Bitdefender®

COMBATING ADVANCED THREATS WITH NETWORK TRAFFIC ANALYTICS

WHITE PAPER

Improving Threat Hunting and Reducing Time-to-Detection

"What network traffic analytics sees is what is actually happening in the business in real time, with the possibility to thwart attacks before catastrophic damage occurs. Network traffic analytics (NTA) is fast becoming the easiest-to-manage choice to detect infected devices, track account activity and catch data being staged for later exfiltration. NTA goes beyond catching unauthorized east-to-west traffic and improper use of protocols, to include alerts when clients start acting as servers, signs of ransomware via suspicious file share activity, connections to external domains within a few milliseconds of opening an email attachment, and more." [1] Eric Ogren, 451 Research

A sound security architecture goes well beyond endpoint security, and IT chiefs know it. Even organizations with a robust cybersecurity posture can suffer from:

- Late detection.
- Limited support for incident response.
- Spotty detection of insider threats.
- Irresponsible user behavior.
- A fatiguing stream of false positives.

In an increasingly complex environment (IoT, BYOD, etc.) and a digital economy riddled with cyber incidents and threats, organizations clearly need a more proactive solution. A solution with visibility into network-level threats and traffic anomalies, and the ability to detect risky user behavior that can lead to breaches and data leaks. They want automated security analytics to reduce noise and improve threat-hunting efficiency. And they need quick, actionable alerts to speed incident response.

Network traffic analytics represents the next generation of threat detection. It is a solution tailored for combating advanced threats in a security analytics market that Research and Markets predicts will reach $6.5 billion in 2022[2]. Bitdefender Network Traffic Security Analytics (NTSA) is the Bitdefender NTA solution offering real-time breach detection and complete threat visibility to help CISOs employ a more comprehensive and effective approach.

The Costs of Damage Control

High-profile hacker attacks often overpower traditional endpoint and network security tools. Late detection, limited visibility into insider threats, and excessive false positives give attackers the advantage. And when disaster strikes, the costs can be staggering with regulatory scrutiny often dealing a secondary blow.

For example, the late 2017 Equifax incident demonstrated that simply leaving corporate software unpatched can lead to tragedy. The costly breach resulted in the firing of three top executives and damage to their corporate image. Fortunately for Equifax, the breach occurred before Europe enacted GDPR data privacy laws, which would have levied much harsher penalties.

The ransomware attacks of WannaCry and NotPetya were even more crippling, costing both public and private sectors billions of dollars in just days. Like Equifax, most victims had outdated software and poor internal security practices.

In fact, the costs of a weak cybersecurity posture grow every year, partly because legislators have made it

their mission to encourage responsibility and punish organizations with lax security. A recent IBM study found that in 2018, the global average cost of a data breach rose 6.4 percent to $3.86 million[3]. And that doesn't include the hidden costs of lost business, damage to reputation, and countless hours spent on recovery.

Yet while ransomware remains the most damaging and profitable form of malware, it's APTs that security officers truly fear, as they can fly under the radar for years, exfiltrating copious amounts of data.

Advanced Persistent Threats

The year 2018 ended on a note of caution, with the world's largest hotel chain suffering a major, advanced persistent threat (APT) attack. The Marriot incident and its compromise of 500 million records showed that APTs continue to inflict high-profile breaches despite growing public awareness.

APTs, the most resource-intensive form of cybercrime, are multi-layered attacks that take a long-term approach to gaining entry, avoiding detection and collecting large volumes of valuable, protected information. Attackers typically have a clear objective and, although they may deploy their malicious campaign via simple social engineering schemes like phishing, the full scale and impact of the attack is often orders-of-magnitude larger.

Bitdefender 2017 - 2018 APT Investigations

- Operation PZChao: A Possible Return of the Iron Tiger APT >>
- RadRAT: An All-in-One Toolkit for Complex Espionage Ops >>
- Inside Netrepser – a JavaScript-based Targeted Attack >>
- Inexsmar: An Unusual DarkHotel Campaign >>
- Triout – Spyware Framework for Android with Extensive Surveillance Capabilities >>
- Three New Pacifier APT Components Point to Russian-Linked Turla Group >>

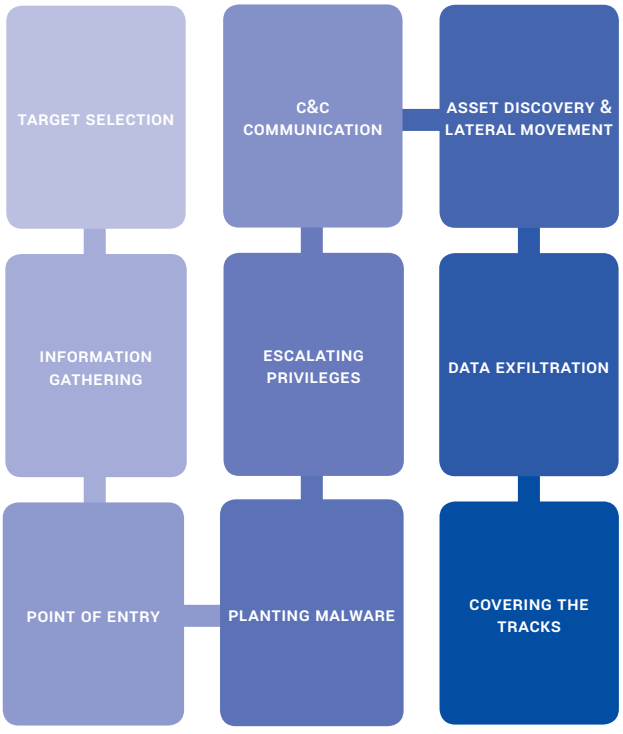

Figure 1: APT across the Kill Chain

What differentiates APTs from other attacks is the ability to quietly exfiltrate sensitive data while remaining undetected for months, or even years. Some attack methods include instructing legitimate applications to go rogue or studying security solutions to learn how to avoid detection. Figure 1 depicts an example of an APT attack mapped to the Cyber Kill Chain.

Unfortunately, APTs persist because no single security solution has been reliably able to thwart them, requiring a combination of security technologies to detect and fight these types of attacks.

The Science of Network Traffic Analytics

High-profile breaches have made network traffic analytics stand out as a formidable weapon against sophisticated attacks and advanced threats that elude prevention mechanisms at the endpoint level.

Network traffic analytics complements existing defenses by offering what no other security tool can: in-depth knowledge of the behavior of every endpoint on the client's network and significant reduction of time required to detect an attack and stop it. A look at the anatomy of network traffic analytics shows how solutions leveraging analytics can prevent advanced attacks from unfolding.

Behavior Versus Signature

Network traffic analytics effectiveness stems partly from the ability to model a behavioral baseline for devices and applications on a network – in short, to perform **behavioral analytics**. By comparing new observations against those baselines, behavioral analytics offers actionable insights about threats never seen before, as opposed to signature-based methods, which only identify known threats.

Analyze Encrypted Data Without Affecting Privacy

Experts agree that traffic analytics is a crucial asset in the fight against data breaches for any organization, regardless of size or business model. A key benefit of network traffic analytics is the ability to investigate encrypted traffic for signs of compromise without affecting the security of the data or the privacy of the data's owner.

As most traffic today is encrypted (approximately 80% according to some estimates), this is instrumental. While encryption protects data, it also creates blind spots for those trying to secure it. Network traffic analytics can decrypt traffic for analysis while ensuring its integrity and security as it flows. The exclusive focus on traffic meta-data enables analysis of encrypted communications without raising privacy concerns.

Agentless, Top-down View

Network traffic analytics tools are designed to let IT staff identify and rank threats according to priority, then create and deploy an incident response plan early in the attacker's kill chain. Network traffic analytics offers real-time network event monitoring from every endpoint and granular network logs to assist in forensic analysis to better understand the attack method and system vulnerabilities. The agentless breach detection capabilities extend to every device in the network and make it possible to track IoT and BYOD deployments. By focusing on the network behavior of endpoints, network traffic analytics can protect devices with limited or no built-in security and no endpoint security agent running on top. These characteristics create a formidable weapon against APTs.

Network Traffic 'Detective'

So, where does network traffic analytics fit into a company's cybersecurity stack? To answer that, we must underscore the main types of cybersecurity controls typically used by an organization's IT department. As defined by the CISSP Common Body of Knowledge (CBK) by ISC2[4]:

- **Directive Controls.** Policies and standards that advise employees of the expected behavior for protecting an organization's information asset from unauthorized access.
- **Preventive Controls.** Physical, administrative and technical measures intended to prevent unauthorized access to an organization's information assets.
- **Detective Controls.** Practices, processes and tools that identify and possibly react to unauthorized access to an information asset.
- **Corrective Controls**. Physical, administrative and technical countermeasures designed to react to security incidents to reduce or eliminate the chances they will happen again.
- **Recovery Controls.** Deployed to repair or restore resources, functions, and capabilities after a violation of security policies.

The (ISC)² CBK is a collection of topics relevant to cybersecurity professionals around the world.

It establishes a common framework of information security terms and principles which enables cybersecurity and IT/ICT professionals worldwide to discuss, debate and resolve matters pertaining to the profession with a common understanding, taxonomy and lexicon. – isc2.org

Network traffic analytics fits seamlessly between preventive and corrective controls as a detective solution, using network communications as the data source for detecting and investigating anomalous activity within the network. From a security technology perspective, network traffic analytics is adjacent to next-gen firewalls and IDS/IPS, but also complements network monitoring and EDR. But network traffic analytics has some strong points that other solutions don't.

A key strength is that network traffic analytics provides complete visibility into threat-related network activity, including lateral, or east-west movement. It uses AI, behavior analytics and superior threat intelligence to detect advanced threats that have never been seen before. And it stores volumes of meta-data for use in compliance and forensics, as well as to retroactively detect threats.

Bitdefender Network Traffic Security Analytics (NTSA)

Bitdefender NTSA lets organizations quickly detect sophisticated threats by complementing their existing security architecture – network and endpoint – with specialized network-based defense.

It uses network traffic as its primary resource to detect both generic and advanced persistent threats by sensing behavior anomalies. Alerts are generated to inform security operations about endpoint behavioral changes that indicate an attack is deployed and endpoints are compromised.

But how does it spot behavioral anomalies?

Threat Intelligence and Artificial Intelligence

NTSA draws from superior threat intelligence collected from over 500 million endpoints globally. It combines this knowledge with advanced machine learning and heuristics to analyze the network meta-data in real time and accurately reveal threat activity and suspicious traffic patterns.

Incident Alert Triage Automation

Automated analytics and alert triage reduce noise and provide human readable context to reduce the investigation time and increase the effectiveness of security operations and incident response teams.

BYOD and IoT Protection

An agentless technology, NTSA has every endpoint covered, focusing on the network behavior of endpoints, protecting even devices with limited or no built-in security or security agent running.

Compliance

Today's regulatory landscape forces data breach victims to quickly provide detailed information about malicious activities after a breach. NTSA helps organizations meet compliance standards by recording information about network data traffic for extended periods of time. The recording contains only meta-data, with no actual payload, and access to recordings is restricted to the Data Privacy Officer only, eliminating the risk of exposing sensitive information.

Beat Attackers at Their Own Game

Combating multi-phased attacks like APTs requires multi-layered defenses. Network traffic analytics complements your existing security architecture with specialized network-based defense, analyzing behavior at the network level and producing data indicating potential points of compromise and risky or malicious user behavior.

All malicious and risky behavior leaves clues on the network. By recording network meta-data over time and applying advanced machine learning models, network traffic analytics can detect even the smallest deviation from expected behavior. By including network traffic analytics in their entire cybersecurity stack, organizations can reach unprecedented levels of visibility into all abnormal activity in their infrastructure.

To learn how Bitdefender NTSA can help you improve threat-hunting and reduce time to detection, visit the Bitdefender Network Traffic Security Analytics website for more information.

[1] Machine Learning Signals a New Analytics Era in Security, 451 Research, December 2017

[2] Research and Markets: Security Analytics Market - Forecasts from 2017 to 2022

[3] IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses

[4] CISSP Common Body of Knowledge

Bitdefender®

www.bitdefender.com

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers and Cloud infrastructure. Today, Bitdefender is also the provider of choice, embedded in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on.

Bitdefender-Business-Whitepaper-NTSA-CREA3335-A4-en_EN