal with their credentials. A *Social Engineering Toolkit (SET) is* also initiated for penetration testing, and an email sent with the server address to the users, masking it with *bitly* or *tinyurl* to shorten the URL and manage the links. The attacker is often impersonating an authorized user. It's difficult to spot an attacker in this phase.

Phase 4. Maintaining Access

Maintaining access is the fourth phase of hacking (Chatterjee, 2019). Since control over access channels and credentials was acquired in the previous phases, the attacker now seeks to identify and gain the necessary level of privilege to achieve their objectives (Merisalo, 2020). The attacker has acquired multiple e-mail accounts. They begin testing the accounts on the domain. An administrator account is created based on the naming structure to blend-in. As a precaution, the attacker identifies accounts that have not been used for a long time, assuming they are either forgotten or abandoned. The attacker