IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Preventing Data Loss: The Role of Internal Network Traffic Analysis in Cybersecurity

August 2016

Adapted from *Worldwide Specialized Threat Analysis and Protection Forecast, 2015–2019: Defending Against the Unknown* by Pete Lindstrom and Robert Westervelt, IDC #256354

Sponsored by Arbor Networks

The threat landscape is rapidly evolving with financially motivated attackers, nation-states, and hacktivists out to disrupt business operations, steal data, or conduct corporate or cyberespionage. The security industry is flooded with a variety of untested security start-ups. Some of these emerging solutions provide innovative approaches to attack detection and prevention. A comprehensive approach for data protection has network monitoring and traffic inspection at its core. Network traffic analysis is an essential element of most threat prevention and data protection strategies. This IDC Technology Spotlight explores why these solutions are a requirement and describes the most critical components necessary to identify and contain attacker movement before critical network resources and servers containing sensitive data are exposed. It also discusses the role of Arbor Networks solutions in addressing the challenges described.

The Data Breach Era: The Rapidly Evolving Threat Landscape

Financially motivated criminal groups are more organized than ever. They have incorporated advanced persistent threat tactics stemming from nation-state cyberespionage attack activity. This has enabled organized criminal gangs to carry out successful targeted attack campaigns against a variety of organizations regardless of company size or industry. While senior management is always considered to be a top target, criminals now incorporate reconnaissance activities into their targeted attack campaigns. The goal is to identify and exploit payroll and HR managers and others supporting financial operations.

Attack campaigns are becoming more calculated and profit driven, but it's clear that most attackers gain initial access to the corporate network by using less sophisticated measures. Widespread vulnerabilities and configuration issues make this stage of an attack relatively easy. Time-tested tactics such as phishing help these attackers obtain account credentials and leverage user privileges to gain almost unfettered access to corporate resources. Once inside, attackers set up a staging area, often using an attack toolkit to open a back door and maintain persistent access to the network.

One essential element of the attack scenario remains lateral movement within the network from the point of entry to the sensitive resources in data repositories and servers supporting critical business applications. This is where network traffic analysis security solutions play a critical role in an enterprise's arsenal. Organizations that have deployed solutions that can perform deep packet inspection and network flow analysis are in the best position to identify this attacker movement and stop it before critical resources are accessed and data is removed from the environment. In fact, an IDC survey of more than 1,000 IT decision makers found that network traffic analysis security ranked the highest among large and very large organizations, with 42% of respondents citing it as a top initiative.

CISOs consistently tell IDC that gaining visibility and full situational awareness about the organization's security posture at all times is a significant challenge but paramount to detecting threats and containing threats as quickly as possible. This heightened visibility helps decision makers address weaknesses that put the most critical data at risk.

Adopting a risk-based approach enables security teams to allocate resources effectively and get the most value out of IT security architecture. The alternative approach, and one that is often encountered by forensics investigators following a breach, involves blindly adopting technology without consideration of the data assets that require protection. In the first half of 2016 alone, more than 473 data breaches were publicly disclosed, exposing more than 12.6 million records, according to the Identity Theft Resource Center, which maintains a database of security incidents that result in data loss or exposure.

The modern network security solutions being adopted to detect advanced threats may have prevented many of these breaches. Emerging solutions no longer provide limited visibility and inadequate performance. They provide comprehensive protection and tools and insight that enable security teams to proactively hunt for security threats already on the network.

The immediate value that enterprises gain in adopting some of these solutions helps ease the burden on today's incident responders and shifts their focus to the threats that matter most. Specifically:

- **Prioritize threat indicators:** Security teams of all sizes can use the risk scoring provided by some solutions to prioritize response efforts and eliminate being side tracked by investigating ghost alerts. In addition to risk scoring, these solutions often give analysts the capability to remotely remediate threats.
- **Provide desired automation:** Solutions that provide automated correlation of threat indicator data and traffic patterns decrease false positives and reduce the dwell time an attacker has on the network. This level of automation can quickly identify abnormal network activity and assist incident responders in blocking botnet communication and preventing attacker movement.
- **Examine historical patterns:** Solutions that provide retrospective analysis may speed threat detection by incorporating previous security incidents and network activity into real-time traffic analysis. They also give investigators tools to conduct high-speed searches as well as visualize, validate, and confirm the extent of a newly identified threat.
- **Deliver detailed intuitive context to verify and speed remediation of an incident:** Solutions can ingest both network flow and network packets to provide visibility into all traffic emanating from hosts and the connections between those hosts. Alerts gain context to speed up an incident responder's ability to gauge the scope of an attack and quickly contain it.

The following data breaches illustrate the complexity involved in maintaining a comprehensive information security program:

- **Website vulnerabilities expose lapses:** Verizon Enterprise Solutions, which publishes an annual report analyzing data breach activity, acknowledged a data breach of its own in March. The lapse resulted in the leakage of contact information of 1.5 million customers of Verizon Enterprise. The breach stemmed from a website security flaw that was exploited to steal customer contact information. Meanwhile a website vulnerability was the cause of a data breach at Woodland, California–based Bailey's Inc. It impacted some 250,000 customers who shopped at the outdoor equipment retailer's website from 2011 to January 2016.

- **Attacker movement to point-of-sale systems:** The massive Target data breach in 2013 exposed how account credential theft where an attacker had access to one platform can provide a pathway to other sensitive systems on the network. A criminal group gained access to a business partner's account credentials and moved to the retailer's "segmented" network, which supported payment systems. A security platform alerted the organization to the presence of malware, but the security team failed to respond. A solution that identifies threat indicators and attacker behavior (rather than simply the presence of malware) may have provided more supporting evidence to raise the criticality of the alerts.

- **Lost laptops, probed database:** California Correctional Health Care Services acknowledged a data breach in May following the theft of a laptop containing the personally identifiable information of at least 400,000 people incarcerated between 1996 and 2014 at the California Department of Corrections and Rehabilitation. Attackers also probed a database at 21st Century Oncology, which operates 181 cancer treatment centers in the United States and Latin America. The company announced in March that it was informed by authorities that an intruder had gained access to a server with information about 2.2 million current and former patients, including patients' names, Social Security numbers, physicians' names, medical diagnoses, treatment information, and insurance information.

- **Database misconfiguration:** A misconfigured database from a child tracking and monitoring firm exposed millions of text messages and images as well as more than 1,700 child profiles. An authentication error was exploited in a data collection node implemented by a third-party service provider on behalf of the company uKnowKids.

Network traffic visibility is essential because tactics often change. Hacker tactics include automated attack toolkits and custom malware designed to evade detection as well as polymorphic malware able to modify its characteristics to avoid detection by antivirus scans. Distributed denial-of-service (DDoS) attacks are also used to cripple a victim's resources.

Specialized Threat Analysis and Protection

The specialized threat analysis and protection (STAP) market consists of three segments:

- **Endpoint STAP:** Modern endpoint STAP solutions provide the visibility necessary to help validate a threat and assist incident responders in remediation using embedded forensics capabilities. These modern endpoint security solutions harden and protect endpoints (computers, servers, smartphones, and tablets), making them less vulnerable to targeted attacks and sophisticated malware. For endpoint, some type of client is required even when many of the functions (such as analytics and calculations) are performed at a central server or in the cloud. These solutions may simply detect and alert, or they may detect, alert, and prevent files from executing. They are designed to complement traditional antivirus or simply replace it. Modern endpoint antimalware solutions are often tied to a suspicious file analysis sandbox for additional support.

- **Boundary STAP:** Boundary STAP has been widely adopted by enterprises of all sizes and is provided by many security vendors to detect previously unseen malicious files. Boundary STAP is typically a file analysis sandbox tied to a cloud-based threat intelligence database of URLs, file hashes, etc. It is designed to function when the legitimacy of a file is challenged, typically when antimalware engines fail to determine the risk and digital software credentials are uncertain. The boundary technology is designed to detonate suspicious files in a protected environment to document malware activity or malicious indicators (such as known command and control locations) that will enter the enterprise network. Boundary supports files delivered through all types of traffic (e.g., HTML, SMTP, TCP/IP). Today's antimalware sandboxes consist of on-premises sandboxes and SaaS subscription-based services.

- **Internal network analysis STAP:** This emerging network security segment is made up of security technologies that are at the foundation of enterprise incident response and forensics. These solutions monitor network flow or other traffic to discover anomalies within the network that indicate attacker reconnaissance activity, malware movement, and botnet or malware command and control activity. Network flow essentially answers the following questions about network traffic: Who? What? When? Where? How? Solutions also may combine network packet capturing capabilities and perform deep packet inspection. Network packets are collected and analyzed to provide source, destination, and application information that includes destination IP addresses as well as port information. Traffic is usually classified to provide bandwidth information and can be broken down to provide data on applications, users, and servers.

The emergence of STAP products has caused considerable confusion because technologies often span traditional functional markets (endpoint, web, messaging, and networking security), making product evaluations and functionality comparisons extremely difficult. A comprehensive approach to detecting advanced threats involves adopting solutions from all three STAP segments.

Security vendors are increasingly offering products from each STAP category to provide seamless integration and cohesion across the IT security architecture. APIs are often made available for these products to function with third-party tools. IDC has noted that some large enterprises are choosing products from multiple vendors, but some security teams are more comfortable standardizing on a solution from a single vendor. Midsize organizations are also considering these products and can choose to engage with a trusted managed security services provider (MSSP) to assist with management and incident response.

Arbor Networks Spectrum

The Arbor Networks Spectrum network-based advanced threat protection platform is designed to enable security teams to quickly uncover, investigate, and prove attack campaigns. The product helps modernize today's security operations center, transforming manual processes into natural workflows and data visualizations for active threat hunting.

Spectrum conducts integrated network flow analysis and performs packet capture for deep packet inspection and retrospection to correlate indicators through historical analysis of traffic patterns. It can also be configured to interrupt command and control communication and provide updates to bots and tools. The solution is designed to provide the data and performance necessary to be engaging for senior responders to proactively hunt for threats and intuitive enough for novice analysts to quickly get up to speed. Spectrum is delivered as an on-premises solution and consists of a packet collector, management console, and flow collector.

Arbor is the leader in DDoS attack prevention and has been adopted by nearly all top-level internet service providers. Arbor leverages its anti-DDoS legacy with Spectrum by tapping into its Active Threat Level Analysis System (ATLAS), a global platform of real-time attack traffic shared by more than 330 global network service providers. This provides a significant differentiator from competitive solutions that incorporate data from far fewer service provider resources. It can also ingest third-party threat intelligence feeds. Arbor combines its ATLAS threat intelligence with a human element, Arbor's Security Engineering & Response Team (ASERT), to rapidly investigate new threat indicators to provide an early warning to customers with relevant context to gauge the risk of the newly discovered threat.

Challenges

Arbor Networks Spectrum is a solution that should appeal mainly to organizations with a dedicated security team, but it can also be managed by a service provider. Because of the need to capture and record network packets in real time, Arbor currently offers on-premises appliances for visibility into east-west traffic within the enterprise, with virtual versions available in fall 2016. Spectrum is also a standalone product for internal network (east-west) visibility. It can be combined with Arbor Networks APS, which provides on-premises and cloud-based DDoS mitigation.

Conclusion

Most data breach analysis reports suggest that the average dwell time of a data breach is greater than 200 days. This gives criminals far too much time to monitor, move laterally through, and steal valuable data from the corporate network before covering any trace of their presence. Proactive network security monitoring and threat hunting are essential to detect the rising tide of these targeted attacks and advanced threats designed to evade traditional security solutions. In fact, in 2015, advanced attacks used seven or more toolkits, demonstrating how attackers have bolstered their arsenal.

Organizations committing to establishing and maintaining a proactive security posture require a dedicated security team and the tools necessary to rapidly detect, investigate, validate, and remediate a threat before the security incident becomes a high-profile data breach. This involves creating a cohesive IT security architecture that pulls in relevant data to establish situational awareness at the endpoint, application, and network layers. Gaining that visibility requires modern products that encompass endpoint STAP, boundary STAP, and internal network analysis STAP. This approach enables rapid incident response and provides the sophistication necessary to prevent threats and protect sensitive resources from falling into the hands of criminals. Arbor Networks' Spectrum product addresses many of these challenges. To the extent that Arbor Networks can address the challenges described in this paper, IDC believes that Spectrum is well positioned for success in the STAP market.
