8

THE CYBERSPACE CHANNEL

Within the complex domain that we call CYBER, there are three basic types of deception. One supports cyber offense; one is a part of cyber defense; and one supports deception operations that transcend the cyber domain. Many of the examples in this chapter are of the first two types: They describe deception where the objective was a cyber target, and the deception remained entirely in cyberspace. But deception can be conducted in cyberspace to support operations across all of the PMESII domains. It is used to support covert actions and influence operations. It is used to manage perceptions, beliefs, and understanding, and to create a flawed situational awareness among individuals or groups, thus increasing the chance that deception will succeed. It can be a powerful tool for conducting deception against a defined group as discussed in Chapter 1.

Cyberspace is especially important for today's military. Some military leaders consider it a complementary domain to support real-time operations by land, sea, air, and special operations components. Others argue that, from a military doctrinal perspective, cyberspace is an independent domain for operations. As conflict is moving more into cyberspace, it appears to be etching out a fifth battlespace domain—cyber—to join air, land, sea, and space. The last five years have seen many countries in the West establishing cyber commands for the express purpose of managing cyber warfare as a fully integrated battlespace domain. Consequently, deception—one of the important tools for winning conflicts—must move there also. And it has.

Chapter 7 addressed the deceiver's own intelligence channels as having two distinct roles in deception. One role is to provide intelligence that supports the deception: assessing the targets, constructing the story, identifying the opponent's channels, and assessing deception effectiveness. The second role is to identify an opponent's deception attempts. Chapter 7 also noted the importance of knowing the opponent's intelligence channels for projecting a deception.

The cyberspace channel serves all of these functions in deception operations. But the cyberspace channel has become a key one for projecting a deception, and for that reason it is treated in this separate chapter. Before discussing the various subchannels, let's review some of cyberspace's unique features.

DECEPTION IN CYBERSPACE

Up front, an important definition must be understood. Although this chapter is about deception in cyberspace, the term *cyber deception* is applied in only one section. The term has a specific meaning in the cyber community and, from its perspective, a narrow one. Cyber deception refers to a set of deceptive tactics and strategies in cyberspace that is used to defeat cyber attack and exploitation—that is, to defeat hacking. This type of deception is discussed extensively in many books and articles.[1] But cyber deception also potentially has a useful role in projecting deception; that role is discussed in the last section of this chapter.

Deception in the cyber domain shares features with counterintelligence, specifically counterespionage. Counterespionage has often been referred to as a "wilderness of mirrors"—a term credited to the CIA's former head of counterintelligence, James Jesus Angleton, when he described the confusion and strange loops of espionage and counterespionage. Deception in cyberspace shares similar characteristics.

For the purposes of this book, and to remain within the focus of intelligence support to a deception plan, CYBER here is treated as a two-way channel from which information can be extracted to support planning, as well as a communication platform from which to project information in executing the deception. The cyber realm therefore divides into two broad types: computer network exploitation (CNE), which is basically passive, and computer network attack (CNA), which is unquestionably active. Both have roles to play in deception: CNE, for collecting intelligence, and CNA, for projecting a deception by providing material to the target to support the deception.

So the World Wide Web via the Internet is a primary channel for conducting CNE/CNA. But the web can be an effective channel for projecting a deception without using CNA, as discussed next.

WEB-BASED DECEPTION

In 2012 a popular US television commercial featured a young woman proclaiming, "They can't put anything on the Internet that isn't true." In response to the question "Where'd you hear that?" she responds, "The Internet."

The Internet and its associated social media provide what is probably the most commonly used channel for deception by governments, organizations, and individuals today. The extensive development of cyber-based social media and information sources over the past fifteen years has opened a richly dynamic environment in which to conduct deception and counterdeception. It literally provides the communication backbone for a wide variety of possible channels to and from adversaries that can be used to monitor, analyze, and exploit.

In the world of cyber operations, much attention is paid to malware—computer viruses and those who develop and deploy them. The succeeding sections delve into these more aggressive techniques of cyber operations. But first, let's investigate the web as a channel for projecting deception much as it is done in traditional open-source publications.

News and Reference Media

Over several centuries, first newspapers, then radio (think of the Atlantiksender case described in Chapters 3 and 7), then television, became the primary sources of news reporting. Today the Internet seems on its way to dominating such reporting. Yet it is the most vulnerable of all media for conducting deception by planting false news reporting. More recently, the dominant deception has taken the form of *fake news*. Fake news websites promulgate false information and hoaxes, often by appearing to be legitimate journalistic reporting. The sites then rely on social media (discussed later) to spread the message. They offer a major new tool for applying deception in psychological warfare. As such, they can be used to affect elections and consequently to shape government policy. Fake news, during 2016, reportedly had an effect on the outcome of the UK referendum on exiting the European Union (Brexit) and on the US presidential election—a phenomenon that led the Oxford dictionary to choose *post-truth* as its word of the year. *Post-truth* is defined as circumstances in which "objective facts are less influential in shaping public opinion than appeals to emotion and personal belief."[2] German chancellor Angela Merkel, alarmed at this trend and the prospect of fake news affecting the 2017 German elections, observed, "Something has changed—as globalization has marched on, [political] debate is taking place in a completely new media environment. Opinions aren't formed the way they were 25 years ago. Today we have fake sites, bots, trolls—things that regenerate themselves, reinforcing opinions with certain algorithms and we have to learn to deal with them."[3]

The web also has become the primary source for research about almost any topic. The web pages that search engines lead to, and online reference sites, are excellent places to plant misleading information. Sites that have editors or a validation process, such as Wikipedia, are somewhat better suited to defend against deceptive inputs, but they are not immune. Ironically, on its own site, Wikipedia displays an article noting that it has been banned by many academic institutions as a primary source due to reliability and credibility issues.[4] The increased access to CYBER has increased the depth and scope of "common knowledge" available, leaving artists of deception projection an easily accessible canvas for "designing common knowledge" through sites such as Wikipedia and blogs.

E-mails

E-mails that appear to come from a trusted source have a well-known role in emplacing malware. But such e-mails also can be used to project a deception. Sometimes, it isn't even necessary to impersonate a trusted source. Prior to operation Desert Storm, PSYOPS specialists from the coalition called senior Iraqi officers directly on their personal cell phones and sent e-mails to their personal accounts, attempting to induce them to surrender and providing deceptive information about the upcoming conflict. These measures developed a level of discord and mistrust among the senior Iraqi leadership that had a definite adverse impact later on in the conflict.[5] To return to the terms introduced in Chapter 1, this was an "A" type deception.

Cyber operations to acquire e-mails can be a powerful tool in PSYOPS, as demonstrated in Russian cyber activities prior to the 2016 US elections. US intelligence agencies concluded that Russia conducted a cyber operation to obtain—and subsequently release—information from e-mails that damaged the campaign of Democratic nominee Hillary Clinton, while withholding damaging information they had collected from e-mails of Republican nominee Donald Trump.[6]

Social Media

Social media may be the most widely used channel for deception today. Individuals, organizations, and governments convey deceptive information via social media for both worthy and nefarious purposes. Because it is difficult to determine that a profile presented on the Internet is that of an identifiable person, deception is easy to pull off. Such deception is, in effect, an online version of pseudo operations.

Law enforcement uses social media, for example, to ensnare online sexual predators via posts that appear to come from young girls. Websites pretending to recruit for Daesh are used to identify and arrest would-be Daesh volunteers.

Social media is readily used in deception to further government objectives. A Harvard University study found that the Chinese government produces about 488 million false social media posts a year in an effort to divert attention away from sensitive issues. Most of the bogus posts are designed to indicate popular support for the government. They appear to be written by workers at government agencies assigned to make the posts in addition to their regular duties.[7]

Deceptive posts such as the Chinese example often are the work of Internet trolls—persons either anonymous or using assumed names. These posts typically are intended to advance causes and influence thinking through emotional appeals. The Russian government has developed a sizeable team of Internet trolls who regularly post deceptive information in an ongoing psychological operations campaign to undermine NATO and US interests and promote Russian interests.[8]

Social media such as Twitter, YouTube, Facebook, Instagram, and blogs are just the tip of the iceberg of available cyber social networks that contribute significantly to the formation of public opinions and perspectives across national borders. It has been demonstrated repeatedly that "going viral" in social media can quickly inspire violent events in the physical domain. A single picture illustrating political hypocrisy can in a matter of seconds weaken international alliances abroad, and undermine support for policy at home. Perhaps the most dramatic outcome of this online mobilization, Internet activism, and grassroots organization occurred in 2011. The events of that year that became known as the Arab Spring started in Tunisia and spread rapidly to Egypt and Libya, toppling governments in all three countries, and to Syria, sparking what seems to be an endless conflict that has drawn in major powers.

Memetic Conflict

Deception plays a major role in a new area of interstate and intercultural conflict known as memetic warfare or *memetic conflict*. A meme (derived from the word *gene*) is an idea or type of behavior that spreads from person to person within a population. It is a carrier of cultural ideas, symbols, or practices from one person to another through writing, speech, gestures, symbols, or rituals.

The term *meme* was introduced by Oxford professor Richard Dawkins in his 1975 book *The Selfish Gene*. Though the name is of recent origin, the meme obviously has been around for a long time in human affairs. But it has become a powerful tool for shaping opinions and actions in the era of social media.

Memetic conflict has been defined as "competition over narrative, ideas, and social control in a social-media battlefield. One might think of it as a subset of 'information operations' tailored to social media."[9] In contrast to cyber conflict,

> Cyber warfare is about taking control of data. Memetic warfare is about taking control of the dialogue, narrative, and psychological space. It's about denigrating, disrupting, and subverting the enemy's effort to do the same. Like cyber warfare, memetic warfare is asymmetrical in impact.[10]

So memetic conflict is a new type of psychological warfare. In this conflict, Internet trolls play a critical role. They are the warfighters of the Internet, and memes are their weapons.[11] For nonstate actors such as Daesh, memetic warfare has been a powerful tool for spreading their message, motivating their supporters, and attracting recruits to the cause.

Of course, the tools of these conflicts can be used by both sides. In a memetic conflict campaign against Daesh, for example, it has been suggested that one could

- Systematically lure and entrap Daesh recruiters
- Create fake "sockpuppet" Daesh recruiting sites to confuse sympathizers and recruits
- Expose and harass those in the Daesh funding network, along with their families
- Weaken the Daesh appeal to supporters and possible recruits by enlisting gay activist trolls to start and spread a #ISISisgay hashtag[12]

Techniques such as these are easily applied by, for example, the Russian government. They would pose both political and legal problems for many Western governments that tried to apply them. The United States, for example, is not allowed to spread propaganda domestically, and social media knows no borders.[13]

WEB-BASED CNE/CNA

The preceding section discussed a straightforward use of the cyber realm to project a deception; such use requires no specialized technical expertise. This section is about applying the tools of cyber operations for obtaining intelligence or to project a deception. Cyber offense falls into two broad objectives when conducted against networks:

- *Computer network exploitation (CNE).* The objective here is to target the Internet or an intranet (a privately maintained computer network that requires access authorization and may or may not be connected to the web via an administrative computer), but not for attack. Instead, the focus is on *collection* operations where the network continues to function normally.
- *Computer network attack (CNA).* CNA operations are conducted with the intent to degrade, disrupt, deny, or deceive. The effects of CNA typically are readily observed. In this chapter, the term *CNA* is used as a convenience, for any projection of deception that uses CYBER means—via the Internet or placing deceptive information directly on an intranet or standalone computer.

Although these terms refer to offensive deception against a network, the same principles and tools apply in attacking or exploiting a single computer that is not connected to a network; only the techniques for obtaining access are different. Let's look at some of the channels for CNE/CNA and then examine some of the tools for using them to obtain access and implant malware.

Web-Based Channels

A basic rule of deception is that the more trustworthy a channel is believed to be, the more effective it is as a channel for deception. Several components in cyberspace are designed to provide a trusted environment for sharing information or conducting daily activities. Making use of these generally requires CNE/CNA tools, but the channels can then be effective in projecting a deception.

Intranets

An intranet is an internal network that people can access only from within their organization or trusted group. It is intended as a place to securely share files or sensitive documents. Some intranets are not connected to the Internet; others have Internet access, but only through a gateway administrator from within the organization. In this section, we're looking at the type of intranet that connects to the Internet but has some form of protection. They're usually called virtual private networks (VPNs), and they allow people to operate with an expectation of privacy on the Internet. An intranet that does not connect directly to the web requires a different approach and is discussed in a later section.

A VPN is an attractive channel for projecting deception because people using intranets for communications and sharing sensitive documents tend to blithely accept the material in their system as valid—far more so than they would if it came directly from the Internet rather than through the organization or group's intranet. But because these VPNs connect to the web, they are relatively easy for an attacker to get into via a web-based attack.

The Deep Web and the Dark Web

The terms "deep web" and "dark web" are often used interchangeably. Some argue that the two should be differentiated, while others disagree. Both are based on the concept of privacy; the dark web emphasizes anonymity.

The deep web refers to the vast part of the Internet that is not indexed and therefore not normally visible or accessible from search engines. Access-restricted commercial databases, websites, and services comprise much of the deep web. Special browser software such as Tor (originally created by the US Navy to transfer files securely) is required for access. The Tor software makes use of a set of VPNs, allowing users to securely travel the deep web and remain anonymous. It protects users by bouncing their communications around a distributed network of relays run by volunteers around the world, which prevents others from watching users' Internet connections to learn what sites they visit, prevents the sites that users visit from learning their physical location, and lets users access sites that are blocked to anyone unless granted permission. Government databases, such as those maintained by NASA and the US Patent and Trademark office, also use the deep web space for obvious reasons.

Within the deep web lies what is often referred to as the dark web. Much of the dark web content fits well with the name: It includes all types of black markets, illicit drug traffic, fraud-related material, and child pornography. It is used for a number of scams and hoaxes, but it also is used for political discussion groups, whistleblowing sites, and social media sites often to avoid government censorship. These legitimate uses of the dark web offer attractive channels for projecting a deception, because many governments pay close attention to the material posted on these sites. Tracing the source of a post in the dark web is very difficult—an added advantage in executing deception.

Blockchains

Blockchains are another example of a seemingly secure channel for projecting a deception. The challenge is to find a way to make use of it.

A blockchain is software that allows the creation of a digital ledger of transactions that is then shared among participants in a distributed network. It relies on cryptography to allow each participant on the network to manipulate the ledger securely without the control of a central authority. Once software is deployed on a blockchain, programs run automatically and are accessible to any Internet user. This design makes them basically autonomous and uncontrollable by governments.

Blockchains are best known as the technology underpinning the bitcoin cryptocurrency. Commercial enterprises are now using blockchains to make and verify transactions on a network instantaneously without a central authority. Once an item is entered into the blockchain ledger, it is extremely difficult to change or remove. If a participant wants to change it, others in the network run algorithms to evaluate and verify the proposed transaction. If a majority of participants agree that the transaction looks valid, then it will be approved and a new block added to the chain. The key feature is that the entire network, rather than a central authority, is responsible for ensuring the validity of each transaction.[14]

Like Intranets, blockchains tend to be trusted. So if they can be compromised, the resulting deception is more likely to succeed. Of course, compromise of a blockchain is much more difficult than some of the softer targets on the Internet.

The Internet of Things

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings, and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The objects can be sensed and controlled remotely via the web.

Experts estimate that 6.4 billion connected things were in use worldwide in 2016, up 30 percent from 2015. The Internet of Things is expected to consist of almost 50 billion objects by 2020. It includes a wide class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation, and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

These network-connected devices automatically collect and exchange data, allowing enterprises to be more efficient and productive. However, IoT networks also incorporate an extensive set of connected devices that can introduce multiple points of vulnerabilities in the networks.

The Internet of Things can be used in a cyber attack on infrastructure, as the Mirai attack suggests. But it can be used to convey a deception, often as part of an attack, by presenting a false picture of security systems or the status of equipment that has been altered. The Stuxnet malware, described later in this chapter, was not web-based but did exactly that: The sensors that Stuxnet infected provided the monitoring personnel at Iran's Natanz nuclear facility with a false picture of their enrichment centrifuges while the centrifuges were being destroyed.

MIRAI

On October 21, 2016, the US East Coast encountered Internet outages from a massive distributed denial of service (DDoS) attack that overwhelmed web service with traffic. The attack was targeted on servers maintained by Dyn, a company that controls many of the Internet's domain names. The attack took down many popular websites in Europe and the United States, including Twitter, Netflix, Reddit, CNN, and *The Guardian*.

The attack relied on a malware package called Mirai, which organized what is called a *botnet* to conduct the attack. The controller of a botnet is usually referred to as a command-and-control (C&C) server. This server issues instructions to the botnet, directing the activities of infected computers (referred to as zombies) through communication means such as Internet Relay Chat or HTTP.

The Mirai botnet used vulnerable IoT technology to launch an attack. One of the major IoT resources used was the security cameras sold by a Chinese firm, Hangzhou Xiongmai. Millions of these cameras are sold in the United States. The DDoS attack exploited the default passwords in the equipment and organized them into a botnet. Hangzhou Xiongmai issued a recall for the cameras on October 24, 2016, while complaining that users should have changed the default passwords.

Botnets such as Mirai exploit weak security measures in IoT devices. Most such devices, if they have any protection at all, are delivered with a standard password and username combination—"admin" and "1111" are typical ones. The botnet scans the Internet for IoT systems using these standard passwords and infects them with malware that directs them to the C&C server; the server then uses them as hosts to launch cyber attacks.

The Tools of Cyber Operations

CNE and CNA use the same tools. There are many of them—thousands, in fact, with new ones and improvements being added daily. This introduction touches on some traditional ones, and some of the latest developments in tools at the time of publication. But it scratches just the surface of the field.

An attacker must gain access to the target network, have tools to exploit it, and remove any evidence of the operation. Attackers can exploit a vulnerability that occurs in the network or is presented by the supply chain. They can masquerade as an authorized user or use human assets to gain physical access to the network. Once they gain access, they usually leave behind a software implant called a *backdoor*. The implants communicate back to the controlling organization, allowing the attackers to acquire data from the network and introduce malware.

In poorly defended systems, a backdoor can give unlimited access to data in the system. Valuable corporate proprietary information has been acquired time and again from competitors through backdoors.[15]

This can happen, for example, when the target receives an e-mail that appears to come from a trusted source—an acquaintance or someone within the same organization. The e-mail might ask the target to open an attachment. Adobe PDFs, images, and Microsoft Office files are commonly used. When the file is opened by the vulnerable program on the victim's computer (such as Adobe Acrobat or Microsoft Excel, PowerPoint, or Word), a backdoor program executes and the computer has been compromised. At the same time, a seemingly normal file or image appears on the target's computer screen, so that the recipient has no reason to suspect that something is amiss. E-mails are widely used for deception because it is possible to identify an employee's trusted relationships and professional networks by looking at his or her e-mail patterns.[16]

Alternatively, the e-mail may direct the target to a website that contains the backdoor, with much the same outcome. Such a website is called a *drive-by download* site. It typically relies on vulnerabilities in web browsers and browser add-ons. Users with vulnerable computers can be infected with malware simply by visiting such a website, even without attempting to download anything.[17] The attacker can then acquire files from the computer or e-mail or send data from the computer, or force the compromised computer to download additional malware. From there, the attacker can use the infected computer to exploit the victim's contacts or other computers on the target network.[18]

The basic tools of malware are known as *exploits*, discussed next.

Exploits

An exploit takes advantage of software vulnerabilities to infect, disrupt, or take control of a computer without the user's consent and preferably without the user's knowledge. Exploits take advantage of vulnerabilities in operating systems, web browsers, applications, or other software components.[19]

The preferred target of exploits changes constantly as vulnerabilities are found and corrected in all of these targets. For example, exploitation of the Adobe Flash Player had been quite low until 2011, when it suddenly became a major target. Adobe provided patches and updates to eliminate the vulnerabilities, only to encounter new versions of malware year after year as hackers went after the patched versions and even moved to place Trojans (discussed below) on mobile versions of Flash Player.[20] In 2016, new malware targeting Flash Player continued to be discovered.

Four of the most widely known exploits are Trojan horses (usually abbreviated "Trojans"), worms, rootkits, and keystroke loggers.

- A *Trojan horse* is a seemingly innocent program that conceals its primary purpose. The purpose is to exfiltrate data from the target computer system.
- A *worm* can do many of the things that a Trojan does, and can also do such things as install a backdoor. But in contrast to the Trojan, the worm is designed to be completely concealed instead of masquerading as an innocent program.
- A *rootkit* is software code designed to take control of a computer while avoiding detection. The rootkit is often concealed within a Trojan.
- *Keystroke loggers,* or keyloggers, can be hardware or software based. Their general purpose is to capture and record keystrokes. For CYBER collection, they specifically are intended to capture passwords and encryption keys.

Although all of these exploits can be used for cyber deception, they are most effective when they are used against a *zero day* vulnerability. Also called a *zero hour* or *day zero* vulnerability, this is an application vulnerability that is unknown to defenders or the software developer. It derives its name from that time (called the zero hour or zero day) when the software developer first becomes aware of the vulnerability. Until that moment of awareness, the developer obviously cannot develop a security fix or distribute it to users of the software. Zero day exploits (software that uses a security gap to carry out an intrusion) are highly valued by hackers and cyber espionage units because they cannot be defended against effectively—at least not until sometime after zero day arrives.[21]

Exploits are usually emplaced via the web, but they can be emplaced directly on machines, as discussed later. Deception via the web requires more than the deployment of exploits. The cyber espionage organization must control the exploits and use them to insert the desired information while maintaining the secrecy, or at least the deniability, of the operation. Often this is done by botnets such as Mirai, used in the DDoS attack described earlier. The botnet's command-and-control server can't be easily shut down because it's hard to determine its real location.

Advanced Persistent Threats

An advanced persistent threat (APT) might be thought of as an integrated system of exploits. It is a set of stealthy and continuous computer hacking processes. The term *advanced* refers to the use of multiple malware components to exploit system vulnerabilities that are tailored to defeat detection by software security firms.

Persistent refers to the existence of a continuing external command system that controls the malware package and extracts data from the infected machine or network.[22]

APTs originally appear to have been government-sponsored efforts used for intelligence gathering or CNA, but increasingly they are being used by organized criminal groups. Some of the first to be observed have been named Duqu, Flame, and Gauss.

DUQU, FLAME, AND GAUSS

Duqu. Duqu was a sophisticated piece of malware discovered in 2011, having been used in a number of intelligence-gathering attacks against a range of industrial targets. Duqu has a number of similarities to the Stuxnet APT discussed later, though it appears to have the purpose of CNE, not CNA. It attacks Microsoft Windows systems using a zero day vulnerability. It uses a stolen digital certificate to create the façade of being secure software.

Duqu was detected on servers in Austria, Hungary, Indonesia, the United Kingdom, Sudan, and Iran. It may have had a number of CNE roles, but one clear role was to compromise certificate authorities and hijack digital certificates. These certificates could then be used on attacked computers to cause malware to appear as secure software.[23]

Flame. In 2012, malware was discovered that appears to have targeted Microsoft Windows computers in the Middle East for intelligence purposes. Called Flame, it reportedly had been operating for five years in these countries.[24] Flame is more powerful and flexible than Stuxnet and has a number of features that illustrate the level of sophistication and precise targeting that is possible today in cyber espionage:

- Flame incorporates five distinct encryption algorithms and exotic data storage formats both to avoid detection and to conceal its purpose.
- It does not spread itself automatically, doing so only when directed by a controlling entity (the command-and-control server).
- It allows the controlling entity to add new malware at any time for targeted collection.
- It enables the controlling entity to remotely change settings on a computer, gather data and document files, turn on the computer microphone to record conversations, log keystrokes, take screen shots, and copy instant messaging chats.[25]

Flame is a very sophisticated piece of malware, far more complex than Duqu—so sophisticated, in fact, that it almost certainly is the product of a government that has an advanced software industry. It functions as a backdoor and a Trojan. It also has wormlike features, so that it can replicate itself in a local network and on removable media if it is instructed to do so by its controller. Flame's sophistication earned it the "Epic Ownage" award from the 2012 Black Hat convention—the equivalent, among cyber security experts, of an Oscar. (So far, no one has come forward to accept the award.)[26]

Gauss. In 2012 a new CYBER collection toolkit appeared—apparently created by the same government that developed and deployed Flame. Called Gauss, it has many similarities to Flame: architecture, module structures, and method of communicating with command-and-control servers are strikingly similar. The owners of the Gauss command-and-control server shut it down shortly after its discovery.

Gauss is an example of a highly targeted intelligence collector. It infected personal computers primarily located in Lebanon, and stole browser history, passwords, and access credentials for online banking systems and payment websites from its targets. More than 2,500 infections were identified; total infections probably numbered in the tens of thousands.

It appears that the targeting was intended to collect intelligence about financial transactions. The targets included a number of Lebanese banks such as the Bank of Beirut, EBLF, Blom Bank, Byblos Bank, FransaBank, and Credit Libanais. Flame also targeted specific Citibank and PayPal accounts.[27]

The current state of the art in APTs has been named Duqu2. It had an unusual target, though a logical one for a government that is in the cyber espionage business.

DUQU 2

Kaspersky Lab is one of the world's major software security companies, operating in almost 200 countries from its Moscow headquarters. Its founder, Eugene Kaspersky, reportedly has ties to Russia's intelligence services (he is a graduate of the FSB academy; the FSB is the successor to the KGB). Kaspersky Lab has been the most prominent of software security firms in identifying, analyzing, and countering the malware described in this chapter.

In 2016, Kaspersky Lab was itself the target of a malware attack. The attack successfully accessed the company's intellectual property and proprietary technologies and its product innovations. It was targeted specifically on the Kaspersky tools used for discovering and analyzing advanced persistent threats, and the data on current Kaspersky investigations into sophisticated malware attacks. The attack was discovered only after it had been inside the company's intranet for several months.[28] It was, in counterespionage terms, a wilderness of mirrors event—using computer espionage to target the web's equivalent of a counterespionage organization—presumably so that the attacker could better evade discovery by Kaspersky in future cyber attacks.

The malware, which Kaspersky named Duqu 2, has very little persistence, making it difficult both to detect and to eliminate. It exists almost entirely in the memory of the targeted system. As a result, according to the Kaspersky Lab report, "the attackers are sure there is always a way for them to maintain an infection—even if the victim's machine is rebooted and the malware disappears from the memory."[29] Duqu 2 was so named because it shares much of the code of the original Duqu and of Stuxnet, leading observers to believe that it was developed by the same unidentified organization.

STANDALONE COMPUTERS AND INTRANETS

Attacking a network that is physically isolated from the Internet (a private intranet) or a single computer that never connects to the Internet requires a different type of effort from that used in CNE. The collector has to gain access to the computer or the intranet in some way. Once access has been gained through a USB drive, a network jack or cable, a utility closet, or some similar device—almost anything can be done. From the defense point of view, the game is over and the defense has lost.

One of the simplest targets is a personal notebook computer that is carried on trips or to conferences. With a few minutes of uninterrupted access, a collector can download the contents of a notebook's hard drive or upload malware. Computers or any devices containing electronic storage—separate hard drives or USB flash drives, for example—can be legally searched when they are taken across international borders, and they often are. Encrypting the material does not provide protection. Customs officials can demand the encryption key, deny the traveler entry to their country, or confiscate the computer. In many cases, customs officials are looking for terrorist material, pornography, or hate literature, but countries that have a reputation for commercial espionage also are likely to make intelligence use of the material acquired.

Gaining direct access to an isolated intranet or a standalone computer on a continuing basis requires some effort. But IT systems rarely exist for long periods in isolation. Upgrades, patches, software fixes, and new software have to be added to these systems. All of those provide opportunities for a determined attacker to use methods such as social engineering to implant malware or obtain information from the system.

Social Engineering

Isolated intranets are not connected to the Internet most often as a security measure. They therefore are viewed generally as safe from attack and placement of deceptive information. But this perceived trust makes them more vulnerable to deception. The challenge, of course, is to get into the intranet to place the misleading information. Social engineering is one means of doing that. It's used to facilitate both CNA and CNE.

In cases where computers never leave a secure facility, and where remote access is not possible, it is necessary to use field operations to access networks. This category encompasses deployment of any CNA or CNE tool through physical access or proximity. In intelligence, these are called HUMINT-enabled operations; in the world of hackers, they are usually referred to as social engineering.[30] They encompass such classic HUMINT techniques as gaining access under false pretenses, bribery or recruitment of trusted personnel in a facility, and surreptitious entry.[31] HUMINT-enabled operations are often facilitated by human error or carelessness, and complex intranets are particularly susceptible to both.

The case of Stuxnet, which has attracted much international attention and even been the source of a 2016 TV documentary titled *Zero Days,* illustrates the importance of direct access to an intranet as well as the value of social engineering. Although Stuxnet is an example of CNA, it relied heavily on deception for its success.

STUXNET

Stuxnet illustrates the type of precision attack that is most effective in both CNA and CNE. Stuxnet was a worm designed to infect and disable a specific type of computer performing a specific task. The target, investigators believe, was the computer controlling the isotope separation centrifuges in Iran's Natanz uranium enrichment facility.

Stuxnet was used in a sustained and directed attack, conducted over a ten-month period beginning in 2009. Reportedly, at least three versions of the program were written and introduced during that time period. Investigators found that the first version had been completed just twelve hours before the first successful infection in June 2009. One attack, in April 2010, exploited a zero day vulnerability in Windows-based computers.

Once introduced, the Stuxnet worm infected all Windows-based industrial control computers it found while searching for specific equipment made by the Siemens Corporation. Upon finding its target, the worm was programmed to damage a centrifuge array by repeatedly speeding it up and slowing it down, while at the same time hiding its attack from the control computers by sending false information to displays that monitored the system.[32]

The attack appears to have been at least partially successful. International inspectors visiting Natanz in late 2009 found that almost 1,000 gas centrifuges had been taken offline. Investigators therefore speculated that the attack disabled some part of the Natanz complex.

How the complex became infected has been a matter of speculation, because there are several possible ways the worm could have been introduced. A classified site like Natanz is unlikely to be connected directly to the Internet. The attacker could have infected an organization associated with Natanz that would be likely to share files, and therefore the malware, with Natanz. An infected e-mail sent to one of the Natanz operators could have carried the worm. Or a USB flash drive carrying the worm could have been provided to one of the Natanz staff as part of routine maintenance.[33]

A sophisticated and targeted worm such as Stuxnet would need to be tested to ensure that it would succeed against its target, preferably without causing damage to unintended targets. Stuxnet recorded information on the location and type of each computer it infected, indicating a concern about protecting unintended

(Continued)

(Continued)

targets.[34] Israel reportedly built an elaborate test facility at its Dimona nuclear weapons development center. The facility contained a replica array of the Natanz Iranian uranium enrichment plant.[35] Such a test site would have been necessary for the design of the attack software.

Although Stuxnet was an attack malware, it illustrates what can be done in CNE. Stuxnet operated by fingerprinting any computer system it infiltrated to determine whether it was the precise machine the malware was looking for. If not, it left the computer alone.[36] The Duqu program that was associated with Stuxnet could gain access to a specific computer on a network, acquire classified or proprietary information from it, manipulate the defense system so that everything appeared to be operating normally, and exfiltrate the data via the operator's apparently secure mechanisms (probably USB drives) for placing data on the infected computer or network.[37]

Stuxnet represents the pre-2009 state of the art in attacks on standalone computers and intranets. Malware has improved substantially since then. In 2016 the current state of the art was represented by another malware package known as Project Sauron.

PROJECT SAURON

In October 2016 the research teams at Kaspersky Lab and Symantec published separate reports about a new malware package called Project Sauron. According to their reporting, it was responsible for large-scale attacks on government agencies; telecommunications firms; financial organizations; and military and research centers in Russia, Iran, Rwanda, China, Sweden, Belgium, and Italy. It appears to have specifically targeted communication encryption software used in those countries.

Project Sauron relies on a zero day exploit, presumably delivered by a USB drive that is inserted into a computer on the secure intranet. When a user logs in or changes a password, the malware logs keystrokes and acquires the password. It also acquires documents and encryption keys. It then waits for another USB drive to be attached to the infected machine and downloads its payload to the USB drive.

The malware appears to have been carefully designed to defeat efforts by software security experts at companies such as Kaspersky Lab and Symantec. These experts rely on finding patterns or signatures that can identify malware. Project Sauron creates no distinguishable patterns and relies on an almost random selection of disguises. It uses file names similar to those used by software companies such as Microsoft. It regularly changes its method of sending data back to the attacker. And, of course, it relies on very powerful encryption to conceal its presence on a USB drive or victim machine.[38]

Deception in Hardware

Even better than getting access to a target's computer is to manufacture the computer. Technology has allowed us to hide malware in many places, and the supply chain (all the way from component manufacturer to end user) is a very attractive place. Anyone in the supply chain before sale has the access necessary for inserting malware in a computer or other electronic device. Such embedded malware is difficult to detect, and most purchasers do not have the resources to check for such modifications.

The hardware can be modified in ways that are not readily detectable, but that allow an intelligence service to gain continuing entry into the computer or communications system. Targeted components can be add-ons that are preinstalled by the computer manufacturer before the computer is sold. A user may not even use the vulnerable add-on or be aware that it is installed. [39] Malware inserted in a computer before sale can call home after being activated, exfiltrate sensitive data via USB drives, allow remote control of the computer, and insert Trojan horses and worms. Such backdoors are not limited to software installed on the computer. Hardware components such as embedded radio-frequency identification (RFID) chips and flash memory can be the sources of such malware.

CYBER DECEPTION

This chapter is about the use of cyberspace means to project a deception. But, as previously stated, the term *cyber deception* has a specific meaning within the cyber community. The target of this type of deception is the cyber attacker. The objective is to deceive the attacker and cause him or her to behave in a way that gives the defender an advantage.

Much effort is spent worldwide on cyber defense—to protect organizational networks from hacking. Cyber deception is a technique to complement the defense with an aggressive offense. It offers a way to penetrate the opponent's cyber espionage system, identify the source of cyber attacks, and raise the cost of intrusion into protected networks. These three go together; without knowing the source, it is difficult to retaliate. It is important, for example, to distinguish casual hackers from foreign intelligence services.

The idea of using deception in cyber defense developed after it became apparent that traditional cyber security measures taken alone were losers. The cyber defender could defend against known types of attack. But the attacker could repeatedly develop new ways to counter network defenses. The pattern reinforced the basic maxim of strategic conflict: *The offense always wins*. The best that traditional cyber security defenses could do was slow the attacks or make them more expensive. Winning on defense was not an option.

The deception-based defense changes that equation. Instead of monitoring for known attack patterns, the defender instead uses sophisticated techniques and engagement servers to entice attackers away from its sensitive servers. Attackers tend to work on the fundamental assumption that the infrastructure data they see are real. Deception technology uses carefully designed lures to attract attackers during infiltration and instantly identify them.

In brief, cyber deception conceals your real network, while deceiving attackers into believing that they have hacked into your network; or at the least, it leaves attackers uncertain and confused about what they are seeing. It levels the cyber battlefield. It leads opponents into an alternate reality, and when they apply their attack methods and insert malware, all of it is captured for later examination by a cyber forensics team. An advantage of the cyber deception approach is that a hacking attack typically takes weeks to identify and deal with using purely defensive measures. Deception, in contrast, detects hackers immediately and allows the defender to obtain intelligence about the hacker's strategies, methods, and identity.

How Cyber Deception Works

Cyber deception is like all other deceptions: It works by hiding the real and showing the false. It might manipulate network activities to mask the actual network while creating a notional one. The notional network takes the form of a *honeypot* or *honeynet*—a server or network that attracts and traps would-be attackers. This type of defense generally includes the following steps:

- *Install an engagement server*. This is a separate server that appears to be an integral part of an organization's network or network of networks but is intended to lure hackers, trap them, and analyze their attacks.
- *Place a special operating system on the server*. Engagement servers can use either an emulated operating system or a real one. Emulation is simpler to deploy, but it is easier for the hacker to identify deception. In the simplest versions, when the hacker breaks in, he finds nothing there. If he attempts to run malware, it has no impact. Real operating systems make deception harder for an attacker to identify. They can be designed with applications and data to closely match the actual network environment, both adding credibility to the deception and allowing better assessment of the threat as the attacker moves around in the engagement server.
- *Misdirect the attacker.* This step relies on lures that work with deception engagement servers to draw attackers away from the organization's servers and instead pull them into the engagement server. Publishing misleading details about the organization's network can sometimes help in this step.
- *Assess the threat*. This step makes use of forensics to capture the methods and intent of the hacker. It then identifies the indicators of compromise so that defensive systems across the real network can identify and block subsequent attacks.

- *Counterattack*. This optional step depends on the forensics being able to identify the attack source; retaliation can then take the form of placing malware on the attacker's machine or network.
- *Recover*. The operating system should have a self-healing environment that, after containing and analyzing an infection, destroys the infected virtual machine and rebuilds itself to prepare for the next attack.[40]

Cyber deception offers a substantial advantage over conventional cyber defense. The conventional approach generates a high volume of alerts that are not attacks (false positives). Cyber deception doesn't have this problem: It only delivers an alert based on actual engagement with the deception server.

During 2016, cyber deception began to be deployed to defeat attacks on the Internet of Things. The defense used special servers and decoys designed to appear as production IoT sensors and servers. When attackers engage with a decoy, believing that it is a standard production device, they are quarantined and subjected to detailed forensics to support countermeasures development.

Projecting a Deception

Cyber deception obviously is a form of deception in and of itself. But it also can be used as a channel to project a deception. You simply place the deceptive material in the engagement server so that it appears to be valid protected files. When opponents hack into your site, they obtain files that lead them into the story that you want to project.

This has been a brief introduction to the topic. Cyber deception to protect against cyber attack is a complex subject that is treated in detailed texts elsewhere. Readers who wish more detail may want to peruse Gartzke and Lindsay's article on the subject[41] or the 2016 book *Cyber Deception*.[42]

Let's next turn to the planning and execution part of the process.

NOTES

1. See, for example, Sushil Jajodia, V. S. Subrahmanian, Vipin Swarup, and Cliff Wang, eds., *Cyber Deception: Building the Scientific Foundation* (Switzerland: Springer, 2016).
2. Oxford Dictionary, "Word of the year is . . . ," https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016.
3. Amar Toor, "Germany Is Worried about Fake News and Bots ahead of Election," *The Verge*, November 25, 2016, http://www.theverge.com/2016/11/25/13745910/germany-fake-news-facebook-angela-merkel.
4. See https://en.wikipedia.org/wiki/Reliability_of_Wikipedia.
5. Wang Yongming, Liu Xiaoli, et al., *Research on the Iraq War* (Beijing, PRC: Academy of Military Science Press, 2003).
6. Intelligence Community Assessment, "Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

7. Gary King, Jennifer Pan, and Margaret E. Roberts, *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, working paper, August 26, 2016, http://gking.harvard.edu/50c.
8. Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," *Defence Strategic Communications* 1, no. 1 (winter 2015): 13.
9. Jeff Giesea, "It's Time to Embrace Memetic Warfare," *Defence Strategic Communications* 1, no. 1 (winter 2015): 70.
10. Ibid, 71.
11. Ibid, 69.
12. Ibid, 68.
13. Ibid, 75.
14. Steve Norton, "The CIO Explainer: What Is Blockchain," *Wall Street Journal*, February 2, 2016, http://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/.
15. John McAfee and Colin Haynes, *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System* (New York: St. Martin's Press, 1989), 79.
16. Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corporation, October 9, 2009, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.
17. *Microsoft Security Intelligence Report,* Vol. 12, http://www.microsoft.com/security/sir/default.aspx.
18. *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Joint Report JR03-2010, of the Information Warfare Monitor and Shadowserver Foundation, April 6, 2010, http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0.
19. *Microsoft Security Intelligence Report,* Vol. 12.
20. Ben Weitzenkorn, "Adobe Flash Player Hit by Hackers on Both Ends," *Security News Daily*, http://www.securitynewsdaily.com/2191-adobe-flash-player-iphone-android.html.
21. *Microsoft Security Intelligence Report,* Vol. 12.
22. Sam Musa, "Advanced Persistent Threat–APT," March 2014, https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT.
23. Kim Zetter, "Son of Stuxnet," *The Intercept*, November 12, 2014, https://theintercept.com/2014/11/12/stuxnet/.
24. Damien McElroy and Christopher Williams, "Flame: World's Most Complex Computer Virus Exposed," *Telegraph,* May 29, 2012, http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html.
25. Ibid.
26. Bernt Ostergaard, "Black Hat Roundup: Keeping Tabs on the Ones That Got Away," July 31, 2012, https://itcblogs.currentanalysis.com/2012/07/31/black-hat-roundup-keeping-tabs-on-the-ones-that-got-away/.
27. Kaspersky Lab, "Kaspersky Lab Discovers 'Gauss'–A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts," August 9, 2012, http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts.
28. David Gilbert, "Duqu 2: The Most Advanced Cyber-Espionage Tool Ever Discovered," *International Business Times UK*, June 10, 2015, http://www.ibtimes.co.uk/duqu-2-most-advanced-cyber-espionage-tool-ever-discovered-1505439.
29. Gilbert, "Duqu 2."

30. Kevin D. Mitnick and William L. Simon, *The Art of Intrusion* (Indianapolis, IN: Wiley, 2005), ch. 10.
31. "War in the Fifth Domain," *The Economist*, July 1, 2010, http://www.economist.com/node/16478792? story_id=16478792.
32. John Markoff, "Malware Aimed at Iran Hit Five Sites, Report Says," *New York Times*, February 11, 2011, http://www.nytimes.com/2011/02/13/science/13stuxnet.html.
33. Ibid.
34. Ibid.
35. William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.
36. Mark Clayton, "Stuxnet Malware Is 'Weapon' Out to Destroy . . . Iran's Bushehr Nuclear Plant?" *Christian Science Monitor,* September 22, 2010.
37. Ibid.
38. Michael Mimoso, "ProjectSauron APT on Par with Equation, Flame, Duqu," *Threatpost.com*, August 8, 2016, https://threatpost.com/projectsauron-apt-on-par-with-equation-flame-duqu/119725/.
39. *Microsoft Security Intelligence Report,* Vol. 12.
40. Carolyn Crandall, "The Ins and Outs of Deception for Cyber security," *Network World,* January 6, 2016, http://www.networkworld.com/article/3019760/network-security/the-ins-and-outs-of-deception-for-cyber-security.html.
41. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48, doi:10.1080/09636412.2015.1038188.
42. Jajodia et al., eds., *Cyber Deception: Building the Scientific Foundation.*