LIGHTCYBER
Stopping Targeted Threats

THE CHANGING FACE OF TARGETED THREATS

MEETING NEW CHALLENGES WITH A NEW TARGETED THREAT PROTECTION PARADIGM

FEBRUARY 2013

LIGHTCYBER
Stopping Targeted Threats

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The recent wave of targeted attacks carried out against RSA, Lockheed Martin, Saudi Aramco, the New York Times, and others represent a quantum leap in attack sophistication and severity of damages. Carefully planned and executed over time, these attacks resulted in billions of dollars in damages, and are spurring security organizations to reexamine some basic network security paradigms.

Targeted attacks are today more effective, and more cost effective. These attacks don't focus on network intrusion, but on the long process of getting to specific information and getting it out of the network. Entering the network has become "merely" a means to an end, and the targeted attacker is not limited by time or resources. Once the attacker has breached the perimeter, achieving the actual goals of the attack can take months to years. *It is at this phase that the attacker is most vulnerable to discovery if the security monitoring systems can differentiate between malicious behavior and normal network behavior – and this is exactly where existing security paradigms fall short***.**

Today, organizations try to bridge the detection gap in the internal network by using big-data analytics, aggregating internal events and network traffic data to help human analysts look for specific patterns that might indicate an ongoing attack, or perform forensics after an attack is discovered.

However, due to inherent limitations in human analysis, existing solutions flood Security Operation Centers with inactionable information. Incident response teams spend most of their time *looking for hints of malicious behavior*, rather than receiving actionable malicious activity intelligence and actively mitigating risk.

To transition security operations teams from reactive to predictive and proactive, a paradigm shift is required. In order to effectively detect targeted attackers, an automated method is needed to identify malicious behavior within the mass of day-to-day network traffic.

To accomplish this, it is crucial to first understand with high granularity how the organization works, and what is considered "normal" behavior *for each individual user and computer in the network.* Leveraging this mass of detailed knowledge, detection of subtle anomalies in the network can identify an attacker at an early phase of the attack, long before real damage has been done.

Light Cyber's MAGNA™, the next generation of targeted threat protection, puts this new paradigm into practice by seamlessly profiling normal behavior of all network users and endpoints enterprise-wide, automatically detecting malicious behavior inside the organizational network at the early stages of an attack, and using Targeted Forensics™ to provide incident response teams with the information they need to quickly understand the nature and severity of the threat.

THE CHANGING FACE OF TARGETED THREATS

Cyber attacks have become more prevalent, gaining media attention and spawning a new generation of tools and solutions to protect online assets. The threat of malware, botnets and other easily-accessible attack methods is of grave concern to both businesses and governments worldwide.

While these "mass market" cyber threats are substantial, it is the threat of targeted and persistent attacks that is spurring governments and enterprises around the world to reexamine some basic network security paradigms.

The targeted attacks carried out recently against RSA, Lockheed Martin, Saudi Aramco, the New York Times, and others represent a quantum leap in both attack sophistication and severity of damages. These attacks were carefully planned and executed over a course of weeks, months or years, and resulted in billions of dollars in damages.

Most notable in the recent spate of targeted attacks is the fact that they were only discovered long after the damage was done. It is clear that enterprises and governments are facing a new level of threat, one that is not fully or effectively addressed by existing security paradigms.

WHAT EXACTLY HAS CHANGED?

Multiple factors are fueling the recent exponential growth in the number and effectiveness of targeted attacks, notably:

Cyber-Attacks Are Cost-Effective

Targeted attacks are today more effective, and more cost effective. Today's targeted attackers are motivated by either financial or ideological gain (hacktivism). As evidenced by recent events, both types of targeted attacks have been wildly successful. Moreover, the cost associated with these attacks, and the possible risks to attack initiators, is still comparatively low.

The proliferation of black market trade in "zero-day" malware and exploits - at costs ranging between thousands and hundreds of thousands of dollars – is another key advantage for the targeted attacker seeking to exploit unknown vulnerabilities and penetrate organizational defenses. Today, there are more exploits available for sale, costs are in decline, and demand is on the rise.

Breaching the Perimeter – Just a Means to an End

The most significant difference between traditional threats and targeted threats is not technical. New vulnerabilities have been discovered and exploited for years, and today's advanced attacks seek to exploit the same kind of vulnerabilities.

What has changed is the concept of the "attack" itself.

We are used to malware that is an IT menace, flooding the network with traffic, deleting files on computers, and resulting mostly in annoyance. Most generic malware has one main goal – to spread and infect as many computers as possible.

Targeted attacks don't focus on network intrusion, but on the long process of accessing specific information and getting it out of the network. *Entering the network has become "merely" a means to an end*.

Moreover, the targeted attacker is not limited by time or resources, and can afford to keep looking for a hole in organizational perimeter defenses until one is found. Attackers can even purchase the specific perimeter or endpoint security products in use by the targeted organization, in an attempt to find a way around them.

The security community agrees that there is no way to prevent 100% of intrusions. It is clear that the persistent attacker will sooner or later (likely sooner) penetrate the perimeter – *a guaranteed 100% success rate*.

However, once the attacker has breached the perimeter, achieving the actual goals of the attack can take months to years. During this phase of the attack, the attacker performs various operations to learn and propagate access inside the network. Controlled by a human attacker, this malicious network behavior looks similar to normal network traffic. *It is at this phase that the attacker is most vulnerable to discovery if the security monitoring systems can differentiate between malicious behavior and normal network behavior – and this is exactly where existing security paradigms fall short*.

WHY EXISTING PARADIGMS CAN'T COPE

Existing security paradigms attempt to stop threats at the perimeter and endpoint, or to detect them inside the network leveraging big-data analytics. However, neither of these methods have proven effective:

PERIMETER AND ENDPOINT – TOO LITTLE

As discussed above, when dealing with targeted attacks, the security assumption should be that the perimeter *has already been breached*. And, once the attacker is past the perimeter, most security solutions are ineffective, as they are not designed to detect an attacker after a breach. Endpoint security solutions are only effective for detecting known threats, and it is easy for an attacker to escape detection by creating unknown variants of malware.

For the above reasons, most breaches are discovered months or years after the incident, long after the damage has been done.

BIG DATA – TOO MUCH, TOO LATE

Today, organizations try to bridge the detection gap in the internal network with big data analytics. Big data technologies aggregate internal events (SIEM solutions) and network traffic data (forensics/visibility solutions), helping human analysts either look for specific patterns that could indicate an ongoing attack, or perform forensics after an attack is discovered.

The problem is that a human analyst can define rules only for *known* attacks and methods, not describe what the next *unknown* attack will look like. In addition, a human analyst simply cannot define unique rules for each user and each computer in an enterprise-size network with tens or hundreds of thousands of users.

Performing forensics after an attack is discovered can enable incident responders to see, for example, everything that an infected computer did in the previous days. However, forensics are by definition *after the fact* – and not effective in actually discovering the attack.

Existing solutions flood Security Operation Centers with inactionable information. Incident response teams spend too much time looking for hints of malicious behavior, rather than receiving actionable intelligence and actively mitigating risk.

To transition security operations teams from reactive to predictive and proactive, a paradigm shift is required.

MEETING THE TARGETED THREAT CHALLENGE

In order to effectively detect targeted attackers, an automated method is needed to identify malicious behavior within the massive volumes of network traffic.

To accomplish this, it is crucial to know how the organization works, and what is considered "normal" behavior *for each individual user and computer in the network*. Only then can we effectively identify malicious network activities – the "abnormal" activities an attacker must ultimately perform to achieve his or her goals in the window of time between perimeter penetration and attack fruition.

UNDERSTANDING NORMAL NETWORK BEHAVIOR

The best way to understand "normal" network and user behavior is to analyze the unique patterns of internal network traffic for each user and computer in the organization.

Activities that are common in one organization will be rare in another one, and even different users in the same organization have very different behaviors. For example, an employee in the finance division and a software developer will have very different network usage profiles, as they use different applications and servers.

Effective learning and tracking of normal behavior for each user and computer in the network is a key enabler for sensitive detection of malicious activities.

EARLY THREAT DETECTION

Detection of subtle anomalies in the network can be used to find the attacker at an early phase of the attack, long before real damage has been done. At this early stage, the attacker is busy "figuring things out" in the network, and thus tends to perform anomalous activities that don't synch with normal user or computer behavior.

By discovering this anomalous activity early, security personnel can drill down, focusing forensics efforts and checking exact activities to facilitate quick investigation and remediation.

This is particularly important in light of the significant manpower expenses associated with forensics resources. The network has an infinite amount of parameters that can be examined. The more focused forensics are on likely threats, the more effective analyst time can be used to identify and block actual attacks.

MAGNA™ - THE NEXT GENERATION OF TARGETED THREAT PROTECTION

Light Cyber's MAGNA™ appliance, the next generation of targeted threat protection, puts this new paradigm into practice with a three-step methodology:

PROFILE MAGNA seamlessly profiles normal behavior of all network users and endpoints enterprise-wide, passively analyzing network traffic with zero configuration and without rules or signatures.

DETECT MAGNA automatically detects malicious behavior inside the organizational network at the early stages of an attack, and alerts the SOC team of malicious behavior. Due to the solution's detailed profiling of normal behavior, detection is sensitive enough to spot low and slow attacks with a very low false positive rate.

INVESTIGATE MAGNA uses Targeted Forensics™ at the network and host level to provide the incident response team with the information they need to quickly understand the nature and severity of the threat and effectively investigate and remediate the attack.

ABOUT LIGHT CYBER

Light Cyber™ is a leading provider of Advanced Threat Protection solutions that enable organizations to detect targeted threats and cyber-attacks inside the network at an early stage, before real damage is done.

Light Cyber helps the security operations team to focus on imminent and serious threats that have penetrated network perimeter and endpoint defenses. Founded in 2011 by leading cyber security experts, Light Cyber serves customers in industries from finance and telecom services to media and technology.