FLOWTRAQ®

WHITE PAPER

TODAY'S SECURITY THREATS AND HOW TO COMBAT THEM

INTRODUCTION

These days, hardly a month goes by when there isn't some news of a cyber attack on a huge global organization that at one time seemed impenetrable. As perpetrators become more sophisticated, they are finding new ways to break down protective barriers, launch attacks, steal data and company secrets, and essentially wreak havoc on organizations around the world.

This white paper will not only detail the different types of security threats organizations face today, but it will also help you understand how network behavior intelligence can work in conjunction with other tools to combat them. It will cover:

1. The three classes of attacks — availability, confidentiality and integrity
2. The impetus for attacks — why attackers target certain organizations
3. The different types of attacks — from DDoS to data leakage
4. How to defend against attacks — from firewalls to network visibility tools

Organizations need to understand the reasoning and strategy behind an attack, and how and where they are vulnerable. Only then can they effectively protect themselves.

CLASSES OF ATTACKS

The cybercrime landscape is not only vast, it's constantly evolving. Looking at the landscape overall, there are three major areas of attack — availability, confidentiality and integrity. Sometimes organizations are vulnerable to all three kinds of attacks, sometimes, just one or two. Regardless, it's important to understand the different types of threats.

1. Availability

This class of attack focuses on making an organization's service unavailable for a period of time. The more significant the attack, the longer the downtime. For instance, perpetrators might target an online retailer to bring its website down on Black Friday, or a bank so it can't dispense money to its customers, or a post office so it's unable to sell stamps or perform transactions. While almost every organization is dependent on the Internet in some way, those with a heavy Web services component or that rely on internal network services are the most vulnerable. DDoS attacks tend to be the most common threat when it comes to availability attacks.

2. Confidentiality Attack

These types of attacks can be very damaging because they are all about stealing confidential information — customer credit card numbers, company secrets, sensitive data — that organizations protect for a reason. Espionage and data breaches are the result of confidentiality attacks because they are focused on stealing private information. Even organizations like the NSA, Staples, the U.S. Postal Service, Morgan Stanley and Sony have been victims of these types of attacks. Social engineering, malicious insiders, compromised credentials and other vectors are the "weapons" that are often used in confidentiality attacks.

3. Integrity Attack

Integrity attacks focus on tarnishing an organization's reputation by modifying data that publicly humiliates them. The idea is to rewrite existing copy about an organization so it can no longer be trusted. News organizations are particularly vulnerable to integrity attacks because their business depends on honest reporting. Similarly, government organizations such as the Centers for Disease Control are susceptible as well since a perpetrator might want to cause panic by creating false information about a deadly disease, for example. Any organization's integrity can be compromised using social engineering, malware or website defacement where the trust in an organization is damaged because it becomes unclear which information can still be trusted, and which cannot.

IMPETUS FOR AN ATTACK

In order to defend yourself from a network attack, you first need to understand what assets you have, what your vulnerabilities are, and why someone might attack you.

Your assets

What do you own that others want to get their hands on? Customer data? Product formulas? Security codes? Intellectual property? Company secrets? Trusted access to third-party resources? You need to take a hard look at what you own that someone else may want, and protect it as if it's in Fort Knox.

Your vulnerabilities

Attackers always look for a weakness they can exploit. If you're an online retailer like Amazon.com or Zappos.com, and you can't do business without your website, you are most vulnerable to an availability attack. If you are an intelligence agency, government contractor or financial institution with top-secret information, you're most susceptible to a confidentiality attack. If you're a news or government organization with high credibility, you're most vulnerable to an integrity attack.

Assess your organization's situation and determine what your most desirable assets are and where your vulnerabilities lie. Understanding this is your first step toward a strong defense.

Why attacks happen

Once you've figured out what's at risk, you need to determine why an attacker would target your organization. This can be looked at three different ways: means, motive and opportunity.

1. Means

You are at risk of attack if someone has the means. Maybe they've swiped a key access card, or hacked into your network, or developed a network of botnets (aka zombies) because they have access to thousands of computers and technology. Essentially, if people have the means to access what they want and the malicious intent, they will find the opportunity to either steal it or destroy it.

2. Motive

In any crime, there is always a motive. In the case of cybercrimes, the motive is usually one of the following that can be remembered with the acronym MICE — monetary gain, ideology, coercion, or ego. You can narrow down what type of perpetrator you're looking at based on motive.

Monetary gain

When someone is being paid to launch an attack, demands a ransom while he or she holds a company's assets hostage, steals information that translates into monetary profit (e.g., credit card theft), or stands to make money off of some other organization's downfall, money is the motive.

Ideology

Attacks are sometimes ideologically based. Someone or some group is angry at an organization for political, religious, environmental, social, competitive or other reasons and wants it to suffer the consequences. They might disagree with specific beliefs and want to stage a public attack in order to make a statement to raise awareness for their beliefs, or simply destroy someone else's.

Coercion

Sometimes attackers are not personally motivated, but are being coerced by a corrupt organization or individual to commit a crime. For instance, a competitor who wants to bring an organization to its knees, or someone with political aspirations, or an activist group that may not have the knowledge or experience to stage an attack coerces someone else into launching an attack.

Ego

Sometimes attacks come right down to ego and are a twisted way of making someone feel like they're important. Attacks can feed the ego by "proving" their power and influence — e.g., "I'm better than you are because I can deface your website and tarnish your brand."

3. Opportunity

To launch an attack, someone has to have the opportunity. Hacking into computers is much easier than breaking down brick walls these days, but you still need an entry point. Because computers are connected via the Internet, someone who knows what they're doing can get in. Edward Snowden had the opportunity to access information because he was trusted by the NSA and no one was watching him — sometimes that's all it takes.

In the end, you can narrow down what type of perpetrator(s) you're looking at by analyzing their approach. But defending your assets is the next step. You can't just invest in network monitoring software and then set it and forget it. Your network defenses are like battle tanks and airplanes; someone must choose which one is going to be most effective against a threat, and that someone needs to make decisions on the fly, and use his or her intuition and experience to determine the true nature of the attack.

TYPES OF ATTACKS

In order to defend your organization, it's important to understand the different types of threats out there so you can build up defenses against them.

DDoS attacks

The goal of DDoS attacks is downtime — essentially bringing down an organization's website to halt business by creating a surge of unauthorized traffic that chokes the system. To stage a DDoS attack you need thousands of computers that overwhelm a website and cause it to crash. One way to acquire multiple computers is through phishing scams where perpetrators try to get innocent people to click without realizing that malware is being launched in the background, compromising their systems.

Brute force attacks

Rather than exploit weaknesses in software, these attacks are much simpler — they focus on breaking down barriers by trying to decipher a login and password. Computers usually try up to 15,000 passwords before they give up and move onto another machine. If you're monitoring your network and you see this kind of activity, it's likely that you're the target of an attempted attack.

Malware

Worms, Trojan horses, viruses, spyware and other malicious software are all considered types of malware. These hostile programs all are a means to an end — that end being data theft, espionage or sabotage. While malware is very damaging to systems and networks, the number of attacks has steadily decreased over the past few years because systems are being built better, and are harder to penetrate; but it is still a threat.

Social engineering

When cybercriminals exploit human weaknesses by psychologically manipulating them into providing system access or divulging confidential information, this is called social engineering. Phishing is a common form of social engineering since it is used to infect computers and exploits the notion that people are naturally trusting, clicking on emails they shouldn't, and unknowingly infecting their computers.

Data leakage

Data leakage occurs when confidential data gets leaked out, either with malicious intent or not. It could be that someone purposefully leaks the data or that someone inadvertently leaks it. Detecting data breaches and exfiltration transmission is critical because sensitive data, such as financial, patient and credit card data, intellectual property and company information can cripple an organization if it gets out.

DEFENDING YOUR NETWORK

Once you understand where your organization might be vulnerable, why someone might want to attack you, and what approach they will likely use, how do you defend yourself?

Visibility

Network visibility is more than just a window into your network, it's insight. It allows you to see what normal activity looks like so you can detect anomalies when they occur. For example, on average, individuals write about 30-50 emails a day. Visibility into your network means you can see when someone sends 1,000 emails, which serves as a warning sign, because it is out of the norm. Similarly, desktop computers typically talk to about 400 other computers every day — a significant increase beyond the typical is considered an anomaly and should be flagged. These days, attackers have become smarter and commonly encrypt their communications, which is harder to detect and defend against; but visibility into behavior — specifically behavior that is unusual — gives you insight into what is happening.

Defenses

Any type of defense is better than nothing at all, but understanding why you might be a target will help you customize your defense strategy most effectively.

Computers today have millions more files than they used to, making it easier and easier for attackers to hide on your computer. When it comes to defending your network in a cost-effective way, you may have to lure the attacker out. The moment the attacker starts communicating over the network is the only time they emerge from cover, and you stand a much better chance of catching him or her. With network visibility you're able to catch hackers in the act. Still, there are some really helpful tools that can help you defend your organization before it even gets to this point.

Firewalls

90 percent of security threats can be stopped by a firewall. It's like building a fence — they can limit who comes in and out of your network on a basic level. They still serve as the front line of defense, but they shouldn't be your only defense. They can't, for example, prevent incoming DDoS attacks.

Patches

Patches are one of the simplest forms of preventing malware from infecting your network. Just by keeping your systems up to date, patches can help keep your systems more secure by addressing vulnerabilities and improving detection.

But in order to keep your network secure, firewalls and patches are not enough. You need to make additional investments.

Visibility tools

Good visibility products are not just network monitoring tools. Visibility tools collect data from many vantage points, offer myriad views into network data, and store histories so you have what you need to understand the impact on your network. Visibility tools prepare you to deal with unknown future situations, so you can always be one step ahead of your perpetrators. These tools provide a level of depth and complexity that allow a skilled operator to gather the necessary insight to keep your network safe and operational.

Although “visibility” and “monitoring” are often used interchangeably, they are not the same thing. Most monitoring products collect only what is needed to solve the “uptime” problem, and don’t offer much in the way of handling the unexpected. Timeframes are rough, often 5-minutes-by-5-minutes, and historical data is notional at best. Most of all, the different views of the network are limited and simplistic, lacking insight.

This can be risky because as perpetrators become more and more savvy, they know how to hide their malicious activity, which can go undetected. It’s important to have access to ALL your network data so you can be proactive and not reactive and have a system that provides real-time data analysis and high-speed detection and forensics.

CONCLUSION

While the real intelligence starts with human beings who can recognize anomalies, network behavioral intelligence tools are also essential for fending off attackers. These high-speed visibility tools can handle significant volumes of information that would be difficult to digest by even a super human.

To successfully fend off cyber attacks, your organization needs both network analysis tools and a dedicated individual who can make actionable and intelligent decisions on the fly. It will make all the difference in the end.

ABOUT FLOWTRAQ

FlowTraq® provides software and services for high-performance network monitoring, analytics, security and forensics to detect a range of network behaviors, including distributed denial of service (DDoS), brute force attacks, botnets, worms, network scans and other network traffic anomalies. To request a free trial of FlowTraq, visit **www.flowtraq.com/trial**.

FLOWTRAQ®

16 Cavendish Court, Lebanon, New Hampshire 03766
Phone +1 (603) 727-4477 | Email info@flowtraq.com