Deploying Deception Countermeasures in Spearphishing Defense

Robert Zager and John Zager

Abstract

Spearphishing is the attempt to infiltrate systems by engaging users with highly targeted deceptive emails. The attacker's objective is to induce the targeted individual into taking actions on behalf of the attacker which will grant the attacker system access. Spearphishing is the predominate method used by state-affiliated cyber attackers to infiltrate targeted systems. Defending against spearphishing attacks is generally addressed as a matter of computer science in which defenses seek to isolate the human target from the spearphishing attackers by means of email filtering, malware detection, firewalls, limited user privileges, and system monitoring. These computer science defenses leave systems unnecessarily exposed to attackers because the human attack surface remains easily accessible and subject to successful attacks based on principles of psychology which are exploited using military deception. The authors propose deception countermeasures which modify the email interface, thereby making the user less susceptible to email-based deception. Moreover, the modified interface increases the likelihood that the user can detect and report attacks to security personnel.

Keywords: military deception, phishing, spearphishing, APT, computer network defense, human sensors, cyber counterattack, deception countermeasures

Spearphishing – The Infiltration Path of Choice

… cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines.

- *Dr. Frederick Chang, former NSA Director of Research*[1]

On 28 October 2014, FireEye released *APT28: A Window Into Russia's Cyber Espionage Operations?*[2] In this extensive report, FireEye analyzes cyber espionage operations against Eastern European targets and Western Security Organizations such as NATO. The attack vector in every case was spearphishing, a cyber-infiltration tactic used in Advanced Persistent Threats (APT) in which a highly targeted email is used to deceive the recipient into taking a compromising action.

Once the province of secret government cables[3], infiltration using spearphishing is now a common occurrence that is widely reported in the press. The lid was blown off the shadowy world of state-affiliated spearphishing APT cyber-attacks with the publication of Mandiant's *APT1* report on 18 February 2013.[4] The November 2014 cyber-attack on Sony Pictures Entertainment used spearphishing to infiltrate Sony's defensive cyber perimeter.[5] Spearphishing victims include governments, the media, industry – every major company in the United States has already been penetrated by China.[6] According to General Keith Alexander, then the director of the National Security Agency and commanding officer of U.S. Cyber Command, cybertheft of intellectual property is the greatest transfer of wealth in history.[7]

APT is defined by the National Institute of Standards and Technology ("NIST"), the agency charged with administering the Federal Information Security Act of 2002 ("FISMA")[8]:

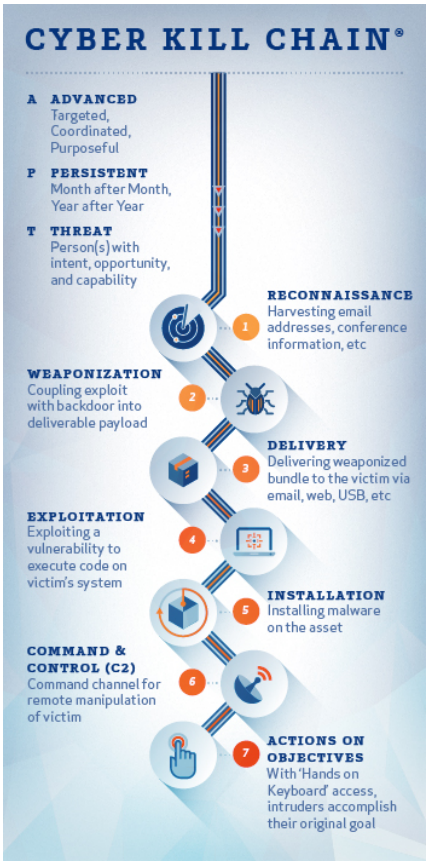
> An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.[9]

It is estimated that 91% of APT infiltration involves spearphishing and of that 95% uses email attachments.[10] Reports of state affiliated APT often find that 100% of the attacks use spearphishing.[11] This paper discusses the significance of deception in spearphishing and how deception countermeasures[12] can be applied as part of wider APT defenses to decrease the effectiveness of spearphishing as a method of system infiltration.

APT Kill Chain

> *… to attack our forces, an adversary must complete a sequence of actions, commonly referred to as a "kill chain." … [B]ecause each step must work, our forces can focus on the weakest links in the chain, not each and every one.*
>
> - *Admiral Jonathan Greenert, Chief of Naval Operations, and General Mark Welsh, Chief of Staff of the Air Force*[13]

In *Intelligence-Driven Computer Network Defense,*[14] Lockheed Martin sets forth the phases of an APT attack as a cyber kill chain.



Source: Lockheed Martin

In the Reconnaissance phase, the attacker is gathering information about the target. This could include technical information about defenses, information for use in social engineering efforts, and information about objectives to be obtained from the attack.

In the Weaponization phase, the attacker is creating the malware, if any, required to compromise systems.

In the Delivery phase the malware is delivered. The most common delivery mechanisms are email attachments, websites and USB removable media.

In the Exploitation phase the weapon is activated.

In the Installation phase a remote access trojan or backdoor on the targeted system allows the attacker to maintain presence inside the attacked systems.

In the Command and Control (C2) phase the attacker has access to the targeted systems.

In the Actions on Objectives phase the attackers, having successfully completed the prior six phases, are able to implement their objectives. The duration of this period constitutes the attacker's "time on target." That time could be short, such as attacks by the Syrian Electronic Army in which their misinformation mission is completed within a few hours,[15] or could last for years, such as the Red October attacks that exfiltrated data for over five years.[16]

To the extent an attacker can be thwarted in any aspect of the kill chain, the attacker's objective will be frustrated and the defenders can mitigate the damage inflicted by the attack. Kill chains do not address:[17]

- Inventory/Force Structure – number of platforms, sensors, and weapons required.
- Capacity – rate at which kill chains can be executed.
- Training – proficiency at executing kill chains.

Kill chains are a tool in the larger Course of Action (COA) framework. COA is an element of planning which is set forth in Joint Publication (JP) 5-0, *Joint Operation Planning*.[18]

The Defenders

> *In the near future, the Department intends to expand and deploy applications that detect, track, and report malicious activities across all DoD networks and information systems on a near real-time basis.*
>
> *DoD Report to Congress, November 2011*

These diagrams from *Coordinated Cybersecurity Incident Handling*[19] show the notional timeline for APT response:

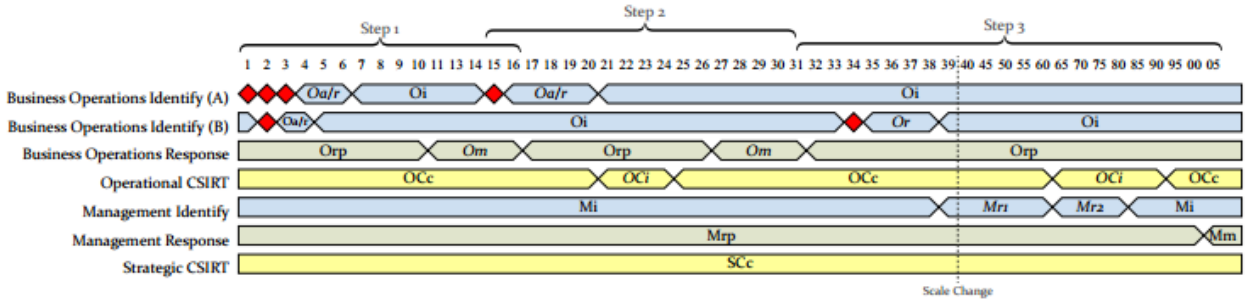


Figure 13. Timing diagram for first three steps of scenario

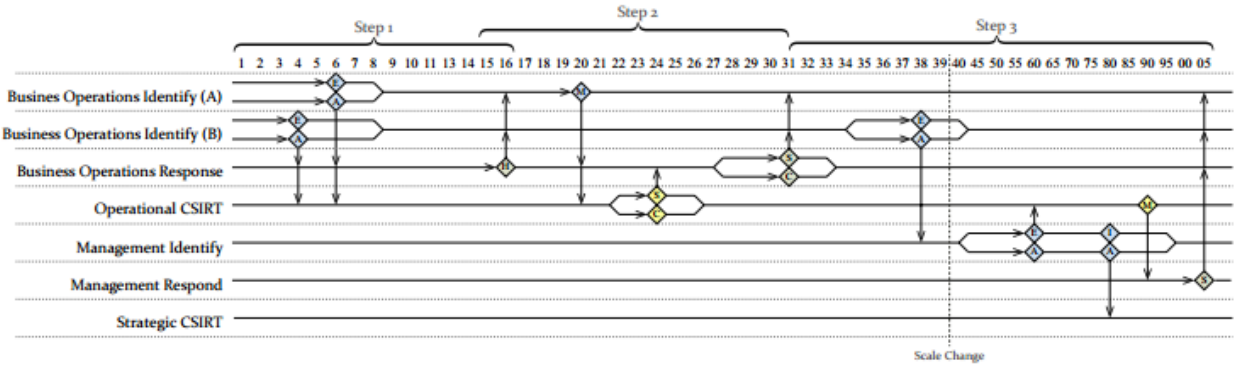


Figure 14. Communications diagram for first three steps of scenario

During the first 105 days of the incident response illustrated in “Figure 13” and “Figure 14,” the intelligence system completes the first three steps of incident handling process.

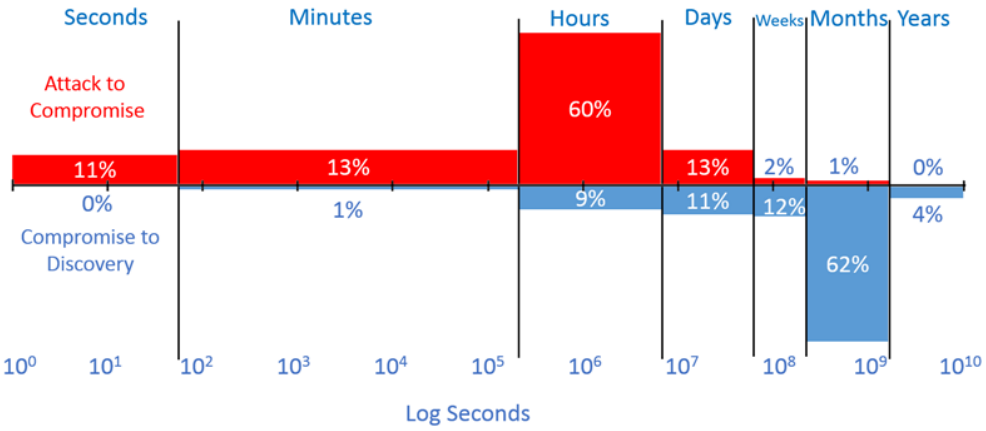
105 Days {
- Step 1. AFTER determining they have been attacked, victims notify CSIRT.
- Step 2. Coordination with operational CSIRT.
- Step 3. Working with management and notifying of vulnerabilities.

- Step 4. Potential victims assess their vulnerabilities.
- Step 5. Formulation of response.
- Step 6. Threat response is disseminated.

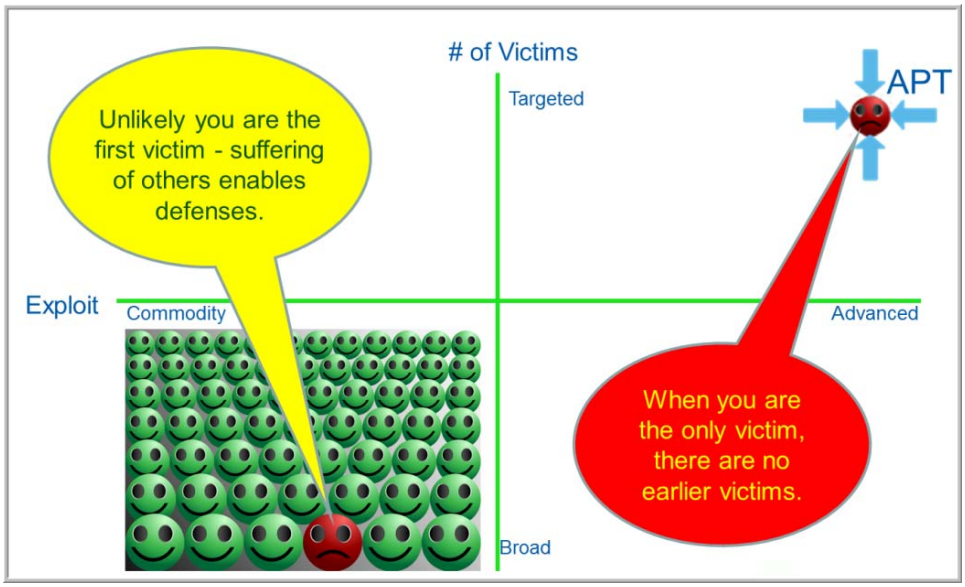
Coordinated Cybersecurity Incident Handling reveals the non-real-time nature of an intelligence-based detect, track, report system. At its core, intelligence is the correlation of past events.

The first step in this process is discovery of the attack. Using the backward-looking tool of intelligence, **discovery may occur long after the attack has ended**. If the intelligence from the first victim is developed too late to prevent time on target on the first victim, the assumption is that suffering of the first victim can be used to defend subsequent victims.

This is Verizon's observed infiltration and response timeline:[20]



Attackers use spearphishing to complete the first six stages of the APT kill chain very quickly, opening the time on target window which can last for years. The infiltration is completed long before it is detected. Intelligence provides limited defense against spearphishing because the attackers understand that intelligence is a correlation activity which is easily defeated by not reusing attack elements. Thus, attackers use unique malware and single-use throwaway domains. Attackers misuse legitimate email services.[21] Not only is the data from the attack on the first victim generated after the first victim has sustained substantial time on target, the suffering of the first victim does little to defend subsequent victims. By changing attack characteristics as needed, every victim of an APT attack is the first victim.



As a practical matter, intelligence turns out be little more than chasing what's already gone.[22] By focusing the attack on a small number of victims (as few as one), attackers deprive intelligence-based defenses of the dots needed to connect the dots. After the kill chain is completed, defenders are left to collect artifacts of the attack in hopes of limiting time on target.

> The fallacy of the logic in monitoring and response is that you can detect the attack that bypassed the tools. If you could, then you would simply update the tools, which is how the security industry works (and failed) by and large. Instead, **humans end up detecting artifacts of attacks long after the attack has been successful—after the damage is done** [emphasis added]... It turns out once your customer records are leaked, your email archive published, your IP stolen, all the remediation and incident response in the world can't get it back. All the King's men couldn't put Humpty Dumpty back together and nor can you.
> – Anup Ghosh[23]

Rather than near real-time detection, tracking, and reporting of malicious activities, cyber defenders are in a situation more akin to that described by Plato almost 2,300 years ago in the *Allegory of the Cave*:[24]

> [Socrates] And now, I said, let me show in a figure how far our nature is enlightened or unenlightened: --Behold! human beings living in a underground cave, which has a mouth open towards the light and reaching all along the cave; here they have been from their childhood, and have their legs and necks chained so that they cannot move, and can only see before them, being prevented by the chains from turning round their heads. Above and behind them a fire is blazing at a distance, and between the fire and the prisoners there is a raised way; and you will see, if you look, a low wall built along the way, like the screen which marionette players have in front of them, over which they show the puppets. … To them, I said, the truth would be literally nothing but the shadows of the images.
>
> [Glaucon] That is certain.

The Attackers – Overall Capabilities

Rommel... you magnificent bastard, I read your book!

- *Gen. George S. Patton, as portrayed in the movie "Patton"*[25]

Cyber attackers read cyber security books. The attackers understand cybersecurity. The attackers are not static actors; the attackers adjust their attacks to overcome the defenses that are mounted against them.[26] The adaptability of human adversaries helps explain why infiltration is so successful and the median time on target is 229 days. [27]

In spearphishing attacks, the attackers understand and exploit the two-faced nature of email.[28] Email presents one face to the worldwide email system. It presents a completely different face to the email recipient. The face email presents to the worldwide email delivery system conforms to published standards to deliver email. The worldwide standards-based email system is designed to deliver email.[29] The technical requirements to create a technically valid email are published standards.[30] By conforming to the technical standards and industry practices, hackers exploit this

bias to deliver small numbers of deceptive emails.[31] The attackers create deception stories that are alluring to the target. This may consist of creating alluring social media personas[32], exploiting current events[33], mimicking conference materials[34], fake HR memos[35], or fake benefits documents[36] – there is no limit to the possibilities when deception is the goal. Clever draftsmanship drawing upon preconceived perceptions reinforced with intelligence gathered from the internet and elsewhere can result in a very convincing deception.

The attackers understand the defenses used to frustrate attacks.[37] The attackers:

- Misuse legitimate services.[38]
- Use polymorphic methods to create new malware.[39]
- QA their attacks against defensive measures.[40]
- Mount reconnaissance attacks to test technical defenses.[41]
- Utilize single-use throwaway domains.[42]
- Use clever programming techniques to defeat advanced sandboxing filters.[43]
- Circumvent malware blocking technologies with payloads that remain inert until the user is deceived into activating the payload.[44]
- Understand that human beings monitor system activity and the attackers use deception to hide in the monitored data stream.[45]
- Are patient.[46]

Verizon summarized the state of affairs by observing that attackers are getting better and faster at what they do. [47]

APT Courses of Action

Hope is not a course of action.

- *Adm. Leighton W. Smith, Jr., USN*[48]

Using its Cyber Kill Chain, Lockheed Martin describes the potential courses of defensive action at each phase of the attack:

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Source: Lockheed Martin[49]

Lockheed Martin's kill chain demonstrates the power of kill chain analysis. In this kill chain, before the attacker gets time on target, it must successfully complete six preliminary steps. Interdiction at **any** step prevents time on target. Defenders can focus their efforts on those steps in the kill chain at which the defender can disproportionately increase the attacker's costs and decrease the likelihood of a successful attack.

The kill chain alone also demonstrates why a kill chain must be used in the context of a larger frame of reference – the Course of Action (COA). "A COA is a potential way (solution, method) to accomplish the assigned mission."[50] A COA must pass five validity criteria:[51]

(a) Adequate – Can the COA accomplish the mission within the commander's guidance?
(b) Feasible – Can the COA accomplish the mission within the time, space and resource limitations?
(c) Acceptable – Are the costs and risks balanced with the benefits to be gained?
(d) Distinguishable – Are alternative COA's sufficiently different from one another?
(e) Complete – Does the COA answer the questions of who, what, where, when, how, and why?

Time is a crucial element in all COA's. Time is an express element of the COA feasibility criterion. Are defenders responding to what the attacker is doing or what the attacker did? Information about what the attackers did may be useful in interdicting future attacks which reuse attack elements, but that information cannot be applied retrospectively to deal with completed phases of the current attack.

Time is the factor that differentiates intelligence that may be used to defend against a current attack from intelligence that can be used to defend against future attacks. This diagram from *Intelligence-Driven Computer Network Defense* illustrates the time dimension of intelligence in kill chain analysis:

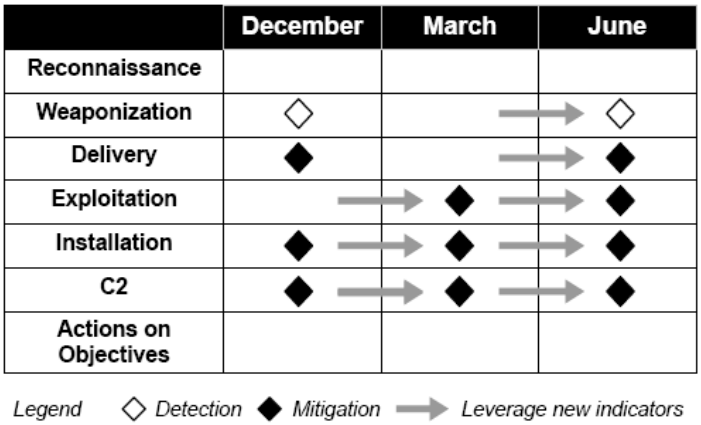


Figure 2: Illustration of the relative effectiveness of defenses against subsequent intrusion attempts

Source: Lockheed Martin

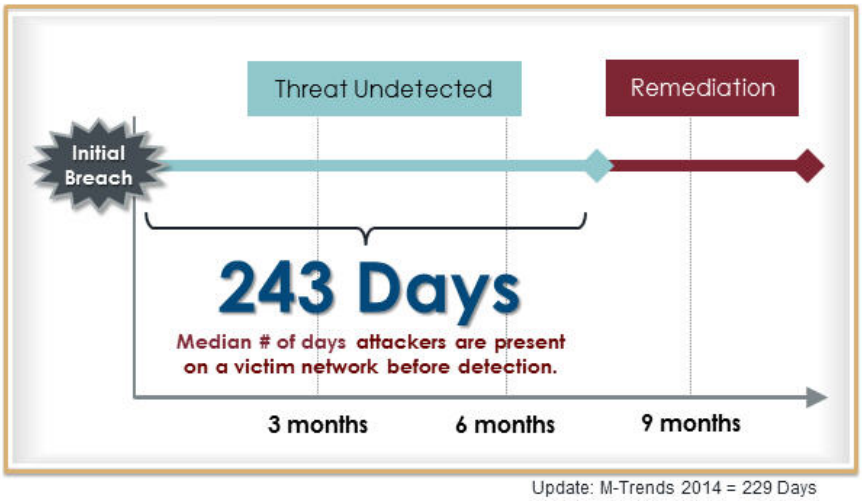
In December, no defenses were available regarding the subject exploit. In March, no defenses were available against the weaponized software or the delivery mode; however, by March a defense had been devised against the exploitation. "Figure 2" also gives meaning to the term "layered defense," illustrating that defenses do not need to be in place all of the time at every

level of the kill chain; effective defenses at any phase break the kill chain and prevent actions on objectives.

"Figure 2" also highlights a fundamental weakness of intelligence-based defenses – intelligence is the correlation of past events. This means that the following steps are required to convert observations into effective action:

- Realize that there is a problem.
- Analyze the problem.
- Determine the cause of the problem.
- Formulate a response to the cause.
- Test and validate a response.
- Release the response.
- Deploy the response.

In *Before We Knew It*[52], researchers from Carnegie Mellon University discuss the real world problems of finding malware, the time this process takes and the responses of malware authors. Realizing there is an APT attack and responding to it are generally not real time events.



Source: Mandiant[53]

Despite the fact that the initial breach required the completion of six preliminary steps, APT attackers consistently use spearphishing to complete the six steps to achieve time on target.[54] In the Red October attack, the attack went undetected for 5 years.[55] According to Mandiant, 63% of breaches are not detected by the victim, but are discovered by third parties.[56]

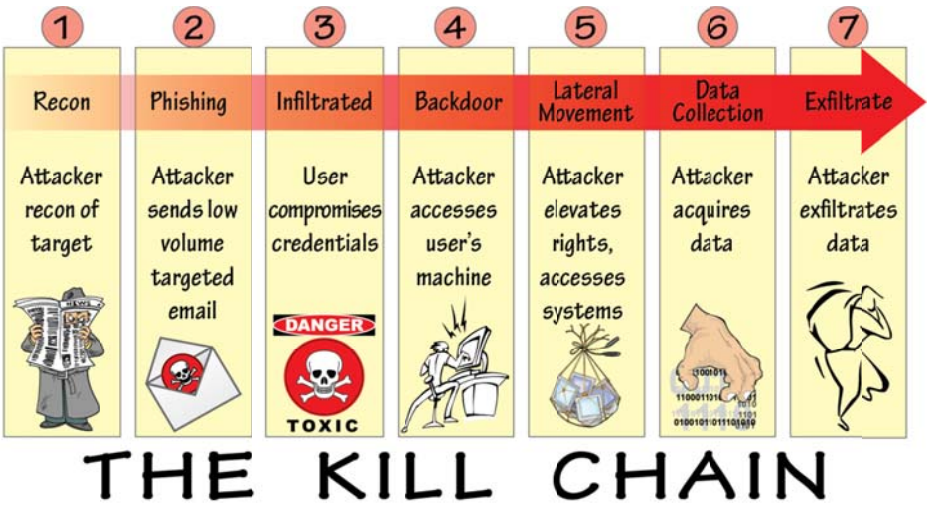
Moreover, the presence of malware is frequently purely transitory or non-existent. Malware is merely a means to obtain what every authorized user possesses – credentials. Mandiant is currently reporting that 100% of breaches involved stolen credentials.[57] After credentials have been obtained, the attackers erase the evidence of their intrusion, including the malware.[58] Mandiant reports that 46% of compromised machines contain no malware.[59] Once credentials are stolen, finding the unauthorized uses of credentials is extremely difficult.[60] During the time on target phase, defenders are searching for a mole – a user who is misusing real system access rights.

TrendMicro estimates that 91% of APT infiltration involves spearphishing and of that 95% uses email attachments.[61] Users are a unique element in the kill chain because:

- Users are not merely evaded – they must be persuaded to take specific acts.
- The required user acts constitute a non-trivial sub-kill-chain.
- The required user acts facilitate by-passing technical defenses.

While the Lockheed Martin "Courses of Action Matrix" posits a role for vigilant users, the reality is that users are not defensive assets – users are latent internal threats waiting to be activated with deceptive emails.

From the attacker's perspective, this is the APT kill chain:

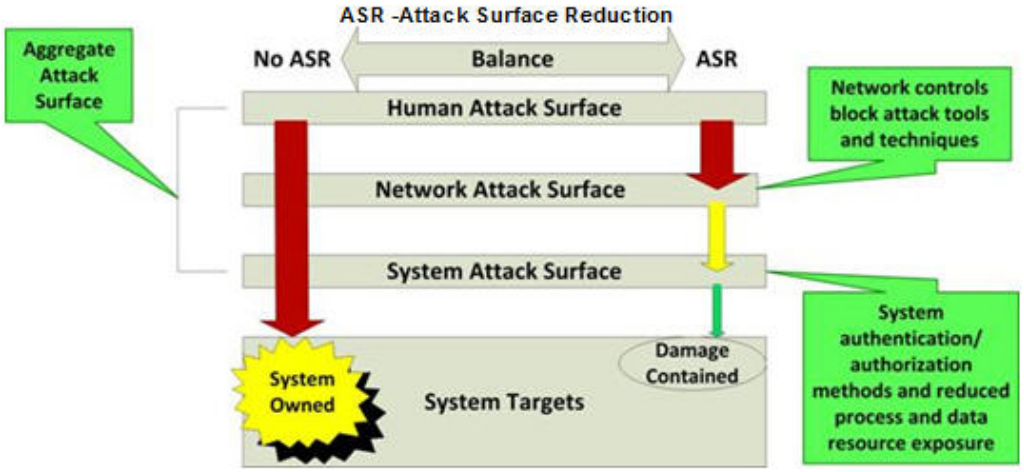


The focus of the attack is the user. The user provides three strategic objectives to the APT attacker:

1. The user by-passes the formidable security measures that isolate the intranet from the internet – a bridge that is easily accessible by email.
2. The user has credentials which allow internal system access.
3. Distinguishing authorized user activity from unauthorized user activity is extremely difficult and time consuming.

COA analysis requires a more comprehensive analysis than simple kill chains. Army Field Manual FM 5-0, *Army Planning and Orders Production*, offers three alternative methodologies that can be used alone or in combination to map COAs.[62] FM 5-0 advises that planners may also use methods of their own creation.

This paper adopts Tom Olzak's "Aggregate Attack Surface Model" methodology to map the cyber area of operations.[63] The Olzak model is the cyber analogue of the "belts" methodology described in FM 5-0.



Olzak Aggregate Attack Surface Model

Attackers and defenders realize that this kill chain hinges on the human attack surface, particularly the users' inadvertent decision to compromise credentials. Despite the "vigilant user" COA posited in *Intelligence-Driven Computer Network Defense*, the reality is that each side sees the user as a Pavlovian dog which will inexorably yield credentials on command. Thus:

- Attackers seek to deceive users into becoming internal threats;
- Defenders treat users as potential internal threats to be fenced-in and monitored.

Under JP-5-0, wargaming is the primary method to analyze COAs.[64] Under JP 5-0 the heart of the COA wargaming analysis process is comparison of multiple COAs based on the adversary capabilities, objectives, intent and the actions of other actors that could affect the outcome.[65]

Deception

All warfare is based upon deception.

- *Sun Tzu, The Art of War*

U.S. cyber systems are very vulnerable. Cyber-attacks from state and non-state adversaries are increasing.[66] Spearphishing is an important tool being used by the adversaries of the U.S. to infiltrate systems.

For purposes of U.S. military doctrine, deception is defined in Joint Publication (JP) 3-13.4, *Military Deception,* as follows:

> Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called MILDEC. [67]

Deception occurs in the mind of the decision maker. The purpose of deception is to influence the **perceptions** of the human target such that the target **thinks** a certain way as a step toward getting the target to make a **decision** that will result in the intended action.[68] Perceptions, thinking and decisions take place in the battlefield of the target's mind.

The military objective of deception must end in the desired act. JP 3-13.4 cites this example of military deception methodology:

> A perfect example of the methodology at work was Operation BODYGUARD in 1944, the deception plan in support of Operation OVERLORD (the D-Day invasion). In that example, the Allies conducted air raids, broadcasted false communications, and even built an entire deceptive army to convince the German high command that the real objective of the invasion was Pas de Calais. The German high command saw these operations ***(See),*** drew the conclusion that Calais would be the initial objective of the invasion ***(Think),*** and took the action of reinforcing the area with an entire field army ***(Do).***[69]

Operation BODYGUARD demonstrates a three-tiered cognitive process of deception which culminates in the adversary taking the desired action:[70]

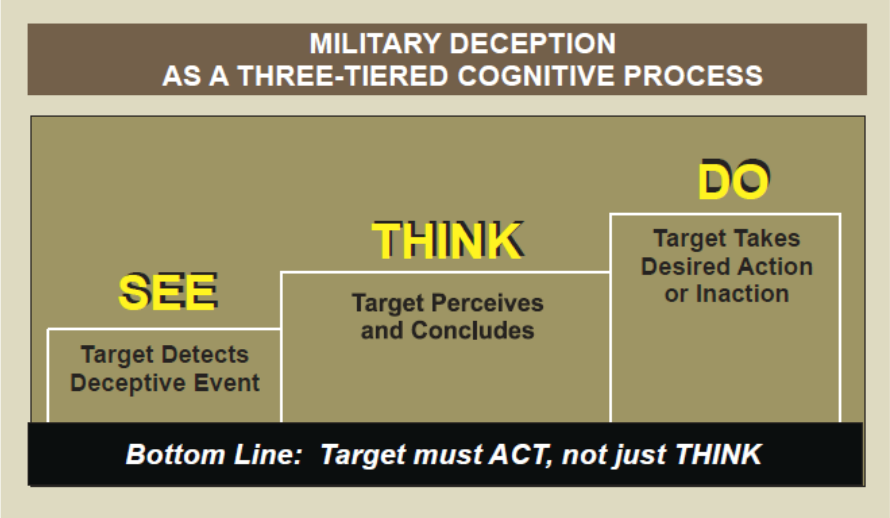


Figure IV-1. Military Deception as a Three-Tiered Cognitive Process

In an increasingly technical world, technology can be exploited as a tool of deception. During the Vietnam War, the air combat superiority of North Vietnamese MiGs was a serious threat to U.S. bombers. In Operation BOLO, the U.S. exploited technology to deceive North Vietnamese forces.[71] U.S. fighters were equipped with electronics to mimic bombers, flew bombing routes, and used bomber call signs and codewords. The North Vietnamese ground controllers saw bombers ***(See)***. The North Vietnamese air controllers drew the conclusion that they were under attack by bombers ***(Think)*** and took the action of deploying MiGs to engage the U.S. fighters which they had incorrectly concluded were bombers ***(Do)***. The superior U.S. fighters inflicted heavy losses on the North Vietnamese air force.

The field of operation of deception is the target's mind. The goal of deception is to manipulate the target's cognitive process in order to induce the target to make decisions that are advantageous to the attacker.

Spearphishing Viewed As Military Deception

Acting is all about honesty. If you can fake that, you've got it made.

- *George Burns*

Joint Publication (JP) 3-18.4, *Military Deception* states, "The cornerstone of any deception operation is the deception story. The deception story is a scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. It is a succinct statement or narrative of exactly what the MILDEC planner wants the target to believe to be the true situation, then decide and act on that basis."[72]

Under military deception doctrine one element in the construction of the deception story is the preconceived perceptions of the target. Reinforcing the target's preconceived notions lends credibility to the deception story. Deception operations that leverage the preconceived perceptions of a deception target have been very successful.[73]

Three factors influence the selection of the deception target. [74]

1. The target must be an adversary decision maker with the authority to take the actions that will achieve the deception objective.
2. There must be conduits to deliver the deception story to the target.
3. There must be sufficient intelligence about the target to develop a convincing deception story.

Applying these targeting factors to a cyber-attack reveals that email users are ideal targets for military deception.

1. The target must be an adversary decision maker with the authority to take the actions that will achieve the deception objective.

Email users decide with which emails to interact and how to interact with those emails. As the custodians of the first phase deception objective – credentials – users have the authority (in the sense of the power, not the permission) to take actions will achieve the deception objective.

2. There must be conduits to deliver the deception story to the target.

Military deception doctrine recognizes that rarely can the deception message be sent directly to the deception target. In the typical deception operation, significant effort must be devoted to assure that the deception message is conveyed to the targets and that other sources of information do not contradict or invalidate the deception message. Overcoming conduit problems to deliver the deception message to the target can become quite elaborate. Britain's World War II Operation MINCEMEAT, in which a corpse dressed as a British officer and chained to a briefcase full of fake documents was dumped off the Spanish coast, shows the lengths that must sometimes be taken to effectively overcome the conduit to deliver the deception story to the deception target.[75]

Email is the rare case in which the deception message can be delivered directly to the deception target.

3. There must be sufficient intelligence about the target to develop a convincing deception story.

The internet makes intelligence gathering about targets trivial. Attackers know how to use the Internet to find out who works inside organizations. Social media was used to identify the CIA agent responsible for the successful bin Laden operation.[76] Finding targets is as easy as taking pictures of employees in the parking lot.

Carnegie Mellon University researchers led by Alessandro Acquisti took photographs of student volunteers. Using facial recognition software on social networking sites, the researchers were able to identify 31% of the students by name. In another experiment, the Carnegie Mellon team was able to identify 10% of people who had posted their photos on public dating sites. The researchers have posted their research online, Faces of Facebook: Privacy in the Age of Augmented Reality.[77] The researchers report that they have been able to use profile photos and facial-recognition software to get details such as birth date and social security number predictions.

Hackers use LinkedIn as another source of useful information about people and the places they work.[78] Hackers even set up fake social media accounts to collect information about people inside an organization.[79]

Social networking sites are not the only source of useful social engineering data. Companies unwittingly publish vast amounts of information on their websites and in their public document filings in the form of metadata that is attached to their files. The metadata can include user names, IP addresses and email addresses.[80]

Email is an ideal medium for deception because the deception story can be so abbreviated. The email environment provides a vast array of highly compressed preconceived perceptions that are easily exploited. Employees expect emails from HR. Employees expect emails from colleagues. People expect to receive emails about current events. People expect package notifications from FedEx. People anticipate security notifications from IT. They respond to these messages through force of habit.[81] **It is easy for an attacker to conceive of a sender that the recipient trusts and to steal that trust with a cleverly designed email that appears, in the overall context of the email experience, to be from the trusted sender. The trust relationship to be abused is an integral element in the construction of the deception story.**

Operation MINCEMEAT demonstrates how the conduit is part of the deception story. Had the same information reached Hitler without the corpse, the uniform, the handcuffed briefcase, the fake love letters, and the other packaging, it is unlikely the false information delivered in the deception story would have been believed. In the case of spearphishing, the conduit is email. The email conduit brings with it predictable target behaviors.

Five studies on human behavior regarding deceptive emails are worth noting. The first is the West Point Carronade study from 2004.[82] The 2004 Carronade study was followed-up with Carronade II[83] and Carronade III.[84] The Carronade experiments showed how easily email

recipients could be deceived. The fourth study is the 2014 study, *Going Spear Phishing: Exploring Embedded Training and Awareness*, which demonstrated the ineffectiveness of training to overcome deceptive emails.[85] The fifth study is the 2011 five university study entitled, *Why Do People Get Phished?*[86]

In *Why do People Get Phished?*, the researchers concluded that two factors contribute to the success of phishing attacks. First, people do not adequately process information. Instead of carefully analyzing emails to determine the authenticity of the message, people pay little attention to the email interaction and merely rely on simple clues (such as urgency and perceived relevance) in making email decisions. Second, when dealing with a large volume of email, habits, rather than careful thought, govern email interactions. The researchers conclude:

> Domain specific knowledge gained through education, awareness, or experience, therefore, has a limited effect because the application of knowledge requires elaboration. Among the cues used by phishers, the urgency cues are by-far the most virulent. Such cues engender a higher degree of information processing. As a result, other deceptive clues in the email's source or the grammar and spelling in the email do not receive much elaboration. This overall effect is further strengthened by the individuals' media use habits, which is the other main reason people get phished. Habitual patterns of media use, in the presence of high levels of email load, tend to trigger automatic responses to relevant looking emails. That is, individuals exposed to relevant emails, with strongly worded urgency cues, in the presence of high email load, are significantly more likely to be phished. Together, relevance, urgency cues, and habitual media use patterns form a triad of influence and largely determine individuals' phishing susceptibility.

The job of the spearphisher is to craft an email which contains a consistent constellation of content to trigger the perceived relevance/urgency/habit triad. **A crucial element in triggering this perceived relevance/urgency/habit triad is the trust relationship between the recipient and the perceived sender.** For example, an email that appears to be from the trusted sender FedEx about a package delivery would satisfy the triad. On the other hand, an email from trusted sender FedEx about a tax penalty would be less likely to satisfy the triad because a message from FedEx about taxes fails the relevance test and is, therefore, easily identified by the victim as a likely attempt at deception. More simply stated, an email from FedEx about taxes is a poor deception story because taxation is not a preconceived notion generally associated with the FedEx trust relation.

The following sample spearphishing emails demonstrate stealing trust to trigger the perceived relevance/urgency/habit triad. In these three typical examples, the conduit is email, email technology displays deceptive sender information, the content is deceptive and the call to action is an integral element of the deception story. The emails are not perfect – they are merely good enough to steal trust and trigger the perceived relevance/urgency/habit triad.

Sent: Tue 4/23/2013 12:12 PM
From: [An AP staffer]
Subject: News

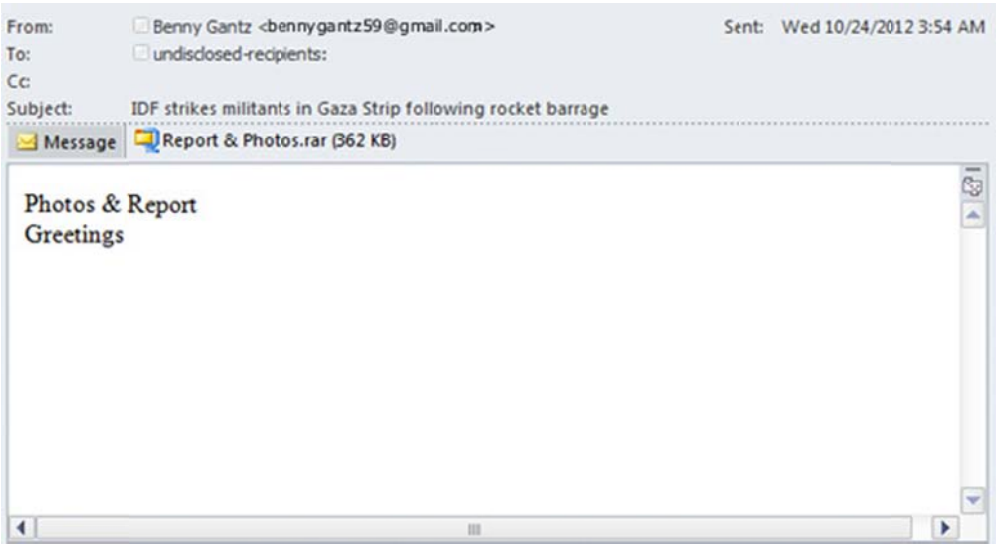
Hello,

Please read the following article, it's very important :

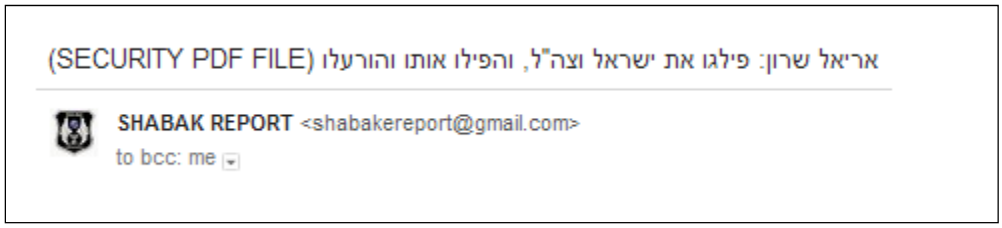
http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/

[A different AP staffer]
Associated Press
San Diego
mobile [removed]

This email compromised the Associated Press, resulting in a fake tweet that the President was injured in a bombing at the White House.[87] The reporter saw an indication of relevance from a trusted colleague ***(See)***. The target drew the conclusion he should click on the link ***(Think)*** and took the action to click the link ***(Do)***. The consistent constellation of content comprising the perceived trusted sender, the text and the call to action caused the recipient to conclude this email was real, despite the fact that the purported sender and the purported signer were different.



This email forced all police computers in Israel to be taken offline.[88] The Israeli police officer saw an email from the trusted head of Israeli defense forces delivering a report about enemy rocket attacks ***(See)***. The police officer drew the conclusion that he should open the attachment ***(Think)*** and took the action of opening the attachment ***(Do)***. The consistent constellation of content comprising the perceived trusted sender, the text and the call to action caused the recipient to conclude this email was real, despite the fact that the purported sender, an Israeli general, probably does not send critical security email to police from a Gmail account.



This email compromised computers in Israel's Civil Administration of Judea and Samaria.[89] This agency is responsible for entry and work permits from the West Bank to Israel. Shabak is the common name of the Israel Security Agency, the internal security service that is analogous to the FBI. Note how the attacker used the logo function of Gmail to enhance the perceived trustworthiness of the sender. The consistent constellation of content comprising the Shabak name, the Shabak logo, a reference to a report, all combined in the recipient's mind into an important attachment from Shabak, a trusted sender. Thus, the recipient saw an email from Shabak with an important attachment ***(See)***. The recipient drew the conclusion that he should open the attachment ***(Think)***. The recipient took the action of opening the attachment ***(Do)***. The victim did not question Shabak using a Gmail address (shabekreport@gmail.com) instead of a government email address.

In February 2015, the compromise of over 80 million health care records in the custody of Anthem, the second largest health insurer in the United States, was disclosed.[90] The attacker leveraged military deception by using "we11point.com" instead of the company's real domain "wellpoint.com" to deceive email recipients.[91] Substituting two numerals for two letters of similar appearance was all that was needed to mount an effective deception campaign.

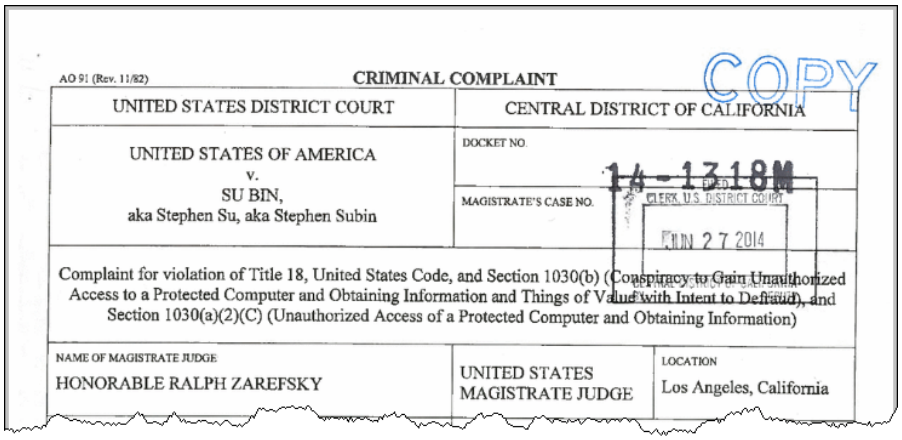
Addressing the problem of differentiating attack emails from benign emails, Col. Gregory Conti, U.S.A, Military Academy Professor and the Director of the Information Technology Operations Center at West Point, observed:[92]

> What's 'wrong' with these e-mails is very, very subtle. They'll come in error-free, often using the appropriate jargon or acronyms for a given office or organization.

These examples demonstrate how spearphishing efficiently accomplishes the three-tiered cognitive deception process. In constructing the deception story, the sender is not bound to tell the truth.[93] The mission of the attacker is to fabricate a consistent message that exploits the victim's preconceived notions. Email facilitates extremely compact and persuasive deception stories in which the highly personalized conduit reinforces the deception story. In these real world examples, the results of the deception were compromised systems.

The effectiveness of spearphishing and the difficulty of detecting network intruders were again demonstrated with the 27 June 2014 charging of Chinese cyber spies who broke into Boeing's networks using spearphishing, remaining undetected from 2009 to 2013. These spies targeted

information related to the C-17 transport and the F-22 and F-35 fighters.[94]



AO 91 (Rev. 11/82) **CRIMINAL COMPLAINT**

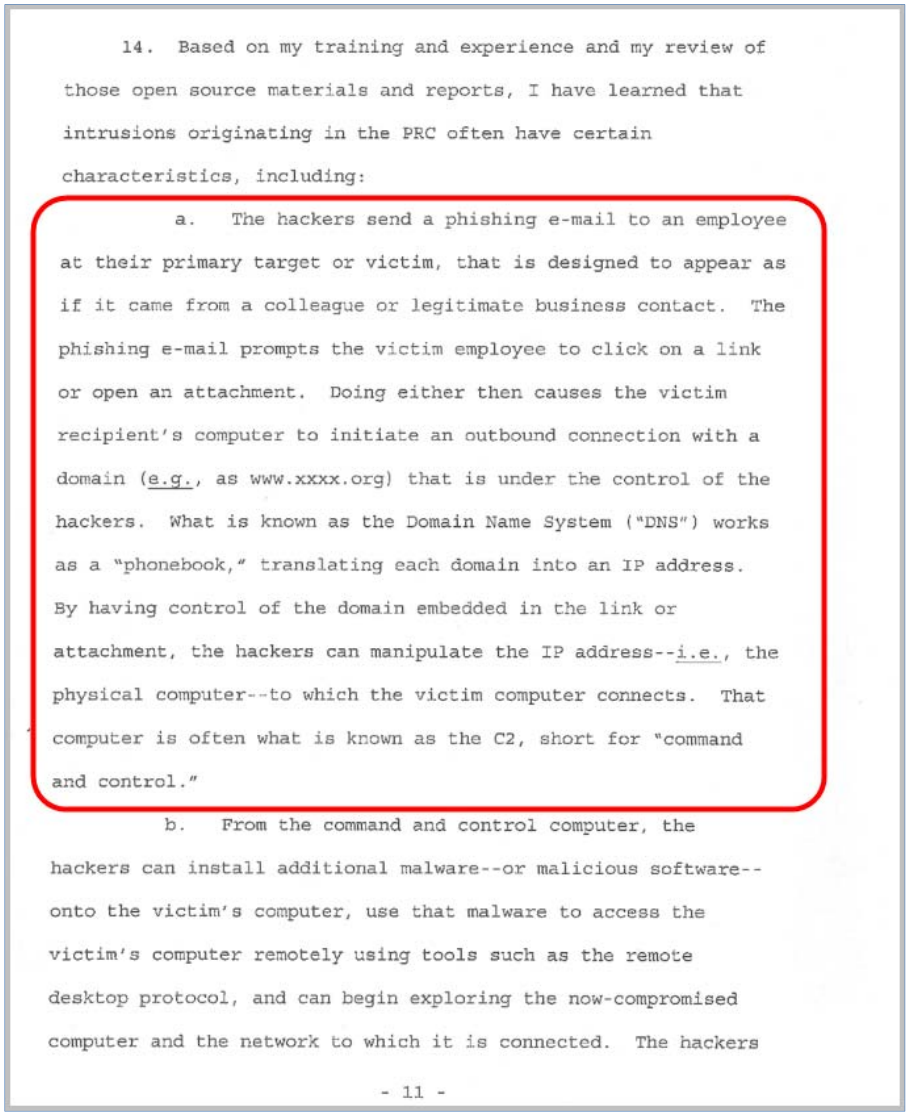
COPY

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v. SU BIN, aka Stephen Su, aka Stephen Subin	DOCKET NO. MAGISTRATE'S CASE NO. 14-1318M

FILED
CLERK, U.S. DISTRICT COURT
JUN 27 2014
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

Complaint for violation of Title 18, United States Code, Section 1030(b) (Conspiracy to Gain Unauthorized Access to a Protected Computer and Obtaining Information and Things of Value with Intent to Defraud), and Section 1030(a)(2)(C) (Unauthorized Access of a Protected Computer and Obtaining Information)

NAME OF MAGISTRATE JUDGE		LOCATION
HONORABLE RALPH ZAREFSKY	UNITED STATES MAGISTRATE JUDGE	Los Angeles, California



14. Based on my training and experience and my review of those open source materials and reports, I have learned that intrusions originating in the PRC often have certain characteristics, including:

a. The hackers send a phishing e-mail to an employee at their primary target or victim, that is designed to appear as if it came from a colleague or legitimate business contact. The phishing e-mail prompts the victim employee to click on a link or open an attachment. Doing either then causes the victim recipient's computer to initiate an outbound connection with a domain (e.g., as www.xxxx.org) that is under the control of the hackers. What is known as the Domain Name System ("DNS") works as a "phonebook," translating each domain into an IP address. By having control of the domain embedded in the link or attachment, the hackers can manipulate the IP address--i.e., the physical computer--to which the victim computer connects. That computer is often what is known as the C2, short for "command and control."

b. From the command and control computer, the hackers can install additional malware--or malicious software--onto the victim's computer, use that malware to access the victim's computer remotely using tools such as the remote desktop protocol, and can begin exploring the now-compromised computer and the network to which it is connected. The hackers

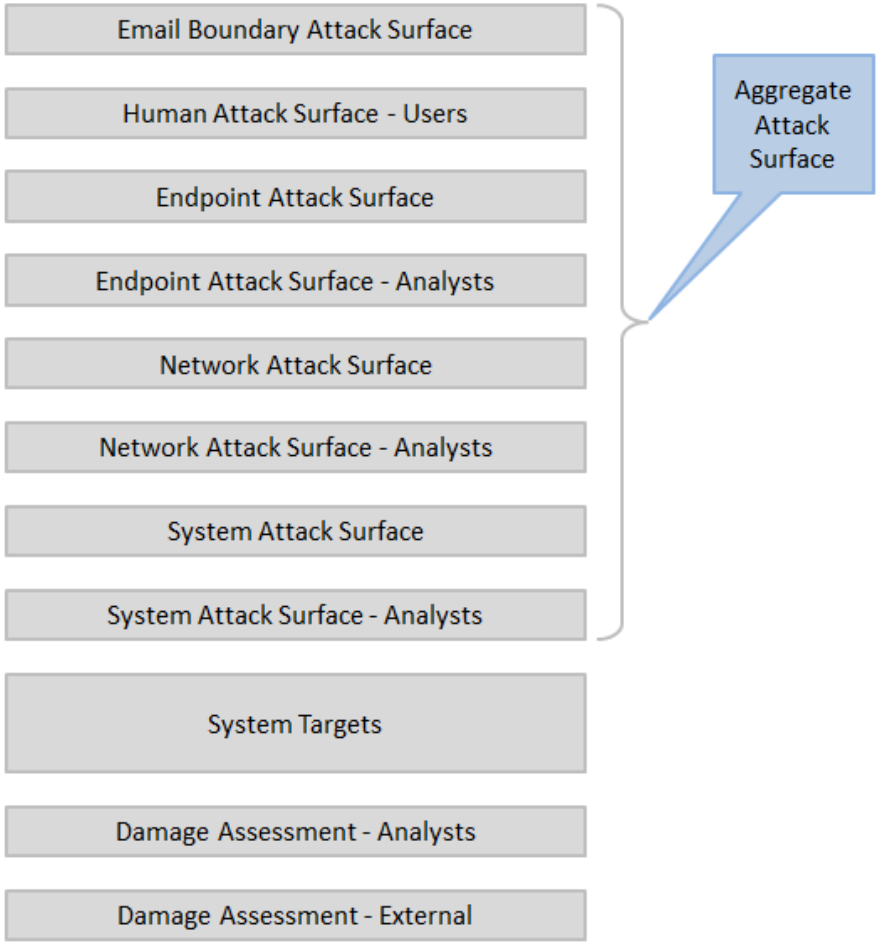
- 11 -

The charging document also details the anti-forensics that the attackers used to evade detection after they infiltrated Boeing using deceptive emails.[95]

Wargaming APT

> … France's vigilance once was lulled by undue reliance on the supposedly impregnable Maginot Line.
>
> - Irving R. Kaufman, Chief Judge of the U.S. Court of Appeals for the Second Circuit

In this paper we propose a modified version of Olzak's "Aggregate Attack Surface Model" methodology to map the cyber area of operations.



Modified Olzak Aggregate Attack Surface Model

Starting from the top of the model.

- Email Boundary Attack Surface: Technical measures such as proxy filters, in-line AV and queuing block content from reaching the user. This layer also includes "next generation firewalls" which use sandbox technology to detect malicious email payloads.
- Human Attack Surface – User: The deception target, the email recipient.
- Endpoint Attack Surface: Technical means such as AV and patches, DEP, and "chroot" jail prevent the execution of exploits which the user implements as the result of deception. HIDS and endpoint logging report user activity to analysts.

- Endpoint Attack Surface – Analysts: Recent advances in technology have seen the introduction of Endpoint Threat Detection and Response (ETDR) solutions which provide endpoint data to analysts.
- Network Attack Surface: Technical means which extend the endpoint technical defenses to network activity. These include "chroot" jail, AV, Firewall ACL, NIPS, Tarpit and DNS Redirect.
- Network Attack Surface – Analysts: Skilled cyber security professionals monitor and analyze endpoint and network activity logs generated by NIDS and NIPS to discover unauthorized activities.
- System Attack Surface: Technical means such as "chroot" jail and DEP block the attacker from accessing the objectives.
- System Attack Surface – Analysts: Skilled cyber security professionals monitor and analyze endpoint and network activity logs generated by HIDS, NIDS and NIPS to discover unauthorized activities.
- System Targets: The objective.
- Damage Assessment – Analysts: Skilled cyber security professionals monitor and analyze endpoint and network activity logs generated by HIDS, NIDS, NIPS and non-cyber sources (for example financial audits to reveal discrepant bank activity) to discover unauthorized activities.
- Damage Assessment – External: Agencies outside of the targeted enterprise discover apparent discrepant activity and report that information to the victim.[96]

When this modified model is applied to the Lockheed Martin Course of Action, the table below shows how the wargame proceeds.

Time/Event	H-4	H-Hour	H+ Minutes	H+ Hours	H+ Days/Weeks/Months
Enemy Action	Finalizes deception story	Transmits deception story		Credentials Seized C2 Established	Actions on Objectives
Email Boundary Attack Surface					
Human Attack Surface - Users			See, Think, Do		
Endpoint Attack Surface				Reporting	
Endpoint Attack Surface - Analysts				Analysis	
Network Attack Surface				Reporting	
Network Attack Surface - Analysts				Analysis	
System Attack Surface				Reporting	
System Attack Surface - Analysts				Analysis	
Damage Assessment - Analysts					Monitoring, Response, Remediation
Damage Assessment - External					Monitoring, Notifying, Coordinating, Recommendations

H-4. In the hours preceding the attack, the attacker finalizes the deception story. Carefully coordinating the deception story with the preconceived perceptions to be exploited enhances the deceptive power of the deception story.

H-Hour. The attack commences with a deceptive email targeting a single user. The message is crafted to evade email filters. It carries a latent payload that is only activated by human

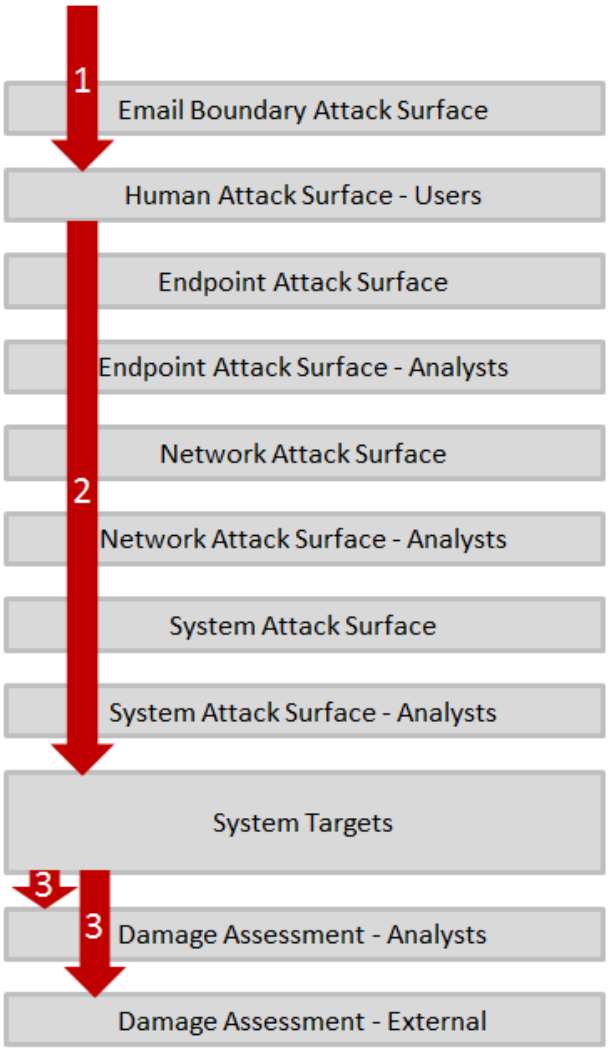
intervention, thereby evading advanced firewall and other defenses. The email is delivered to the target.

H+ minutes. The target Sees the email, Thinks it is real and Does the compromising action intended by the attacker. The attacker now has legitimate user credentials to use as the attacker sees fit. The exploit is of a nature that it evades the automated defenses.

H+ Hours. The attacker has established C2 and has access to the System Targets. The defenders are receiving reports from their system monitoring tools. The data being reviewed is being manipulated by the attackers; the analysts See normal data, Think they are secure and Do nothing.

H+ Days/Weeks/Months. After enjoying substantial time on target – and possibly attaining all mission objectives – the attack is discovered and remediation is implemented.

This is the wargame as viewed using the Modified Olzak Aggregate Attack Surface Model:



Events

1. Attack email delivered to target.
2. Target deceived into compromising systems.
3. Internal and external analysts look for evidence of compromise.

APT Wargame – Modified Olzak Attack Surface Model

In comparing the time to compromise to the time to discovery gap, Verizon made these observations:[97]

- The attackers seldom need days to get their job done, while the defenders "rarely manage to get theirs done in a month of Sundays."
- The trend plainly shows that attackers are getting better and faster at what they do at a higher rate than defenders are improving their trade.
- The amounts spent on network monitoring are ineffective.

Much as the French invested vast sums in defenses that were easily circumvented, vast sums are being spent on a cyber-Maginot line[98] which is easily overcome by spearphishing attacks.

The weak link in cyber defenses is the user. Lockheed Martin posits a "Vigilant User" in its Courses of Action Matrix. The notional role of users in cyber security is recognized under the Federal Information Security Management Act of 2002.[99] 44 USC§ 3544 (b)(4) mandates cybersecurity awareness training for federal personnel. 44 USC § 3544 (b)(5) requires periodic testing and evaluation of cybersecurity effectiveness. 44 USC § 3544 authorizes the National Institute of Standards and Technology ("NIST") to implement FISMA. NIST SP800-53r4 requires that personnel be trained to spot spearphishing and that they report spearphishing to security personnel.

In order to support the role of the vigilant user, the Olzak Attack Surface Model is further modified to add the Enterprise Attack Surface – Analysts. This is the wargaming of a COA which includes a vigilant user.

Time/Event	H-4	H-Hour	H+ Minutes	H+ Hours	H+ Days/Weeks/Months
Enemy Action	Finalizes deception story	Transmits deception story			
Email Boundary Attack Surface					
Human Attack Surface - Users			Report to Analysts		
Enterprise Attack Surface - Analysts				Analyze Attack Implement Countermeasures	Counterattack
Endpoint Attack Surface					
Endpoint Attack Surface - Analysts					
Network Attack Surface					
Network Attack Surface - Analysts					
System Attack Surface					
System Attack Surface - Analysts					
Damage Assessment - Analysts					
Damage Assessment - External					

H-4. In the hours preceding the attack, the attacker finalizes the deception story. Carefully coordinating the deception story with the preconceived perceptions to be exploited enhances the deceptive power of the deception story.

H-Hour. The attack commences with a deceptive email targeting a single user. The message is crafted to evade email filters. It carries a latent payload that is only activated by human

intervention, thereby evading advanced firewall and other defenses. The email is delivered to the target.

H+ minutes. The target Sees the email, DOES NOT Think it is real and AVOIDS the compromising action intended by the attacker. The deception target reports the suspicious email to experts.

H+ Hours. The experts analyze the deception message, determine that it is deceptive. The experts can determine the ACT desired by the attacker. The experts are able to understand the attack during the active phase of the attack. The Enterprise Attack Surface – Analysts now have the upper hand. The defenders can use the ACT of the attack message to deceive the attacker. Rather than a passive honeypot[100], the defenders can respond to the deceptive message by providing the attacker with deceptive information, such as providing the attacker with unique credentials that access honeypots.

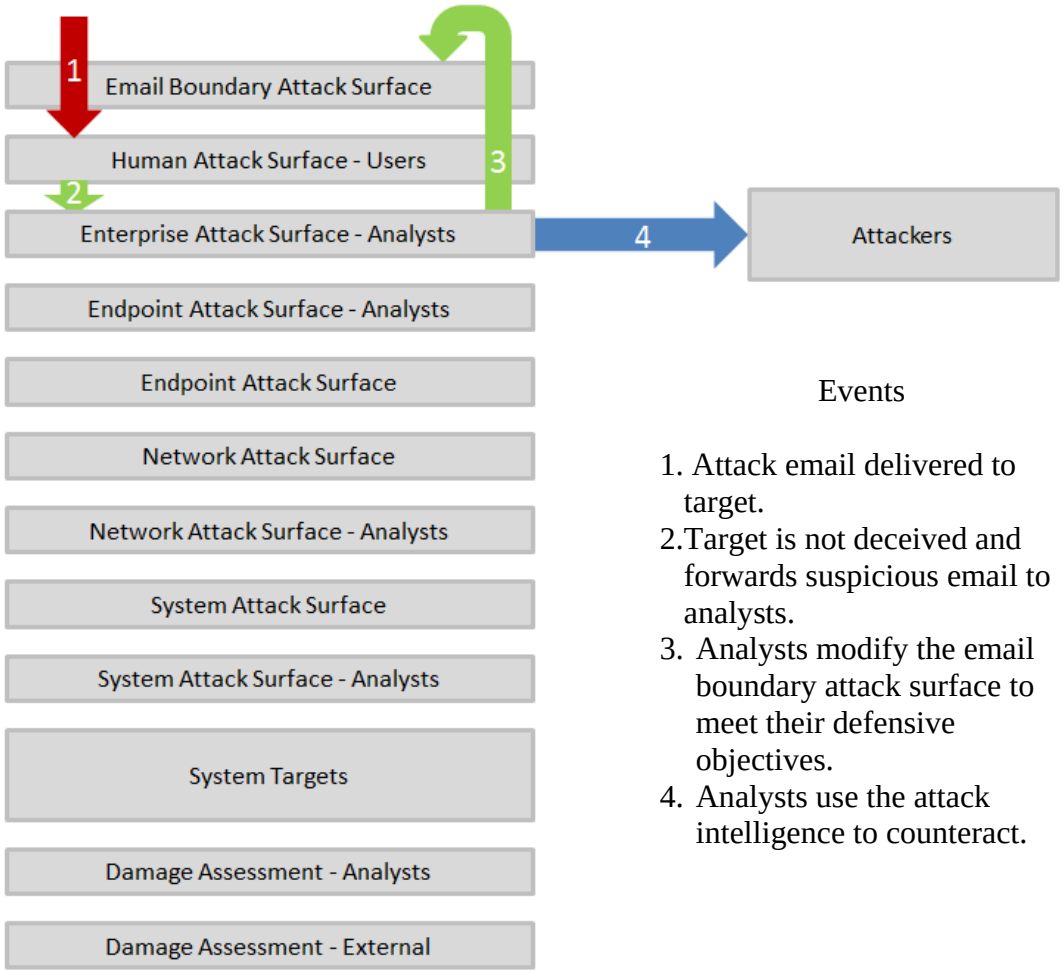
The downstream deception techniques which cause human analysts to be deceived and overlook unauthorized network activity are stripped of their deceptive power by being identified at the beginning of the attack; when the defenders know what to look for, deception is far less effective. The target Sees the deceptive log data, DOES NOT Think it is real and Avoids the error of permitting malicious activity. Instead of looking for an unknown needle in a haystack, the defenders know exactly what to look for.

In order for the attack to succeed, the attacker must support the attack with an external attack infrastructure and a target infrastructure that the attacker must install inside the victim's systems. These attack infrastructures can be used against the attacker IF the attack is identified while it is in progress. In Tools of Engagement - Zero Dark 243 Days, Mandiant describes how defenders can turn the tables on attackers when the attack information is identified during the initial infiltration using the deceptive message.[101]

Actively managing the attack and counterattack are new roles which have been assigned to a new "belt" which is termed "Enterprise Attack Surface – Analysts." The key distinction between Mandiant's defenses in Tools of Engagement - Zero Dark 243 Days and the typical APT is that in Tools of Engagement - Zero Dark 243 Days Mandiant had the good fortune that the attacker reused a spearphishing campaign that was known to Mandiant. Regrettably, good fortune is not systematically reproducible. In the next section of this paper deception countermeasures will be proposed in which never before seen attacks can systematically be identified and turned into counterattacks.

H+ Days/Weeks/Months. The attacker is denied time on target. The attacker is subjected to counterattack.

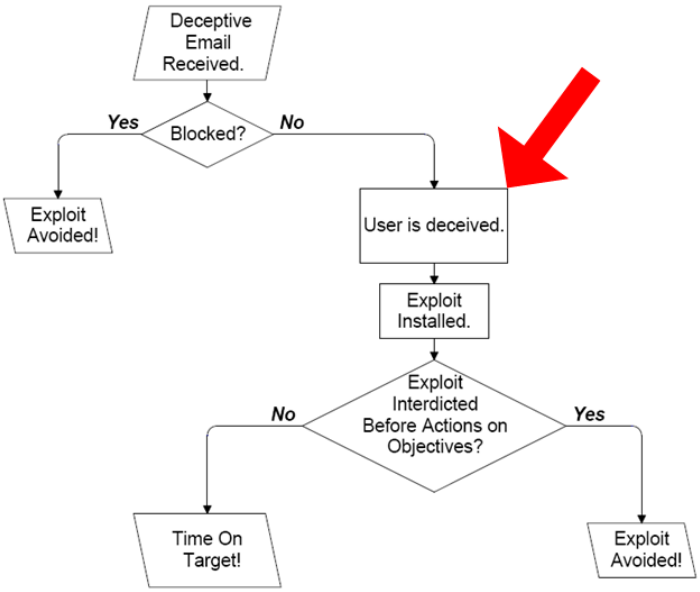
This is the wargame as viewed using the Extended Modified Olzak Aggregate Attack Surface Model:



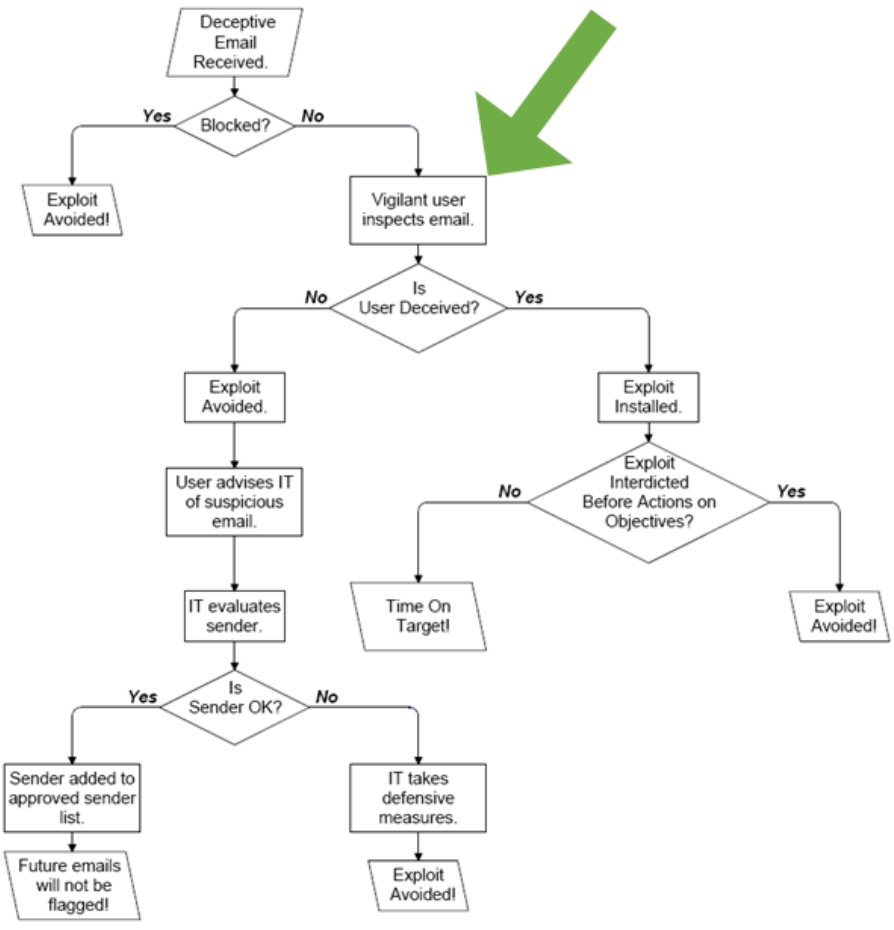
APT Wargame – Extended Modified Olzak Attack Surface Model

An alternative view of the COAs can be shown as flowcharts:

COA1



COA2



This table compares the two COAs using the five COA validity criteria: [102]

	COA1	COA2
Adequate	No	Yes
Feasible	No	No
Acceptable	No	Yes
Distinguishable	Yes	Yes
Complete	Yes	Yes

The summary comparison of the two COA's:

Course of Action	Advantages	Disadvantages
COA 1	Can be implemented consistently with current technology.	Attacker obtains substantial time on target.
COA 2	Attacker is denied objectives. Defenders are able to counterattack and deprive attacker of use of expensive attack infrastructure.	Users are easily deceived, training is ineffective.
Discussion COA 2 is clearly preferred to COA 1. COA 2 requires that rank and file users perform email technical analysis that is impossible.		

COA Decision Matrix – Subjective Analysis[103]

COA2 is clearly superior to COA1. COA2 shows the Attack Surface Reduction benefits to be derived from vigilant users. COA2 is incorporated in FISMA. COA2 is incorporated in Lockheed Martin's Courses of Action Matrix. COA2 is a good theory. Standing between COA1 and COA2 is military deception facilitated by email technology. Email is the cyber analog of a sentry manning a post in which the attackers seeking base admission create their own base passes using the same tools, materials and manuals as base security. COA2 fails because email recipients are unable to distinguish trustworthy emails from suspicious emails in operational environments. With existing email technology, COA2 is not feasible. Like the Maginot Line, defenders hope current cyber defenses are effective, yet these defenses are a failure.

APT Counterdeception – Human Sensors

> In theory there is no difference between theory and practice. In practice there is.
>
> - Yogi Berra

Given the general awareness of spearphishing and the obvious benefits of vigilant users, why is spearphishing so persistent? **Because, in reality, users do not contribute to cyber-defense; users are latent internal threats waiting to be activated with military deception perpetrated**

using email. This is why current defenses rely on blocking threats from reaching users and on restricting users' privileges.[104]

The Committee on National Security Systems National Information Assurance Glossary defines countermeasures as:[105]

> Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

With the unwitting assistance of the deception target, spearphishing attackers are able to circumvent every technical measure to accomplish their presence in targeted systems. In a matter of mere hours, 84% of attackers have completed the intrusion kill chain and are exploiting time on target. The user, rather than being vigilant, is coopted via deceptive emails into being the unsuspecting agent of the attacker. As the public attack surface, the user is a critical requirement for the intrusion. The user is a critical element that is remarkably consistent in its reliability as an intrusion vector.

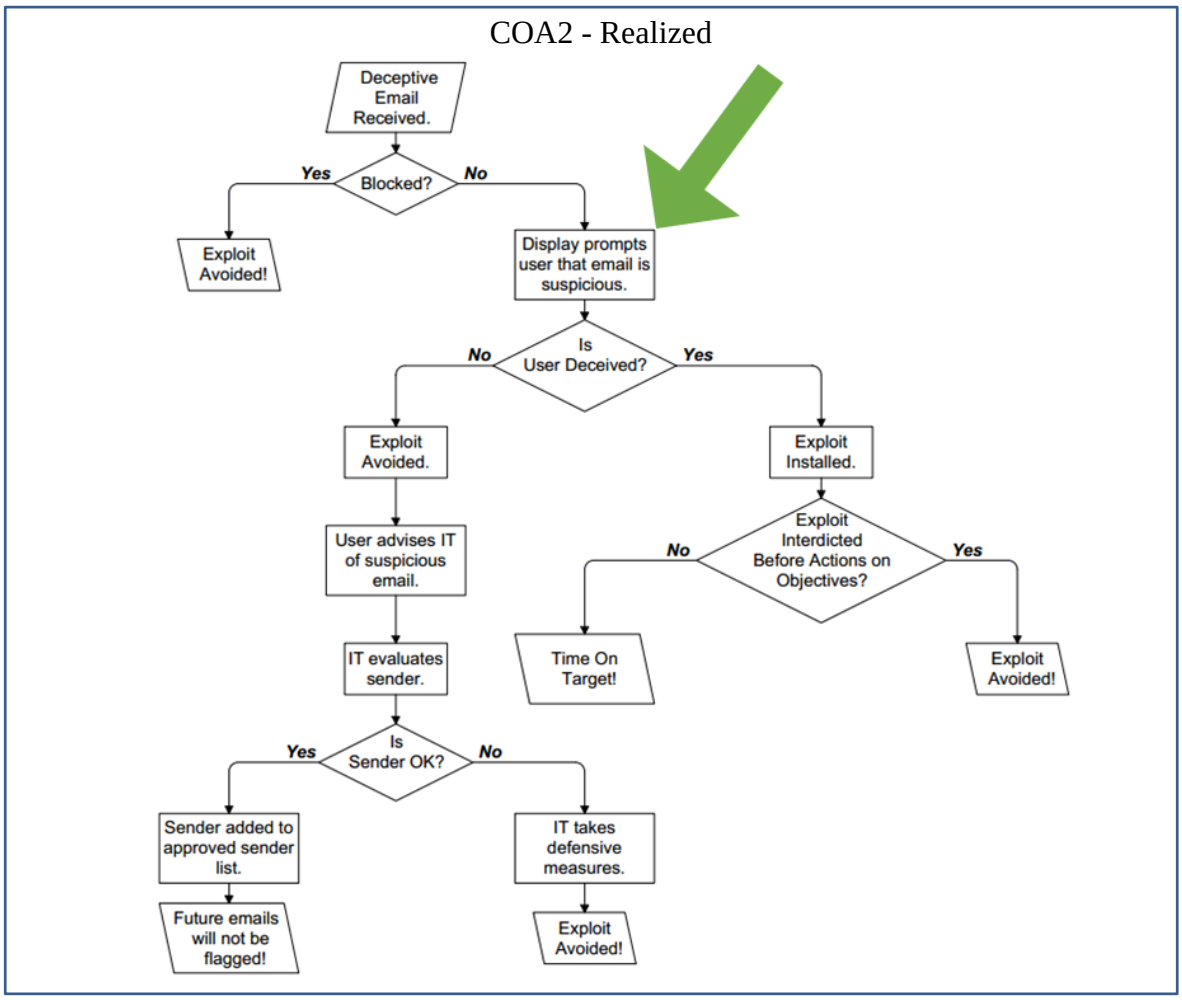
It is critical that many layers of defense are used by organizations to defend their intellectual property. Operating systems and browsers must be current and patched. The latest software applications should be deployed with all patches installed in a timely manner. State of the art security software should be deployed. Systems should be monitored. Staff must be trained. But deploying these means leaves the infiltration method of choice – deceptive emails – essentially un-impacted. A comprehensive cyber defense must implement a solution to address that "relevance, urgency cues, and habitual media use patterns form a triad of influence and largely determine individuals' phishing susceptibility."[106]

In spearphishing attacks the attacker's goal is to deceive the user. Attackers can contrive and dispatch convincing deception stories at will; deception stories which exploit trusted relations. Because intelligence identifies factors which the attackers can change in the face of defenses, intelligence which seeks to adapt defenses in response to spearphishing attacks will be ineffective in countering future spearphishing attacks. The current intelligence driven process of monitoring/response/remediation is the cyber implementation of the old adage, "generals fight the last war." As the defenders identify and respond to yesterday's deception story, today brings new fodder for new deception stories and new attacks.

When military deception is considered in the threat profile, human decision-making factors must be deployed in the defensive measures. Deception targets people, not systems. The technology of deception is psychology, not computer science. Deception must be detected and reported by the human targets – the human targets must become human sensors that perceive suspected attacks and report them to IT professionals. In order for the human targets to act as human sensors, they require real time guidance from IT. When fighting deception which is based on stolen trust, IT can provide guidance about trusted senders. Although it is easy for an attacker to create a deception story and yet another Gmail account that appears to be email from a trusted sender, it is difficult for an attacker to use the real trusted email account. Moreover, while the user is poorly equipped to decide which email senders are trustworthy, IT can make that determination. Leveraging existing email authentication technology, IT can, in fact, divide the universe of email senders into two groups – trusted and untrusted. Armed with trust information from IT, users can

detect and report deceptive emails – those that purport to be from a trusted sender but are not, to IT – thereby:

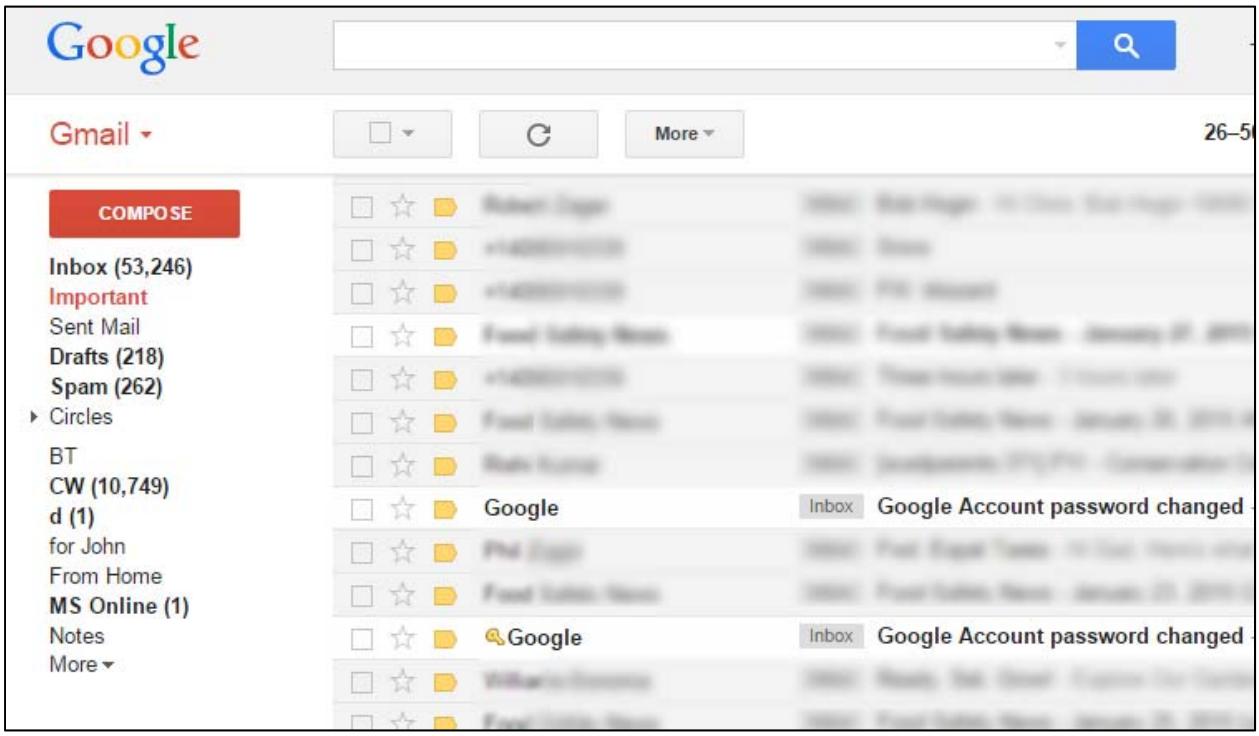
- Disrupting the deception that APT attackers depend upon to compromise users.
- Enabling the defensive response at the delivery phase of the kill chain.



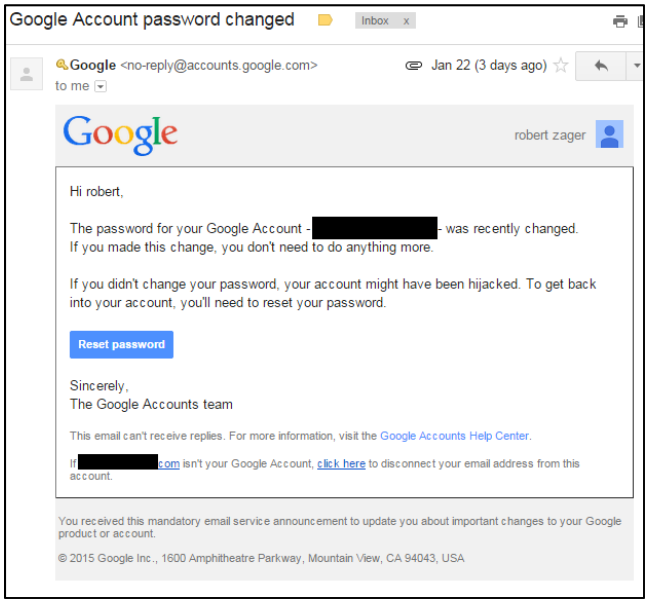
COA2 becomes feasible when military deception countermeasures are implemented by providing trustworthiness indicators to the user.

This is an example from Gmail of technology which modifies the email display to provide a visual indicator when there is certainty respecting identity of the sender of email. This screenshot

shows Gmail with the “Authentication icon for verified senders” feature enabled.

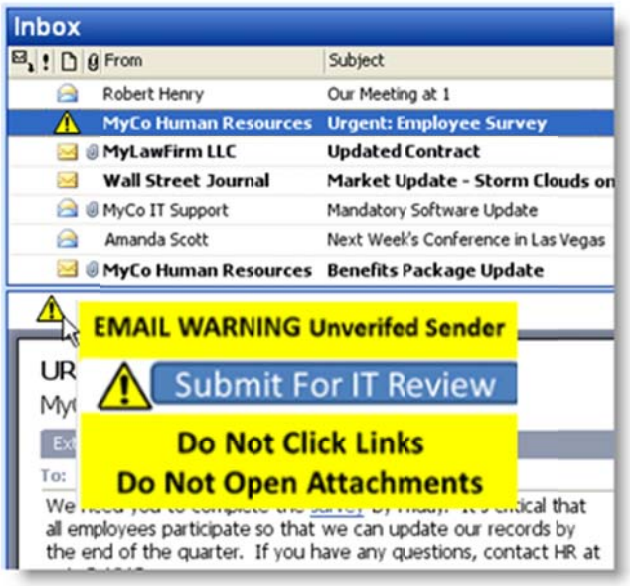


The two Google emails both notify the recipient that a password change has occurred. The upper Google email is a simulated attack created by misusing a real Gmail account for deception. The lower Google email is a real Google alert. Each message provides a strong call to action to click the embedded links. When the user encounters these emails a new factor is added to the constellation of consistent content – trust marking. The lower Google alert has the historical constellation of consistent content and the new factor – the trust indicator. The upper Google alert also has the entire historical constellation of consistent content; however, the trust indicator in the new constellation of consistent content is significant by its absence. That absence disrupts the perceived relevance/urgency/habit triad, thereby reducing the likelihood that the recipient will be deceived by the attempt to co-opt the Google trust relationship. As shown below, the trust indicator also appears in the opened email, further reinforcing the presence of the trust indicator in emails from trusted senders.



With trust indicators it is easy for the recipient to differentiate the real Google warning from the fake warning because the real message has Google's trust indicator in the listview and in the message.

This is an example from *Outlook*, the popular business email client, with *SP Guard*[107] from Iconix installed:



Two emails purport to be from MyCo Human Resources, yet only one is real. Here, the untrusted message is flagged. Again, the user is provided with a simple means to distinguish a trusted sender from an untrusted sender. An alternative implementation is "IFF mode" in which *SP Guard* only identifies known good emails. This is analogous to well-established military Identification: Friend or Foe systems which identify only known friendly elements.[108]

In these marking systems, instead of the unqualified user attempting to engage in complex IT task of determining the trustworthiness of a sender, expert IT personnel have made the trust determination and communicated that in a simple and easy to understand interface. If the user is enticed by the message which attempts to steal the trust of a trusted sender, the modified display provides the user with trustworthiness information. Even in the Shabak spearphishing attack which used the Shabak logo, that sender assigned marking would be inconsistent with actual trust indicators and would stand out for what it is – an attempt to deceive. In this environment, it is more difficult to deceive the user. The user is less likely to be recruited by the attacker – instead the user can alert IT and IT can apply its expertise to determine if the sender is trustworthy, and should be added to the trusted sender list, or if the sender is an attacker. The trust decision is moved, in real time, from the unqualified user to technical experts. Rather than the kill chain advancing to the time on target phase, the attack is interdicted during infiltration.

Systems are under attack from clever and determined opponents employing deceptive spearphishing emails as a means of infiltration. As has been demonstrated in numerous cases, that opponent is persistent – eventually the deception target will respond to a carefully crafted email and that response will initiate a series of events that will result in cyber espionage. Deceptive email is so effective in eliciting the ***See, Think, Do*** deception process that ProofPoint

estimates an attack of as few as ten emails is guaranteed to infiltrate the target.[109] The attacks are crafted to avoid technical defenses (small email volumes that are "under the radar", zero day exploits and other APT countermeasures).[110] The initial point of vulnerability is the person interacting with a compelling email. Training is not effective in defending at the point of vulnerability – user deception. At that point of vulnerability, providing the user with a countermeasure against the spearphishing attack decreases the likelihood of infiltration by email and increases the chances of interdicting the infiltration. Additionally, by reducing the deceptive power of spearphishing emails, the attacker must send more emails, further increasing the likelihood of discovery. Fewer successful infiltrations will result in fewer alerts for IT to process. Finally, identifying the attack at its earliest stages permits the intended target to mount an effective counterattack.[111]

About the Authors

Robert Zager

Robert Zager is an inventor and entrepreneur. He has been granted eleven United States patents in the areas of computer networking and email. He holds a BA degree from the University of California, Berkeley and a JD degree from Santa Clara University. He is currently a security researcher at Iconix, Inc. in San Jose, California

John Zager

John Zager is a graduate student at Hofstra University, Hempstead, N.Y. where he is studying Industrial and Organizational Psychology with an emphasis on decision-making. He holds a BA degree in psychology from Hofstra University.

The views expressed herein are the views of the authors and do not reflect the views of Iconix, Inc.

References and Notes

[1]Chang, Frederick, Ph.D., "Guest Editor's Column," *The Next Wave*, 2012, Web. 5 May 2014, http://www.nsa.gov/research/tnw/tnw194/article1.shtml
[2] FireEye, *APT28: A Window Into Russia's Cyber Espionage Operations?*, 28 October 2014, Web. 6 November 2014, http://www.fireeye.com/news-events/press-releases/read/fireeye-releases-report-on-cyber-espionage-group-with-possible-ties-to-russian-government
[3] Since late 2002, USG organizations have been targeted with social-engineering online attacks by BC [Byzantine Condor] actors. ... BC actors typically gain initial access with the use of highly targeted socially engineered e-mail messages, which fool recipients into inadvertently compromising their systems [spear-phishing]. The intruders then install malware such as customized keystroke-logging software and command-and-control (C&C) utilities onto the compromised systems and exfiltrate massive amounts of sensitive data from the networks. "A Selection From the Cache of Diplomatic Dispatches," *The New York Times*, Web. 25 July 2012, http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/china-08STATE116943 See paragraphs 32-45.
[4] Mandiant, *APT1*, 18 February 2013, Web. 13 July 2014, http://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/
[5] Sanger, Davie E. and Fackler, Martin, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say, *New York Times*," 18 January 2015, Web. 27 January 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0
[6] Richard Clark, former Presidential cybersecurity and cyberterrorism advisor, Smithsonian Magazine interview. http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/?no-ist=, April 2012, Web. 28 July 2014.
[7] General Keith Alexander, remarks before the American Enterprise Institute, http://link.brightcove.com/services/player/bcpid684720698001?bckey=AQ~~,AAAAnrehDVE~,w91IT6IapG54cV-cir05eT1Zcztug5b0&bctid=1727929528001, 9 July 2012, Web. 28 July 2014.
[8] The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.)
[9] NIST, *Managing Information Security Risk*, Special Publication 800-39, March 2011, Page B-1.
[10] TrendLabs APT Research Team, *Spear-Phishing Email: Most Favored APT Attack Bait*, 2013, Web. 6 February 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
[11] Mandiant website, Web. 10 July 2014, https://www.mandiant.com/threat-landscape/
[12] For a definition of "countermeasures" see Committee on National Security Systems, "National Information Assurance (IA) Glossary, CNSS Instruction No. 4009," 26 April 2010.
[13] Greenert, Johnathon and Welsh, Mark, "Breaking the Kill Chain," *Foreign Policy*, 16 May 2013, Web. 1 May 2014, http://www.foreignpolicy.com/articles/2013/05/16/breaking_the_kill_chain_air_sea_battle.
[14] Hutchins, Eric M.; Cloppert, Michael J.; Amin, Rohna M, Ph.D., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Web. 1 August 2014, http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
[15] Johnson, Steven, *Analysis: False White House tweet exposes instant trading dangers*, 23 April 2013, Web. 23 July 2014, http://www.reuters.com/article/2013/04/23/us-usa-markets-tweet-idUSBRE93M1FD20130423
[16] GReAT, *Red October Diplomatic Cyber Attacks Investigation*, 14 January 2013, Web, 6 July 2014, http://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/
[17] Rear Admiral David Dunaway, *Kill Chains, Star Charts and the NAVAIR Capability Based Analysis Process*, 15 April 2008, Web. 1 July 2014, http://www.dtic.mil/ndia/2008psa_apr/Dunaway.pdf
[18] JP 5-0, *Joint Operation Planning*. 11 August 2011.
[19]Osorno, Marcus; Millar, Thomas; and Rager, Danielle, *Coordinated Incident Management Handling*, 2011, Web. 2 July 2014, http://www.dodccrp.org/events/16th_iccrts_2011/papers/189.pdf.
[20] Verizon, *2013 Data Breach Investigations Report*, 2013, Web. 2 July 2014, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf?r=78
[21] Chinese attackers use email accounts of legitimate services such as Google' Gmail and Microsoft's Hotmail to send attack emails. Mandiant, *APT1*, 18 February 2013, Web. 13 July 2014, http://www.mandiant.com/blog/mandiant-exposes-apt1-chinas-cyber-espionage-units-releases-3000-indicators/, see page 56 of the report.

[22] Iconix website, *Secret*, Web. 13 December 2013, http://sp-guard.iconix.com/index.php/secret/
[23] Ghosh, Anup, *Can You Stop a Targeted Attack?*, *Comment*, 5 July 12, Web. 3 August 2014, https://securosis.com/blog/can-you-stop-a-targeted-attack
[24] Plato, The Republic, Trans. Benjamin Jowett, New York: Vintage Classics, 1991.
[25] https://en.wikiquote.org/wiki/Patton_(film)
[26] See Miller, Matthew, et al. "Why Your Intuition About Cyber Warfare is Probably Wrong." *Small Wars Journal*, 29 November 2012, Web. 8 August 2013, http://smallwarsjournal.com/jrnl/art/why-your-intuition-about-cyber-warfare-is-probably-wrong
[27] *Tools of Engagement - Zero Dark 243 Day*, Mandiant Webinar, Web. 25 April 2014, https://www.brighttalk.com/webcast/7451/107051
[28] Zager, Robert and Zager, John, "Combat Identification in Cyberspace," *Small Wars Journal*, 25 August 2013, Web. 1 August 2014, http://50.56.4.43/jrnl/art/combat-identification-in-cyberspace.

The general susceptibly of interactive computer experiences to deception because the user display is substantially under the control of the creator of the content and the not observer is discussed in Conti, Gregory, Ph.D. and Sobiesk, E.; "Malicious Interfaces and Personalization's Uninviting Future;" *IEEE Security and Privacy*, May/June 2009.

There are circumstances in which technical sending data is displayed to recipients. For example, Gmail displays the name of the sending server. However, because people are unable to decode this technical information, this technical content has little, if any, impact on email interaction decisions. The AntiPhishing Working Group noted, "[T]he domain name itself usually does not matter to phishers, and a domain name of any meaning, or no meaning at all, in any TLD, will usually do. Instead, phishers almost always place brand names in subdomains or subdirectories. This puts the misleading string somewhere in the URL, where potential victims may see it and be fooled. Internet users are rarely knowledgeable enough to be able to pick out the "base" or true domain name being used in a URL." Rasmussen, *Global Phishing Survey: Trends and Domain Name Use in 1H2011*, November 2011, Web. 1 August 2014, http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2011.pdf, page 14.
[29] https://www1.ietf.org/rfc/rfc2822.txt
[30] Tschabitscher, Heinz, *SMTP Inside Out*, Web. 4 August 2014, http://email.about.com/cs/standards/a/smtp.htm

http://www.ietf.org/rfc/rfc4405.txt;

OTA Website, *Email Security & Integrity*, Web. 8 August 2014, https://otalliance.org/resources/email-security
[31] Iconix, *Defending Against Spoofed Domain Spearphishing Attacks*, 1 June 2012, Web. 6 August 2014, http://iconixtruemark.files.wordpress.com/2012/06/defending-against-spoofed-domain-spearphishing-attacks-6-1-12.pdf

Return Path, *The Sender Reputation Report: Key Factors that Impact Email Deliverability*" available by registering at http://www.returnpath.net/landing/reputationfactors/index.php?campid=701000000005fQf

Cisco Systems, *Email Attacks, This Time It's Personal*, June 2011, Web. 3 May 2014, http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf
[32] A fake Facebook profile of a senior NATO commander was used to spearphish U.S. and British military members. Roberts, Paul, *Fake Facebook Profile For NATO Senior Commander Used to Phish Senior Brass*, 12 March 2012, Web. 1 August 2014, https://threatpost.com/fake-facebook-profile-nato-senior-commander-used-phish-senior-brass-031212/76316

Researchers created a non-existent pretty young women and successfully used that persona to spearphish organizations. Constantin, Lucian, "Fake social media ID duped security-aware IT guys," *NetworkWorld*, 31 October 2013, Web. 1 August 2014, http://www.networkworld.com/article/2171398/byod/fake-social-media-id-duped-security-aware-it-guys.html
[33] Fake memos from the head of the Israeli Defenses Forces about missile attacks brought down the Israeli police. Macalintal, Ivan, *Xtreme RAT Targets Israeli Government*, 29 October 2012, Web. 1 August 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/xtreme-rat-targets-israeli-government/

[34] Fake industry conference materials were used to infiltrate aerospace firms. Haq, Thoufique and Gomez, J., *LadyBoyle Comes to Town with a New Exploit*, 12 February 2013, Web. 1 August 2014, http://blog.fireeye.com/research/2013/02/lady-boyle-comes-to-town-with-a-new-exploit.html
[35] Fake HR documents were used to compromise RSA. *Anatomy of An Attack*, 1 April 2011, Web. 1 August 2014, http://blogs.rsa.com/rivner/anatomy-of-an-attack/
[36] Fake military pension documents were used to infiltrate the Indian Army. TCIRT, *Where There is Smoke, There is Fire: South Asian Cyber Espionage Heats Up*, 2 August 2013, Web. 1 August 2014, http://www.threatconnect.com/news/where-there-is-smoke-there-is-fire-south-asian-cyber-espionage-heats-up/
[37] For an overview of the technical means used by attackers to evade technical defenses, see, http://cio.energy.gov/documents/Thursday_Marquis_6_830_Ritchey.pdf
[38] Gonsalves, Antone, "Workers at U.S. nuclear regulator fooled by phishers," *CSO*, 19 August 2014, Web. 3 January 2015, http://www.csoonline.com/article/2466725/physical-security/workers-at-u-s-nuclear-regulator-fooled-by-phishers.html

[39] Microsoft, *Understanding Anti-Malware Technologies*, 2007, Web. 1 August 2014, http://download.microsoft.com/download/A/B/E/ABEFDF1C-96BD-40D6-A138-E320B6B25BD3/UnderstandingAntiMalwareTechnologies.pdf
[40] Danchev, Dancho, *How cybercriminals apply Quality Assurance (QA) to their malware campaigns before launching them*,14 June 2013, Web. 4 August 2014, http://blog.webroot.com/2013/06/14/how-cybercriminals-apply-quality-assurance-qa-to-their-malware-campaigns-before-launching-them/
[41] FBI Director Robert S. Mueller, III, "Remarks, RSA Cyber Security Conference, San Francisco, CA, March 01, 2012".Web. 2 April 2012, http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
[42] FireEye, *FireEye Advance Threat Report – 1H 2012*, 2012, Web. 1 August 2014, http://www2.fireeye.com/get-advanced-threat-report-1h2012.html?x=FE_HERO
[43] Blevins, Brandan, *Despite Pwn2Own 2014 hacks, application sandboxing still critical*, 10 March 2014, Web. 1 August 2014, http://searchsecurity.techtarget.com/news/2240216341/Despite-Pwn2Own-2014-hacks-application-sandboxing-still-critical?asrc=EM_NLS_27359086&utm_medium=EM&utm_source=NLS&utm_campaign=20140319_Sandboxing%20fail?%20All%20four%20browsers%20fall%20at%20Pwn2Own_sshea&track=NL-1820&ad=892512

Hwa, Chong Rong; *Trojan.APT.BaneChant: In-Memory Trojan That Observes for Multiple Mouse Clicks*, 1 April 2014, Web. 1 August 2014, http://www.fireeye.com/blog/technical/malware-research/2013/04/trojan-apt-banechant-in-memory-trojan-that-observes-for-multiple-mouse-clicks.html
[44] Hwa, Chong Rong, *Trojan.APT.BaneChant: In-Memory Trojan That Observes for Multiple Mouse Clicks*, Web. 3 May 2014, http://www.fireeye.com/blog/technical/malware-research/2013/04/trojan-apt-banechant-in-memory-trojan-that-observes-for-multiple-mouse-clicks.html
[45] Elgin Ben; Lawrence, Dune; and Riley, Michael, "Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data," *Business Week*, 21 February 2014, Web. 25 March 2014, http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

[46] By operating at low intensity, the attackers are able to hide in the volume of normal activity to evade detection. For example, in the North Korean attack on Sony Pictures Entertainment, investigators could only determine in retrospect that the attackers had leveraged a spearphishing attack to obtain administrator credentials. The attackers used these credentials to spend months mapping Sony's systems, identifying critical files and planning how to destroy their targets. "They were incredibly careful, and patient." See Sanger, Davie E. and Fackler, Martin, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say, *New York Times*," 18 January 2015, Web 27 January 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0
[47] Verizon, *2014 Data Breach Investigations Report*, 2014, Web. 25 July 2014, http://www.verizonenterprise.com/DBIR/2014/, page 12.

[48] Admiral Leighton W. Smith, USN, comments at the West 2000 conference, *Chaos in Littorals*, February 2000, Web. 15 July 2014, http://www.afcea.org/content/?q=node/752

[49] Acronyms:
ACL: Access Control List
AV: Anti-Virus
"chroot" jail: On Unix-like operating systems "chroot" jail is a security architecture in which a section of filesystem is sectioned off for a particular user. This prevents the user from accessing the root directory.
DEP: Data Execution Prevention
DNS: Domain Name Service
HIDS: Host-based Intrusion Detection System
Honeypot: A trap set to detect or otherwise counteract attempts at unauthorized system usage.
NIDS: Network Intrusion Detection System
NIPS: Network Intrusion Prevention System
Tarpit: A system that delays network connections to slow down network abuses such as spamming and broad scanning.
[50] JP 5-0, p. xxvi.
[51] JP 5-0, p. IV-24.
[52] Bilge, Lyla and Dumitras, Tudor, *Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World*, 16-18 October 2012, Web. 8 July 2014, http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf
[53] *Tools of Engagement - Zero Dark 243 Day*, Mandiant Webinar, Web. 25 April 2014, https://www.brighttalk.com/webcast/7451/107051
2015 Update. Mandiant reports that the detection time in 2014 was205 days. See, Mandiant, *M-Trends 2015*, Web. 9 March 2015. https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html
[54] Verizon, *2013 Data Breach Investigations Report*, 2013, Web. 2 July 2014, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf?r=78
[55] GReAT, *Red October Diplomatic Cyber Attacks Investigation*, 14 January 2013, Web. 6 July 2014, http://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/
[56] Mandiant website, Web. 10 July 2014, https://www.mandiant.com/threat-landscape/
[57] Mandiant website, Web. 29 January 2015, https://www.mandiant.com/threat-landscape/
[58] GReAT, *The "Icefog" APT: A Tale of Cloak and Daggers*, 2013, Web. 7 June 2014, http://www.securelist.com/en/downloads/vlpdfs/icefog.pdf
[59] Mandiant website, Web. 10 July 2014, https://www.mandiant.com/threat-landscape/

An archive of post-infiltration exploits which use native administrative tools can be found at the obsuresecurity website, Web. 14 August 2014, http://obscuresecurity.blogspot.com/p/presentation-slides.html.

See, also, room362.com, Web. 14 August 2014, http://www.room362.com/blog/2014/01/16/application-whitelist-bypass-using-ieexec-dot-exe/;
pentestmonkey.com, Web. 14 August 2014, http://pentestmonkey.net/uncategorized/from-local-admin-to-domain-admin ; and
irongeek.com, Web. 1 August 2014, http://www.irongeek.com/i.php?page=videos/derbycon3/1104-look-ma-no-exploits-the-recon-ng-framework-tim-lanmaster53-tomes
[60] Attackers go so far as to mask their activity by hiding in real user sessions, further obscuring their presence in the system. Blasco, Jaime, *Sykipot variant hijacks DOD and Windows smart cards*, 12 January 2012, Web. 7 August 2014, http://labs.alienvault.com/labs/index.php/2012/when-the-apt-owns-your-smart-cards-and-certs/
[61] TrendLabs APT Research Team, *Spear-Phishing Email: Most Favored APT Attack Bait*, 2013, Web. 6 February 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
[62] Army Field Manual (FM) 5-0, *Army Planning and Orders Production*, p. 3-47
[63] Olzak, Tom, *ASR Objectives*, Web. 25 July 2014, http://resources.infosecinstitute.com/attack-surface-reduction/
[64] JP 5-0, page IV-27.
[65] JP 5-0, page IV-29.
[66] Kean, Thomas; and Hamilton, Lee, "Reflections on the Tenth Anniversary of the 9/11 Commission Report," *Bipartisan Policy Center*, p39, Web. 20 July 2014. http://bipartisanpolicy.org/sites/default/files/files/%20BPC%209-11%20Commission.pdf,
[67] JP 3-13.4, *Military Deception*. 26 January 2012. page GL-4.

[68] Yuill, Jim; Feer, Fred; and Denning Dorothy, *Designing Deception Operations for Computer Network Defense*, *DoD Cyber Crime Conference*, 2005, Web 15 July 2014 http://faculty.nps.edu/dedennin/publications/Designing%20Deception%20Operarations%20for%20CND.pdf
[69] JP 3-13.4, p. IV-2.
[70] JP 3-13.4, Page IV-2.
[71] Operation BOLO, Web. 1 July 2014, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=18113
[72] JP 13-3, page viii.
[73] JP 13-3, page I-4.
[74] JP 13-3, page I-4.
[75] Operation MINCEMEAT deceived Hitler, who deployed troops to the wrong place. BBC, Operation MINCEMEAT, Web. 5 July 2014, http://www.bbc.co.uk/history/topics/operation_mincemeat
[76] Gell, Aaron. "How a White House Flickr Fail Outed Bin Laden Hunter 'CIA John'," *New York Observer*, 12 July 2011, Web. 1 August 2013 http://www.observer.com/2011/07/exclusive-bin-laden-hunter-cia-john-identified/
[77] Acquisti, Alessandro, et al., *Faces of Facebook: Privacy in the Age of Augmented Reality*, Web. 4 December 2013. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/
[78] Higbee, Aaron, "Revealing some of the tactics behind a spear phishing attack," *ITProPortal*, 24 December 2012, Web, 1 August 2013, http://www.itproportal.com/2012/12/24/revealing-some-tactics-behind-spear-phishing-attack/
[79] Lewis, Jason. "How spies used Facebook to steal Nato chief's details," *The Telegraph*, 10 March 2012, Web. 1 August 2013, http://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html
[80] Gilbert, David. "Gone Spearphishing: How Cybercriminals are Changing the Way They Work, "*International Business Times*, 11 July 2012, Web. 1 August 2013, http://www.ibtimes.co.uk/articles/361877/20120711/spear-phishing-antivirus-firewall-cyber-criminals.htm
[81] Vishwanath, Arun "Vish", Ph.D.; and Rao, Raghav, H., Ph.D., University at Buffalo; Herath, Tejaswini, Ph.D., Brock University (Ont., CA); Chen, Rui, Ph.D., Ball State University; and Wang, Jingguo, Ph.D., University of Texas, Arlington, *Why Do People Get Phished? Testing Individual Differences in Phishing Susceptibility Within an Integrated Information-Processing Model*, 22 June 2010, Web. 5 August 2014, http://citation.allacademic.com/meta/p_mla_apa_research_citation/4/0/0/3/5/p400353_index.html
[82] Ferguson, Aaron, Ph.D., United States Military Academy, "Fostering E-mail Security Awareness: The West Point Carronade," *Educause Quarterly*, Number 1 2005, Page 54, Web. 3 August 2014, http://net.educause.edu"/ir/library/pdf/eqm0517.pdf
[83] Jackson, James W.; Fergusson, Aaron J., Ph.D.; and Cobb, Michael J.; United States Military Academy, *Building a University-wide Automated Information Assurance Awareness Exercise*, October 2005, Web. 3 August 2014,. http://fie-conference.org/fie2005/papers/1694.pdf
[84] Dodge, Ronald C., Ph.D.; Carver, Curtis, Ph.D.; Ferguson, Aaron J., Ph.D., United States Military Academy, Phishing for user security awareness, Computers & Security 26 (2007) Page 73, Web. 7 August 2014, http%3A%2F%2Fwww.researchgate.net%2Fpublication%2F222730836_Phishing_for_user_security_awareness%2Ffile%2F3deec5161aaaf78130.pdf&ei=genjU9KbD4XaoASnhIKoAQ&usg=AFQjCNHBB6LUHNG3Rgq21OR8Bw8sQ0cm2A&sig2=v0y7aBNPy9_NCwzk_gXn-g&bvm=bv.72676100,d.cGU
[85] Caputo, Deanne, MITRE; Pleeger, Shari, Dartmouth College; Freeman, Jesse, MITRE and Johnson, M. Eric, Vanderbilt University, *Going Spear Phishing: Exploring Embedded Training and Awareness*, Jan-Feb 2014, Web. 3 August 2014, http://www.computer.org/csdl/mags/sp/2014/01/msp2014010028-abs.html
[86] Vishwanath, Arun "Vish", Ph.D.; and Rao, Raghav, H., Ph.D., University at Buffalo; Herath, Tejaswini, Ph.D., Brock University (Ont., CA); Chen, Rui, Ph.D., Ball State University; and Wang, Jingguo, Ph.D., University of Texas, Arlington, *Why Do People Get Phished? Testing Individual Differences in Phishing Susceptibility Within an Integrated Information-Processing Model*, 22 June 2010, Web. 5 August 2014, http://citation.allacademic.com/meta/p_mla_apa_research_citation/4/0/0/3/5/p400353_index.html
[87] Romenesko, Jim, *AP Warned Staffers Just Before @AP Was Hacked*, 23 April 2013, Web. 1 August 2014, http://jimromenesko.com/2013/04/23/ap-warned-staffers-just-before-ap-was-hacked/
[88] Macalintal, Ivan, *Xtreme RAT Targets Israeli Government*, 29 October 2012, Web. 1 August 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/xtreme-rat-targets-israeli-government/
[89] Raff, Aviv, *Xtreme RAT Strikes Israeli Organizations Again*, 27 January 2014, Web. 12 December 2014, http://www.seculert.com/blog/2014/01/xtreme-rat-strikes-israeli-organizations-again.html
[90] Riley, Charles, "Insurance giant Anthem hit by massive data breach," *CNN Money*, 4 February 2015,Web. 8 March 2015, http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/index.html

[91] Krebs, Brian, "Anthem Breach May have Started in April 2014," *KrebsonSecurity*, 15 February 2015, Web. 8 March 2015, http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/
[92] Richtel, Matt and Kopytoff, Verne G., "E-Mail Fraud Hides Behind Friendly Face," *The New York Times*, 2 June 2011, Web. 1 August 2014, http://www.nytimes.com/2011/06/03/technology/03hack.html?pagewanted=1&_r=2&pag
[93] Conti, Gregory, Ph.D., and Caroland, James; "Embracing the Kobayashi Maru - Why You Should Teach Your Students to Cheat;" *IEEE Security and Privacy*, July/August 2011. The authors discuss the strategic advantage that lying and cheating provide to cyber attackers.
[94] Chabrow, Eric, "Details Emerge of Boeing Hack," *GOVinfoSECURITY*, 13 July 2014, Web. 13 July 2014, http://www.govinfosecurity.com/details-emerge-boeing-hack-a-7053/op-1
[95] *United States of America v. Su Bin Criminal Complaint*, Web. 1 July 2014, https://www.documentcloud.org/documents/1216505-su-bin-u-s-district-court-complaint-june-27-2014.html
[96]According to Mandiant, 64% of breaches are discovered by third parties. https://www.mandiant.com/threat-landscape/, Web. 10 July 10 2014. For cyberespionage, Verizon reports that 85% are discovered by third parties. Verizon, *2014 Data Breach Investigations Report*, 2014, Web. 25 July 2014, http://www.verizonenterprise.com/DBIR/2014/
[97] Verizon, *2014 Data Breach Investigations Report*, 2014, Web. 25 July 25 2014, http://www.verizonenterprise.com/DBIR/2014/, page 12.
[98] The current attack-respond cycle favors the attackers. See, for example, Perlroth, Nichole, "Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt," The New York Times, Web 5 January 2013, http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?_r=1&
[99] The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.)
[100] Turning the deception message into a counterattack builds upon the cyber defense concepts advanced by James Yuill. See Yuill, James, "Defensive Computer-Security Deception Operations: Processes, Principles and Techniques." *Ph.D. Thesis, North Carolina State University*, 2006, Web 10 July 2014, http://repository.lib.ncsu.edu/ir/bitstream/1840.16/5648/1/etd.pdf
[101] *Tools of Engagement - Zero Dark 243 Day*, Mandiant Webinar, Web. 25 April 2014, https://www.brighttalk.com/webcast/7451/107051
[102] JP 5-0, p. IV-24.
[103] FM 5.0, Page 3-56.
[104] In theory, restricting users' privileges limits what an attacker can do with stolen credentials, making it harder for attackers to accomplish objectives and easier to find unauthorized activity. Attackers use anti-forensic methods to hide unauthorized activity. Moreover, restricting users' privileges can have the perverse effect of reducing security because, as IT makes it harder for users to do their work, users circumvent the enterprise's security and compliance infrastructure with unauthorized "Shadow IT." 81% of line-of-business workers and 83% of IT staff admit to using non-approved SaaS resources. See Frost & Sullivan, *The Hidden Truth Behind Shadow IT*, November 2013, Web. 18 July 2014, http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf
[105] Committee on National Security Systems, "National Information Assurance (IA) Glossary, CNSS Instruction No. 4009," 26 April 2010.
[106] Vishwanath, Arun "Vish", Ph.D.; and Rao, Raghav, H., Ph.D., University at Buffalo; Herath, Tejaswini, Ph.D., Brock University (Ont., CA); Chen, Rui, Ph.D., Ball State University; and Wang, Jingguo, Ph.D., University of Texas, Arlington, *Why Do People Get Phished? Testing Individual Differences in Phishing Susceptibility Within an Integrated Information-Processing Model*, 22 June 2010, Web. 5 August 2014, http://citation.allacademic.com/meta/p_mla_apa_research_citation/4/0/0/3/5/p400353_index.html
[107] These innovations are covered by one or more of the following patents held by Iconix: U.S. Patents 7,413,085; 7,422,115; 7,457,955; 7,487,213; 7,801,961; 8,073,910; 8,621,217; 8,903,742
[108] See Hesser, Robert and Rieken, Danny. "FORCEnet ENGAGEMENT PACKS: "OPERATIONALIZING" FORCEnet TO DELIVER TOMORROW'S NAVAL NETWORK-CENTRIC COMBAT REACH, CAPABILITIES . . . TODAY," *Naval Postgraduate School*, December 2003, Web. 19 June 2013 http://www.dtic.mil/dtic/tr/fulltext/u2/a420550.pdf for a comprehensive discussion of central role of combat identification in modern kinetic warfare.
[109] Dave, Paresh, "Who's susceptible to email phishing attacks? Study says everyone," *Los Angeles Times*, 26 July 2013, Web 4 August 2014, http://www.latimes.com/business/technology/la-fi-tn-whos-most-susceptible-to-phishing-attacks-20130726-story.html

[110] See, for example, Cisco Systems, *Email Attacks, This Time It's Personal*, June 2011, Web. 3 May 2014, http://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/targeted_attacks.pdf

[111] Much like small raiding parties which operate from a common secret base of operations, APT attackers employ unique elements in the attacks (e.g., malware, domains, messaging) which often use a common obscured infrastructure from which multiple apparently independent attacks can be mounted. By obscuring these infrastructures, attackers use attack infrastructures for long periods of time. Examples of infrastructures that remained undetected for years:

A cyber attack infrastructure that went undiscovered for more than 5 years. GReAT, *Red October Diplomatic Cyber Attacks Investigation*, 14 January 2013, Web, 6 July 2014, http://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/

A cyber attack infrastructure that went undiscovered for approximately 3 years, Mandiant website, Web. 10 July 2014, https://www.mandiant.com/threat-landscape/ GReAT, *The "Icefog" APT: A Tale of Cloak and Daggers*, 2013, Web. 7 June 2014, http://www.securelist.com/en/downloads/vlpdfs/icefog.pdf

A cyber attack infrastructure used by attackers in India for at least 3 years was discovered in Norway. https://www.bluecoat.com/company/press-releases/norman-shark-cyber-research-report-uncovers-first-large-cyber-espionage, Web. 10 August 2014.

Although attackers cannot be stopped from creating new attack infrastructures (See, for example, the deployment of a new attack infrastructure after the publication of Mandiant's *APT1* report,Danger, David and Perlroth, Nicole, "Hackers From China Resume Attacks on U.S. Targets," *The New York Times*, 19 May 2013, Web. 31 July 2014, http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html?pagewanted=1&_r=1&hp), forcing attackers to abandon infrastructures and create new ones introduces delays into attacks and increases the cost of operation for APT attackers.