The Role of Dynamic Deception in the Cyber Kill Chain

The Best Offense is the Best Defense

We have all seen the headlines covering the mega-breaches of retailers (Target, Home Depot, eBay), vendors (Microsoft and Yahoo), banks (JP Morgan, Chase), and even newswires. Today's threat landscape requires organizations to operate based on the assumption that cyber attacks are inevitable—82% of organizations worldwide expect to be attacked in 2015.[1] Knowing they are coming (or already in their network), organizations are focused on trying to quickly identify and minimize the impact of an attack on their organization.

Ponemon Institute estimates that these advanced attacks cost organizations between $250,000 to $5 million, including the cost of technical support, business disruptions, lost productivity, as well as diminished brand and reputation.[2] This helps explain why information technology (IT) spending is on the rise—Gartner predicts it will reach $76.9 billion in 2015[3] and by 2017 strategies of lean forward organizations will routinely include the mapping of their security architecture and/or their processes to the kill chain life cycle.[4]

Despite the increases in awareness and resources, organizations still feel unprepared to defend themselves against the cyberattacks they are facing. This paper examines the challenges of today's threat landscape and the opportunities to address holes in the cyber kill chain (attack lifecycle). It identifies how the adoption of active decoy and deception technologies can help organizations better prepare and protect themselves against advanced, targeted attacks.

Today's Security Landscape Leaves Open Doors Throughout the Kill Chain

Today's cyber security paradigm centers on perimeter security technologies that are designed to prevent attacks and are optimized to try to prevent attackers with known attack patterns from entering the network. The goal is to find and neutralize known attack patterns and suspicious behaviors, such as viruses, malicious URLs, unknown command and control traffic, Denial of Service (DoS) / Distributed DoS (DDoS) attacks, etc., before they can get inside.

The problem is motivated attackers will always find a way into the network. Once inside, they will disguise their activities over a period by hiding in seemingly "normal" internal traffic. As a result, most attacks don't look like attacks, in the traditional sense. It's only when you put together, in context, all the events that make up the attack that you can see the malicious intent of the activity.

Over time, monitoring detection systems deployed in the network may pick up and alert to an aspect of the attack. Unfortunately, due to the high volume of individual alerts and typical time delays to establish the linkage between the activities, alerts may appear harmless and often go uninvestigated until after a breach has occurred.

When a security analyst is facing tens, hundreds, even thousands of alerts every day/week, how do they decide where to spend their time? Typically they will prioritize, which means many of the alerts they receive go unhandled, as the security team focuses on the ones that seem to pose the greatest risk and warrant escalation. In the meantime, an attacker can be traversing the organization's network unimpeded to accomplish their objective.

In practical terms, it appears the security mechanisms these organizations have in place are failing, because they aren't preventing the attacks; but the reality is most have done exactly what they were supposed to do – identifying and alerting on suspicious activity. The ever-increasing number of highly advanced attacks that don't follow known signatures dramatically compounds the problem, and the lack of integration for threat intelligence ill prepares organizations with the tools to understand definitively the relevance of each alert. Without the context, it becomes unclear as to exactly what is happening in their environment, which means they can't proactively identify and stop an attack.

Cyber Kill Chain: The Phases of an Attack Lifecycle

There are multiple phases of an attack that each present opportunities for an organization to detect and prevent an intrusion from being successful. However, most of the security infrastructure is focused on trying to stop the initial infection, which means the attacks that get past the organization's defensive measures often go undeterred in the network for days, even months. According to Mandiant's 2014 Threat Report, the median number of days attackers are present on a victim's network before they are discovered is 229. [5]

This means there is a real opportunity to strengthen an organization's security by focusing more efforts on identifying and shutting down the attack's activities that are occurring in the network. Let's look at the opportunities and challenges within each phase of the attack's lifecycle:

Phase 1: Infection

This phase includes the attacker's initial reconnaissance, weaponization, delivery, and successful exploitation and installation; the goal is to establish a foothold in the organization. There are a host of solutions, such as firewalls, intrusion detection/prevention systems, anti-virus solutions, sandboxes, remote access authentication mechanisms, etc., designed to detect the attack before it can get into the network, however, attackers only need one device (one person) to fall victim to their exploit to be successful. This phase typically consists of:

- **Reconnaissance**—Attackers research their target organizations, looking for potential victims they can use to get inside; it could be an employee, customer, vendor, partner, etc. that supplies the entry they need.
- **Weaponization**—Once a target is determined, the attacker will create an exploit they feel gives them the best chance of success. The more sophisticated attackers will create zero-day exploits (a.k.a. zero-hour or 0-day vulnerabilities) that use undisclosed or uncorrected vulnerabilities to infect devices/systems, applications, or data. They will then determine how they want to deliver these attacks to their intended victims.
- **Delivery**—Attackers will attempt to bypass the security infrastructure in place to deliver their exploit. They may leverage:
  - *Web Services*—taking advantage of the vast, dynamic world wide web to disguise their intentions; attackers try to convince users to go to malicious websites or click on malicious links they have embedded within "legitimate" websites to infect the victim.
  - *Spear phishing*—sending emails from a seemingly familiar and reliable source to trick users into unwittingly downloading malware or providing confidential information (credentials, etc.) that can be used to get "insider" access.
  - *Stolen credentials*—counting on the complexity of geographically dispersed and varied user populations to hide compromised credentials; attackers will use stolen credentials of employees, contractors, 3rd-party vendors, etc. to get into the network.
  - *Endpoint and personal (BYOD) devices*—compromising devices that are out of the direct control of the organization can give attackers an entry point to penetrate the network.
  - **Physical Access**—breaking into the offices of organizations gives attackers access to assets connected to the network.
- **Exploitation/Installation**—Attackers, will then execute the exploit to download the malicious payload, infect the victim device with malware, etc. This compromised system gives the attacker a persistent presence in the network, which they can use to launch other attack activities to accomplish their objective.

Phase 2: Attack Activities

Once the attacker is in and make no mistake about it, a motivated attacker will find a way in, they can then focus on accomplishing what they really came to do—access, contaminate, or steal valuable data, disrupt operations, etc. This phase is all about accomplishing the attack objectives while hiding attack activities in seemingly normal "legitimate" traffic to stay undiscovered for as long as possible. If organizations can accelerate their ability to uncover these attack activities, they can significantly reduce, if not eliminate, the impact of the attack. During this phase, attackers typically conduct:

- **Reconnaissance**—Attackers attempt to learn about the internal network to understand where the valuable assets and resources are located. They will leverage host and port scans to try to identify the network's topography and get an inventory of what is in the network (devices, servers, operating systems, etc.), so they know what they want to target. Attackers can also sniff and capture network broadcast and multicast traffic on compromised machines to learn about devices on the network.
- **Lateral Movement**—Attackers will take what they have learned and use it to move around the network, accessing other systems and data of interest to them. Attackers will often use credentials they have stolen (or elevated to administrative status) from the devices/users they have compromised to spread unnoticed throughout the network.
- **Exfiltration**—At some point, attackers will create a command and control (C&C) channel to access remotely and operate the internal assets they have compromised and move data out of the network. The C&C channel will operate throughout the attack. Organizations may use reputation services and threat intelligence feeds that contain "black lists" of known C&C servers used by attackers, so sophisticated attackers will create new domains or use common Internet services to evade detection and hide their C&C messages.

Phase 3: Incident Response, Post-Attack Analysis, and Forensics

When a system, action, or component of an attack is discovered or blocked, the attacker will typically attempt to return to a compromised machine that has not been identified to try to continue to operate and maintain persistence in the network. This is why, as soon as something suspicious is identified, it is critical the activity is investigated and linked to all the other relevant activities, so the full extent of the attack can be understood and remediated.

- **Incident Response**—As soon as an attack is identified (via an alert from one of the systems that makes up the security infrastructure) organizations need to investigate, contain, and remediate it. To stop the attack from propagating and doing any (further) damage, organizations will be required to manage the event in real-time, making quick decisions and taking immediate actions to shut it down. To minimize the gap between detection and mitigation, organizations need the information and context that ties all the attack activities together, so they can ensure they are mitigating the full extent of the breach (with no "sleeper" persistent attack presence left behind).
- **Forensics**—Once remediated, organizations will typically try to quantify the damage of an attack via a forensics investigation. The goal is to understand the mechanisms of the attack to help improve the organization's defenses against similar, future attacks; in some cases, the forensics investigation provides the evidentiary support for potential legal action against the attackers.

Active Decoy and Deception Can Accelerate Detection of Attack Activities

Organizations need to augment their defensive strategy, which is focused on trying to identify attacks as they enter the network, with more offensive measures that can lure attackers into quickly revealing themselves when they conduct their attack activities to prevent the attack's damage and its propagation throughout the network.

To assume this offensive posture, organizations are using active deception systems for real-time post-infection breach detection. These systems enable organizations to proactively uncover attackers as they conduct:

- **Reconnaissance**—With real operating systems, full network services, protocols, and data elements, deception-and-decoy systems lure attackers into revealing themselves as soon as they start looking at network services, virtual machines, IP services, and subnets for high-value data assets. Authentic deception and decoy technology can catch zero-day attacks (without having to rely on signatures or database lookups) and effectively entice attackers away from real assets.
- **Lateral Movement**—With the ability to detect threats in east-west traffic, active deception systems can accurately identify the infected clients being used by attackers to propagate, including sleeper and time-triggered agents. They also capture the tactics these attacks are using to help organizations understand the overall objective/intent of the attack.

  As a result, these systems significantly reduce detection time, providing the context organizations need for full remediation of an attack before it can cause damage. To avoid the need for heavy compute power and to handle the scale of large data centers, systems that do not inline or do deep packet inspection are highly recommended.
- **Exfiltration**—With the ability to gather information about the attack's payload, its activities and the C&C machines to which it's attempting to communicate, in a safe, contained environment, these systems detect advanced attacks in a low-friction manner, enabling them to play out in a simulated environment and preventing the data from ever leaving the network.

In addition to uncovering attacks on the network to improve an organization's overall security stance and better protect their assets and resources, active deception systems support the post-detection phases of the attack's lifecycle:

- **Incident Response**—Accurate alerts ensure incident response teams don't waste time or resources investigating false positive alerts. These systems provide actionable information, identifying the infected systems, time, type and anatomy of the attack; threat intelligence dashboards and Indicators of Compromise (IOC) reports offer detailed attack information to prevention systems, through UI, PCAP files, Syslog, IOC, and CSV report formats, so the attack can be quickly contained and remediated.
- **Forensics**—A catalog of all attack activity (attempted communications and propagation activity) makes it easy for the organization to understand an attack's anatomy and objectives to support ongoing analysis and forensics activities.

Attivo Networks®: Dynamic Deception for Proactive Defense Against Inside the Network Attacks

Attivo Networks active threat detection solutions detect advanced threats as they propagate throughout the organization's network and data center. Designed to augment existing security systems, the Attivo ThreatDefend™ Deception and Response Platform uses deception techniques to deceive, detect, and defend against attacks as they begin scanning, targeting, and probing network clients, servers, and services for targets.

Based on active decoys and dynamic deception technology, ThreatDefend solutions engage with attackers in real-time, immediately notifying prevention systems and stopping attackers in their tracks. The ThreatDefend platform runs real operating systems, full services, and applications, along with the ability to completely customize the environment by importing the organization's golden images and applications. As a result, Attivo provides an authentic environment that is baited with lures and traps while being indistinguishable from company servers. Additionally, the ThreatDefend solution only generates accurate, actionable alerts based on the solution's actual engagement with the attack to greatly reduce the time it takes to detect and shut an attack down, before it can damage the organization. The alerts include valuable details, such as:

- IP addresses of infected machines
- Username and password combinations
- Any dropped payloads including location and type of attacks
- Attack activity, including any data it's targeted for download or export
- Any system/kernel changes, process creation, process injection, registry and network activity

The BOTsinks's Analyze, Monitor and Record (AMR) Engine feeds events to Attivo's patented Multi-Dimensional Correlation Engine to generate attack sequences that provide organizations with an accurate catalog of all the attack's activity. The BOTsink solution also provides IOC reports to update prevention systems in various reporting formats and a threat intelligence dashboard with the forensics required to capture attacker method and intent, update prevention systems, and prevent future attacks.

Simple Deployment

The ThreatDefend Deception Platform is designed for networks, datacenters, and cloud environments. Available as appliances and virtual machines, BOTsink is designed for rapid deployment to defeat the attacks already propagating inside the network. It uses IPs from the dark/unused space to insert itself into the network, without using any computing overhead. Since they are not inlined and do not need to redirect traffic, Attivo is highly efficient and scalable.

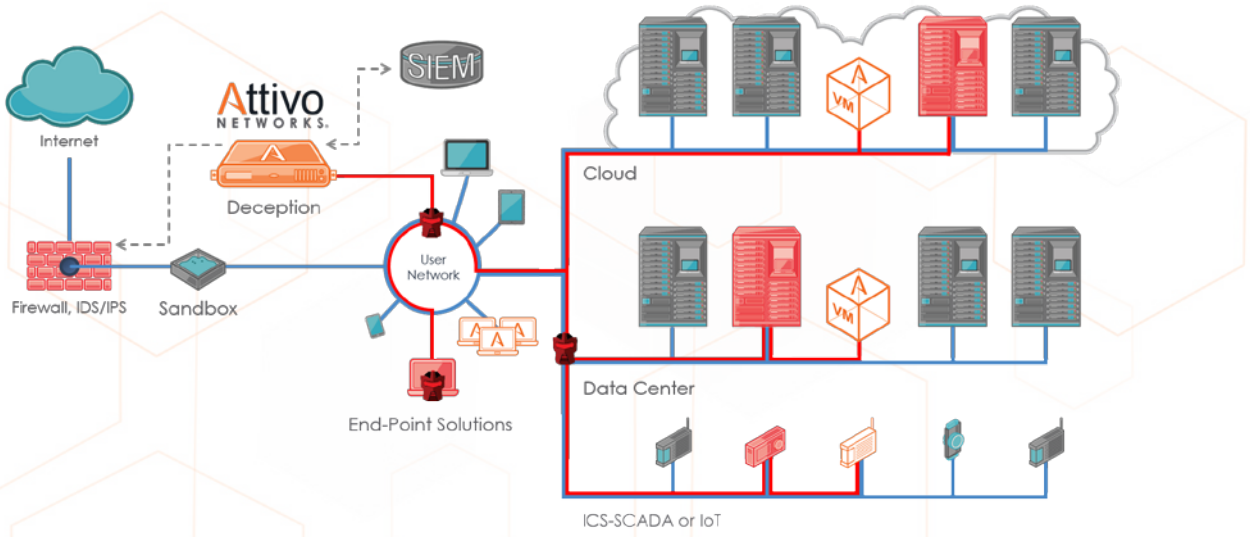
Attivo can turn every node and subnet into a trap that can lure attackers into engaging and revealing themselves, so organizations can quickly identify and understand the attacker's intent for full, prompt remediation. No data or information ever leaves the organization's premises for external (cloud) computation. Leveraging high interaction deception, Attivo provides the next layer of defense for protecting critical assets from attacks already in the network.

Conclusion

Cyberattacks are inevitable; organizations need to add capabilities that enable them to quickly identify and effectively stop the attackers that have bypassed perimeter security and were on the network. Active deception technologies help organizations create a more proactive security stance through the kill chain, one that can get attackers to reveal their activities and intent, so the full extent of the breach can be remediated.

The Attivo ThreatDefend Deception and Response Platform delivers a highly-interactive, distributed decoy system that lures the attackers into engaging with it and then traps their activities to prevent communications and stop the propagation and exfiltration of data. Once an attack is underway and engaging with the ThreatDefend platform, Attivo can provide in-depth visibility on all the attack's activities to support swift containment and remediation, as well as ongoing forensics.

Attivo can identify the breach and all infected endpoints, including sleeper agents or time triggered hosts. A port from the sinkhole can be opened to connect to the hacker's command-and-control server (C&C) to collect additional information about the intent of their attack. With the Attivo ThreatDefend solutions, organizations finally have the ability to engage proactively attackers to identify and shut them down, so they can prevent the damage of the attacks already on their network.



About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com

Sources:

1. See Information Systems Audit & Control Association (ISACA) and RSA Confrence, "State of Cybersecurity: Implications for 2015," http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/Study-82-percent-of-Organizations-Expect-a-Cyberattack-Yet-35-percent-Are-Unable-to-Fill-Open-Security-Jobs.aspx.
2. See Ponemon Institute LLC, "The Economic Impact of Advanced Persistent Threats," May 2014.
3. See Gartner, http://www.securityweek.com/global-cybersecurity-spending-reach-769-billion-2015-gartner.
4. See Gartner, Addressing the Cyber Kill Chain Aug 15, 2014 Research note by Analyst Craig Lawson
5. See "2014 Threat Report: MTrends – Beyond the Breach," Mandiant, April 2014, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf.