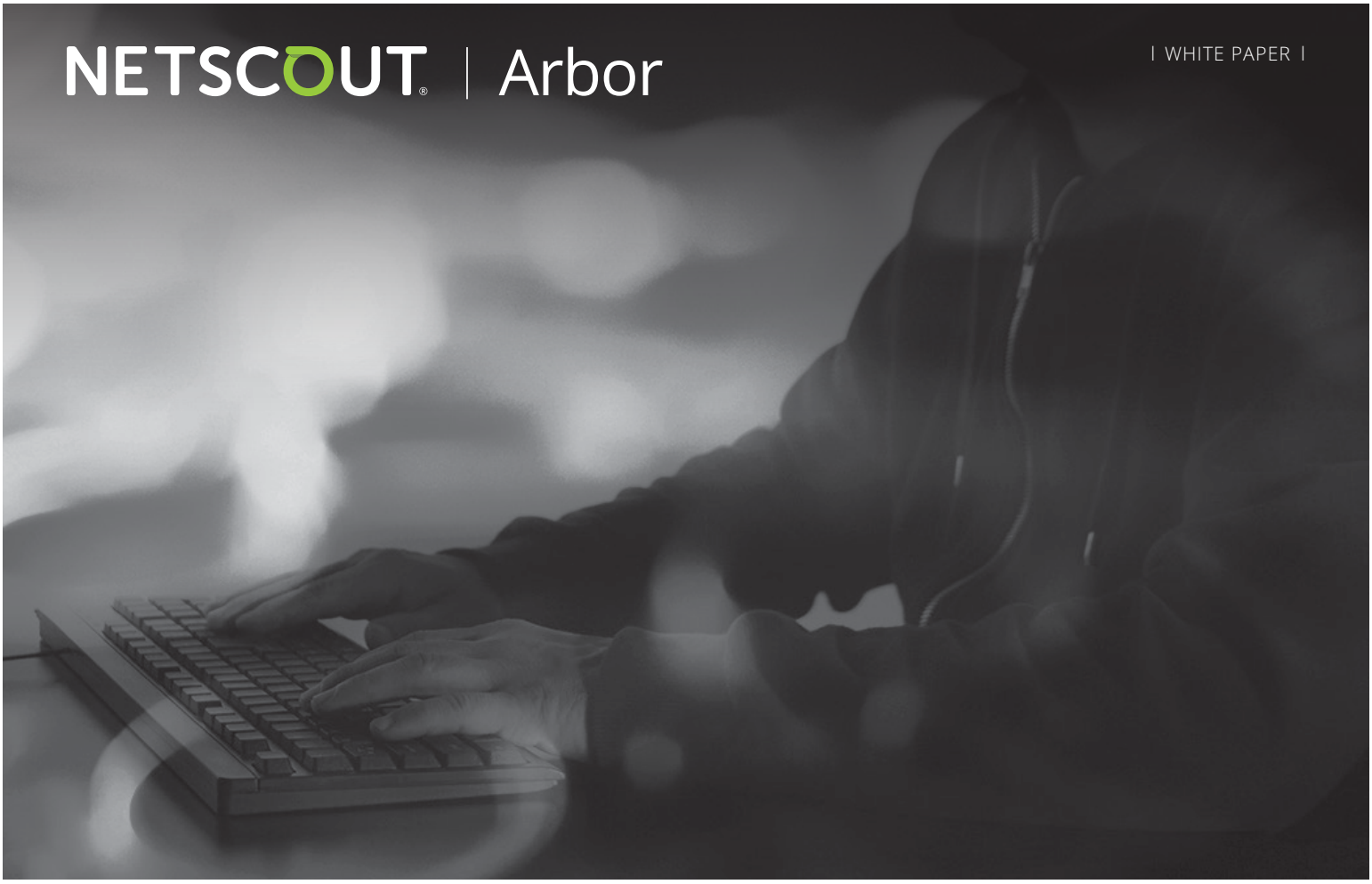
NETSCOUT | Arbor

I WHITE PAPER I



SecOps Analytics for Improved Response

Post-Exploit Visibility

SECURITY

Cybersecurity always has been, and always will be, about effectively integrating people, process, and technology to appropriately reduce risk to a tolerable level. From a technology perspective, solutions should make your people and security processes more effective & efficient.

The main takeaway is that the majority of enterprise security teams lack the ability to quickly assess post-exploit attacker activity. Being able to see and track cyber attackers as they expand beyond their initial access in your network is critical. Why? Because despite your best efforts at preventing attackers from penetrating your network, it's increasingly clear that threat actors are successfully gaining an initial point-of-presence. An attacker's initial access can be leveraged to expand to additional hosts on the network, faster than typical cybersecurity workflow can detect and respond. Therefore, gaining immediate visibility into post-exploit attacker activities is a critical element of prioritizing response.

The purpose of this whitepaper is to explain the importance of post-exploit attacker visibility. After reading this whitepaper you'll better understand one of security's biggest blind spots and how to eliminate it – significantly improving your ability to detect and respond to validated threats before they do damage.

The majority of enterprise security teams lack the ability to quickly assess post-exploit attacker activity.

What is Post-Exploitation?

A common term in Penetration Testing circles, post-exploitation is what an attacker does once they gain access to a targeted system. Post-exploit activities are right of boom; the intrusion has begun. For example, often an attacker gains access to your environment by spearphishing an unsuspecting user, despite your best security awareness efforts. Many of these initial accesses are automated, reporting back to an attacker with initial findings to help determine if it requires manual intervention. If so, an attacker will typically first fortify their access, even patching the system in the enterprise network to ensure no other attackers will attempt to take it over. Next, it's a matter of ensuring the access is persistent, allowing the attacker to come back at will. These activities are all initially performed on a single host, but with the beachhead established, it's time to start searching networked resources for additional footholds and data worth stealing.

What is Post-Exploit Visibility?

Post-exploit visibility is the ability to monitor and track attackers after they've gained an initial foothold in your network. Once an attacker establishes his or her initial presence in your environment, their next objectives include surveying the network, expanding accesses, locating and accessing valuable data they're after, and then exfiltrating the information. We summarize this attacker behavior as Land, Expand, and Action. Let's take a closer look at what an attacker does once they have landed in a new environment. These activities include:

Internal Reconnaissance: While reconnaissance is best known as the first step in the kill chain, it's also a key activity that occurs post-exploit. Internal reconnaissance is about gaining more information concerning the internal workings of the network and systems with the goal of escalating privileges, locating the targeted data, and determining how best to access this information. Common post-exploit reconnaissance activities include port scanning and sweep scanning.

Privilege Escalation: A key attacker goal of internal reconnaissance efforts is gaining access to privileged credentials. While an attacker would love to have immediate access to privileged credentials, they often must take interim steps to achieve this objective. This could mean accessing non-privileged credentials that will provide them with more information and/or access to accomplish their objectives. In fact, many attackers prefer to obtain access to multiple sets of credentials and systems to increase persistence and the overall resiliency of their efforts.

Lateral Movement: Related to the above, lateral movement represents the internal network traffic of attackers as they move between systems in your environment attempting to gain access to additional systems. From a network traffic perspective, lateral movement is commonly referred to as East-West traffic or Host-to-Host communications. Lateral movement is the glue and mechanism that bridges internal reconnaissance, privilege escalation, and access to targeted data. Therefore, having visibility into post-exploit attacker activity has become paramount to effective cyber defense.

Why Does the Post-Exploit Blind Spot Exist?

The post-exploit blind spot exists for two main reasons. First, security organizations have historically spent the majority of their efforts on prevention. Logically, if attackers are blocked from getting past defenses, there's no need to look for post-exploitation activities. However, determined attackers continually outthink and outmaneuver stagnant perimeter-based systems. Despite the significant investment in preventing an attacker from exploiting a host, it's clear that attackers are increasingly successful getting past the initial exploit stage. This is because despite organization's best efforts to prevent infections, there are just too many attack vectors to achieve 100% prevention.

Second, from a network perspective, many organizations have not instrumented for visibility into East-West network traffic. In some larger enterprises, network performance monitoring is conducted between segments, but these products focus specifically on identifying network availability issues. Traditional security experts think that limited internal network monitoring is sufficient if every host on the network is monitored, thereby catching threats before they spread. However, we see ample evidence that advanced threats continue to evade endpoint detection and response (EDR) capabilities. Adding a layer of network visibility enhances EDR capabilities, especially when attackers use non-traditional systems like printers as part of their movements.

To eliminate the post-exploit visibility blindspot, organizations must analyze internal network traffic for attacker tradecraft.

Eliminating the Post-Exploit Visibility Blind Spot

To eliminate the post-exploit visibility blindspot, organizations must analyze internal network traffic for attacker tradecraft – the actions they take as part of their operations. While attackers are having increasing success establishing initial footholds in networks, the good news is there are several additional moves they need to make before they can get to the action phase of the attack. This means the ability of security organizations to detect post-exploit activity is increasingly critical to preventing intrusions from doing damage.

Internal Network Traffic Visibility for Baselining & Monitoring – By monitoring internal network traffic, organizations can baseline what's normal and what's not. For example, it's perfectly normal for every user's computer to communicate with a mail server. However, it's abnormal for two user's computers to be communicating directly with each other. Even more abnormal is a user's computer in the HR department communicating with a source code repository, which contains valuable intellectual property. Monitoring, baselining and analyzing network behavior with the goal of looking for attacker activity is a good first step but it's not enough. This is largely a result of the potential for false positives related to behavioral analytics.

Looking for Digital Exhaust from Attacker Tradecraft – When attackers are inside your network and moving laterally, they leave subtle traces of digital exhaust. Having knowledge of what attacker tradecraft looks like and where to look it is critical to detecting and stopping cyber threats that have made it past the exploit stage. Knowing what to look for is important, but equally important is knowing where to look.

Correlating Post-Exploit Context with Other Security Alerts to Improve Analyst SOC Effectiveness & Efficiency – Post-exploit context in and of itself provides value by enabling you to see and stop attackers that have penetrated your network. However, the value of post-exploit context increases exponentially when it's correlated with security alerts from SIEMs, endpoint, network, and other security controls. By correlating post-exploit context with existing alerts, your security analysts can better confirm which alerts they should be focusing on their scarce time on. This increases the effectiveness and efficiency of your entire security operations team from tier 1 and 2 analysts to incident responders.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECWP_002-1700 10/2017