Protecting the Enterprise Network with Global Attack Intelligence
Arbor Networks, Inc. is a leading provider of network security and management solutions for enterprise and service provider networks, including many of the world’s Internet service providers and many of the largest enterprise networks in use today. Arbor’s proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the ATLAS® Active Threat Level Analysis System. Representing a unique collaborative effort with 270+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.

About Arbor Networks
Executive Summary

The Internet has become such an extension of the corporate network that for many organizations the Internet is the corporate network. Not only has the Internet become essential for connecting workforces with customers, suppliers and business partners, it is also critical for many internal operations as well.

In fact, operations essential to growing revenue, retaining customers and increasing competitive advantage depend on this extended network being available and secure. For the modern enterprise to be successful, the network must remain connected, accessible and dynamic. Unfortunately, these attributes also contribute to making the enterprise increasingly vulnerable. Cyber attackers have grown more sophisticated, morphing “yesterday’s malware” (trojans, keyloggers, botnets, DDoS, etc.) into well-planned cyber attack campaigns.

In this white paper, we’ll examine how the Pravail® portfolio from Arbor Networks can empower your network operations and security teams to more efficiently help protect the integrity and availability of your enterprise network against advanced attacks. Armed with unique global attack intelligence from within and outside your corporate network, these products provide you the visibility and awareness required to help block advanced attacks, solve problems faster and reduce the risk to your business.

The Impact of Advanced Attacks

The impact of advanced attacks on the enterprise can be devastating. In addition to the direct impact to enterprises (e.g., loss of revenue and productivity, reduced competitive strength) there is the possible collateral impact such as fines and damage to brand when breaches and downtime result in non-compliance with government and industry regulations.

- LulzSec, an offshoot of the Anonymous collective, launched a DDoS attack against Sony using Low Orbit Ion Cannon (LOIC) that camouflaged a data breach of 100 million customers. Sony estimated more than $170M (USD) in losses due to the attack while stock analysts expected losses greater than a $1B.

- On March 30, 2012, hackers breached the server housing Medicare claims for the Utah Department of Health, stealing the personal information of 181,604 Medicaid and Children’s Health Insurance Plan (CHIP) recipients—25,096 appear to have had their Social Security Numbers (SSNs) compromised.

- Approximately 80 major law firms were victims of cyber attacks in 2011. Several China-based hackers have broken into law firms’ networks in an attempt to stop a merger or acquisition, or interfere with a business deal.

- American Superconductor Corporation’s stock dropped 83% in the months following theft of its turbine control system source code stolen from its servers in Austria.

- A U.S. metallurgical company lost technology that cost $1 billion, and required 20 years of development, to cyber espionage based in China.

These are just a few representative examples; more attacks are uncovered literally every day. And the reality is that there are far more organizations dealing with these threats, and breaches, than are talking about it publicly.
Costs of Advanced Attacks

- **OPERATIONS**
  How many IT personnel will be tied up addressing the attack?

- **RECOVERY**
  How much manual work will need to be done to re-enter transactions?

- **END USER PRODUCTIVITY**
  How much employee output will be lost?

- **PENALTIES**
  How much will have to be paid in SLA credits or non-compliance penalties?

- **BRAND AND REPUTATION DAMAGE**
  How is the ability to attract new customers affected?

- **INTELLECTUAL PROPERTY THEFT**

- **NETWORK AND PARTNER INFILTRATION**

The Evolution of Advanced Attacks

Advanced attacks have evolved to become more adept at targeting and circumventing enterprise defenses, and more sophisticated in their execution. The success of these attacks is due in large part to their technique. While individual components can be ‘simple malware’, e.g. a variant of a known trojan, or a malicious document, advanced attacks are typically multi-layered campaigns, not singular components.

They are carefully planned and often manipulated in real-time by remote Command and Control. Real-time control enables the perpetrator(s) to intelligently overcome security measures, opportunistically exploit weaknesses they encounter, and extend their attack deeper into sensitive network resources.

The sophistication of these attack campaigns—whether employing uncomplicated but effective malware, or complex zero-day code—belie a high level of skill, organization, and funding—as well as persistence. Perpetrators of advanced attacks continue to gather intelligence and learn; if they fail at first they will tweak their methods and try again.
Though these campaigns all use combinations of malware and sophisticated techniques to distract, infiltrate, rob, disrupt or destroy, the motivation of advanced attack campaigns can vary widely:

- Hacktivists seek a public stage on which to make ideological or political statements. They may design attacks to disrupt or even destroy an organization—ultimately, if they are not seen, they have not achieved their goals.

- Organized cybercriminal groups target personally identifiable information (PII) or intellectual property (IP) for resale or ransom. Their attacks are designed to extract data from the target, not to disrupt or destroy the "golden goose."

- Corporate sponsors of advanced attacks aim to gain a competitive advantage through espionage or theft (e.g., of IP or other corporate data)—or by damaging their competitors through disruption or a complete competitive "take out."

- Nation states may be motivated by ideological position, profit, or even cyber terrorism.

It can be hard to distinguish the true goal of an attack. An overt DDoS attack to cripple a site may be planned cover for a cybercriminal attempt to infiltrate the target organization, steal PII, or delay discovery of financial fraud.

And while DDoS and botnets can represent significant components of advanced attack campaigns, they also are increasing in volume, complexity and frequency (Figure 1, page 4).

Botnets for hijacking servers and generating massive volumes of traffic are prominent components in DDoS attacks. But they can also be used for other tasks, such as to monitor network activity, map topology, and identify assets/targets.

Advanced attack campaigns leverage a combination and variety of computer intrusion technologies and techniques. They may include more focused components like spear-phishing, usually followed by an attempt to deceive a user into opening a malformed document. Once the network perimeter has been breached, attackers infiltrate more deeply into the vulnerable internal network of the targeted organization. Additionally, attackers commonly use SQL injection attack techniques and other tactics to exfiltrate sensitive data.

They continue to expand their attack toolkits by adding new exploits and new variants of malware, all designed to evade detection. Malware may be created anew, purchased in the underground economy, or some combination thereof. Many attackers will utilize "stock" malware and customize it for the company they are targeting - including features that will maximize effectiveness and evade host and network defenses.

There is a lifecycle to an advanced attack campaign. A typical targeted attack involves research on the target to include likely victims and potential vulnerabilities in public-facing sites. Once an attacker obtains access to the target, they often attempt to hide their presence in order to prolong their access. Longer, stealthy access allows for deeper penetration and the placement of multiple backdoors. In some cases, attackers will carefully cover their tracks to complicate forensic analysis once the intrusion is detected. Some attacks, or some components of campaigns, are better at this than others. Advanced Persistent Threat (APT) methodologies are designed to bypass legacy defenses so they may steal data and IP over long periods of time.

These techniques are so successful that most advanced attacks are not detected by the enterprises themselves. A recent survey found that approximately 70% of breaches were discovered by external parties.
Increased Volume
Largest volumetric DDoS has grown from 9 to 10 Gbps in 5 years.

Increased Complexity
Over one quarter of attacks are now application-based DDoS, mostly targeting HTTP, DNS and SMTP.

Increased Frequency
More than 50% of data center operators are seeing more than 10 attacks per month.

Layer 7 DDoS Attacks Against IDC

Average Number of DDoS Attacks per Month

---

*Figure 1 DDoS and botnets are thriving*

Understanding the Risks Posed by More Connections

The proliferation of mobile platforms, and the applications used by the mobile workforce, challenges IT to provide secure access to the infrastructure. A recent study found that 89 percent of IT departments worldwide currently enable BYOD (Bring Your Own Device). IT leaders expect the number of devices per employee, on average, to rise from 2.3 in 2012 to 2.8 in 2014 (see Figure 2). With the incorporation of proxy capabilities that allow attackers to connect deeper into a target network through a compromised device, the mobile workforce is increasingly vulnerable as a “backdoor” to corporate assets. Mobile technologies present a new and significant attack surface that increases organizational risk. Attackers are increasingly targeting these mobile devices and applications. The number and variety of downloadable applications for mobile platforms—frequently free and not under the control of enterprise IT—represents a “target rich” environment for introducing malware. A recent report stated “mobile malware threats increased 163% to more than 65,000 in 2012.” Further malware were becoming smarter, with the top three methods for delivering malware: app repackaging, malicious URLs, and smishing, ‘phishing’ with SMS messages. The mobile workforce is a tremendous boon for attackers looking to gain access to sensitive corporate assets.

Additional attack surface is introduced as the enterprise continues to deploy Internet connected websites and portals. There are public-facing corporate websites, portals used for eCommerce, customer service, and communicating with partners and your supply chain, as well as the growing adoption of off-premise cloud-based services for everything from payroll to email and even security services. Recent IDC cloud research shows that worldwide revenue from public IT cloud services exceeded $21.5 billion in 2010 and will reach $72.9 billion in 2015, representing a compound annual growth rate (CAGR) of 27.6%.

With so many different connected platforms, applications, and conversations taking place across the enterprise, gaps inevitably emerge in network traffic visibility and the detection of potential threats.

Figure 2 Average number of connected devices per knowledge worker, 2012 and 2014
Source: Cisco IBSG, 2012
You Can’t Secure It if You Can’t See It

Though perpetrators of advanced attacks take pains to disguise or hide their actions, some portion of the lifecycle of an advanced attack is inevitably reflected in network behavior. There is no hiding the clues, both specific malware fingerprints and larger traffic patterns, on the extended network. And eventually, some component of an advanced attack or anomalous behavior will be reflected across the internal and external network boundaries.

That is why it is critical to have visibility into both the traffic on the global Internet and the internal network. It is only by synergistically leveraging both these views that you can attain more complete and more effective visibility into what’s happening in your security environment.

Most enterprise security solutions rely on attack signatures to provide protection, which means they are effective only against known attacks and address only individual attack vectors.

• The most widely deployed anti-virus (AV) tools can detect only a limited range of mostly known malware. AV simply cannot keep pace with variations nor detect zero-day attacks. According to a Gartner report, only 24% of advanced malware is actually detected by AV software.11

• Network Behavior Analysis (NBA) and Security Information and Event Management (SIEM) tools monitor log files and trailing data from millions of events (ingress and egress of data—and events in-between)—but no real global network context. Reacting to this data, sorting out false positives, can bury IT.

• Intrusion Detection/Protection Systems (IDS/IPS) can only see clear-text traffic and will only generate alerts for a limited array of threats.

• Malware sandboxes only examine the narrow slice of activity at the point of infection, lacking critical context and adding overhead to the enterprise infrastructure.

Individual solutions provide only a partial view into an attack—they don’t provide the greater visibility, the context and intelligence on the likely shape and progression of an attack, nor how to prioritize and mitigate. Most significantly, given the speed and scope of advanced attacks, by the time these solutions provide any actionable insight, it’s usually too late.
Seeing and Understanding the Big Picture

You need to see the relevant network activity on, and traffic coming in from, the global Internet as well as internal network traffic flows to identify risks. By seeing these risks and analyzing the data, organizations can understand the bigger picture of what is happening on their networks. Only by bringing this intelligence together can you understand the real scope, nature and potential impact of an advanced attack campaign. This intelligence will better enable you to solve complex threats and risks introduced and help protect your business from today’s advanced attacks.

When it comes to fighting increasingly complex, dangerous and constantly evolving advanced attacks, deep knowledge of network behavior is perhaps your most powerful weapon.

The best approach to meeting the challenges of an advanced attack campaign and securing your network operations is one that bridges a view of global, external and internal traffic. You also need to see deeper into applications, users, and the Secure Socket Layer (SSL). Only then can you distill out anomalous and truly suspicious behavior such as “legitimate” users accessing inappropriate resources, valuable data exfiltrating to suspicious (or blatantly wrong) locations, or high volumes of data being transferred at unusual times. The best solution maps this greater intelligence against your most important systems (both web-facing and back-end) and databases, monitors in real-time, alerts and blocks attacks at the perimeter of your network—and quickly identifies those components that exist within the network.

![Figure 3 Integrated workflow](image-url)
Security Intelligence Empowers Organizations to Work More Effectively and Efficiently

Arbor customers enjoy a greater security, availability, and consequently a competitive advantage, because of the depth and breadth of real-time intelligence gleaned from Arbor's ATLAS® Active Threat Level Analysis System. ATLAS is the first globally scoped threat analysis network. Arbor enjoys a privileged relationship with a majority of the world's tier 1 ISPs.

ATLAS® Unparalleled Global Reach

- Over 3 Terabits per second of Internet transit traffic monitored and reported.
- 1 million+ unique IPv4 Internet addresses monitored for globally routed dark IP addresses.
- 31 GB of daily global darknet traffic is analyzed daily.
- Global dark IP route coverage is spread across North America, Europe and Japan.
- 75+ ISPs are sharing all real-time attack data with Arbor.
- 30+ ISPs are sharing full real-time routing data.

With its status as a trusted partner to the global cloud and service provider community, Arbor collects an unparalleled amount of global Internet data through its ATLAS network. ATLAS aggregates information from more than 270+ network operators across the globe, collecting real time security events, traffic and routing information to be used to strengthen the policies within Arbor’s security products.

It is the Arbor Security Engineering and Response Team (ASERT) that leverages this unprecedented, global visibility and disseminates analysis of ATLAS information via Worldwide Infrastructure Security Reports, Threat Intelligence briefs, and specific threat profile feeds to Arbor customers.

ASERT is comprised of more than 20 experts on data and network security, malware analysis, reverse engineering, Incident Response and cybercrime. ASERT's history and knowledge of the global threat landscape is called upon by the Computer Emergency Response Teams, law enforcement, and the security operations communities of virtually all G20 nations.

Arbor’s unique visibility, in-depth experience and deep knowledge of attack behavior provides the basis for protection for both the enterprise and service provider product lines.

Arbor monitors worldwide measurement infrastructure for emerging network-borne threats

Malware
Botnets
Phishing
P2P

Researchers identify, analyze and assess threats

Behavioral Fingerprint

ATTACK:

ASERT

ASERT

Arbor uses real attack data to develop accurate, relevant protection for its Pravail product line

Figure 4
Besides Global Threat Analysis Reports, ASERT generates detailed code “signatures” of emerging malware threats, as well as anomalous traffic behavioral patterns, or “fingerprints,” indicative of advanced attack campaigns. These two types of profiles are distributed to Pravail customers via the Arbor Intelligence Feeds.

The Pravail portfolio of solutions tailors carrier-class visibility to the unique needs of enterprises. Armed with global threat profiles and attack fingerprint information, enterprise operations and security managers can more quickly and confidently identify potential threats and attacks, and help mitigate the impact of an attack. The intelligence provided by ASERT ensures the products detect the latest attacks and improves both the efficiency and effectiveness of the security team.

Pravail Visibility Acts as a Force Multiplier Against Advanced Attacks

Network operations and security staff can succeed against multi-dimensional attack campaigns only with better, real-time visibility and intelligence. Analyzing data, mostly after the fact, from incomplete point solutions will not fully protect the enterprise network.

Pravail acts as a “force multiplier,” helping make network operations and security teams the experts. Pravail brings together deep visibility into network traffic with actual enterprise workflow, policy enforcement and network management. Teams can solve problems faster, thereby reducing the risk to their business, regardless of their size, skill set and scope.

Besides the intelligence from ASERT, two components of the Pravail portfolio are Pravail Network Security Intelligence (NSI) and the Pravail Availability Protection System (APS). Pravail NSI provides the real-time visibility into network behavior. Automatically fed with intelligence from ASERT, NSI can alert operations to malware and advanced attack campaigns. But more importantly, it also provides the context for them to better understand the significance of what they are seeing and what actions to take.

Pravail APS is monitoring all inbound network traffic at the perimeter of the enterprise. APS is kept up to date with specific attack intelligence feeds provide by ASERT. These feeds can identify and block DDoS, botnets and other availability attacks. Organizations can also use internal security intelligence from NSI to inform custom attack identification and enforcement by APS. Together, they connect global, external and internal traffic attack views; map against your most important web-facing, back-end systems and monitor, alert and block attacks—all in a single platform.
Eyes All Around: Pravail Network Security Intelligence (NSI)

The Pravail NSI offers organizations one of the most comprehensive view of anomalous activities occurring in, on and around the network, including unmanaged devices that are accessing corporate resources, botnet communications and application misuse.

Based on automatic, continuously refreshed intelligence from ASERT, NSI identifies malware that may be utilized in an advanced attack.

NSI monitors the critical services and systems, as prioritized by enterprise policy, that process sensitive data and alerts security and network teams to suspicious network activities. Operations and security are given actionable intelligence regarding users, applications, services, domains and URLs for more effective response, and later forensics.

Pravail NSI Step-by-Step

1. **STEP 1**
   Deploy NSI wherever you need to analyze data. NSI collects IP flow data. This includes where traffic originated from, where it is going, who sent it and from what device.

2. **STEP 2**
   NSI analyzes that data based on alert thresholds set by the user or against attack profiles provided by the Arbor Intelligence Feeds.

3. **STEP 3**
   Create and monitor alerts to get a view of what is happening on your network and where your risks are. Identify where risks are originating, such as a user’s infected laptop that is infected with cybercrime malware or a targeted attack Trojan horse.

4. **STEP 4**
   Use the data and contextual intelligence provided by NSI to mitigate any risks. Using the previous example, this would include creating new alerts for this botnet in APS and mitigating the compromise as part of the organizational Incident Response process.
Blocking Advanced Attacks Automatically: Pravail Availability Protection System (APS)

Whether used in conjunction with Pravail NSI or standalone, Pravail APS is designed to effectively block DDoS botnets and most types of DDoS attacks at the enterprise or edge of the data center.

APS helps form a layered defense against both stealthy application-layer DDoS attacks and volumetric attacks that overwhelm network capacity. Data from APS can also be sent upstream via Cloud Signaling™ technology to trigger a carrier-based mitigation which helps stop volumetric attacks before they even reach your network.

Not only do enterprises benefit from the intelligence provided by data from Internet Service and Cloud Providers, Arbor’s Cloud Signaling™ Coalition allows enterprises to anonymously share detailed attack data from Pravail APS with their up-stream partners (ISPs) to enhance availability protection for all of their enterprise customers.

**Pravail APS Step-by-Step**

1. **STEP 1**
   Easy set up at the perimeter for detection of DDoS and botnet attacks.

2. **STEP 2**
   Pravail APS does not rely on state to detect attacks targeted at the organization. Attacks are detected using expert-developed AIF countermeasures developed by ASERT.

3. **STEP 3**
   Attacks are mitigated before reaching their enterprise network targets.

4. **STEP 4**
   Enterprise organizations can see what attacks are currently being blocked on their network with custom developed alerts. Also, if the attack is larger than the inbound pipes allow, the organization can create an attack alert that can be sent to the provider for upstream protection.
Summary

A global perspective on the extended and increasingly Internet connected enterprise network—employees, customers, partners and suppliers—has become a requirement for protecting business operations. Secure network availability across this extended network is essential to growing revenue, retaining customers and remaining competitive.

At the same time, yesterday’s malware has evolved, and cyber attackers have grown far more sophisticated. Cyber threats are now well-planned, advanced attack campaigns consisting of multiple components and phases in a lifecycle.

Arbor’s ASERT services provide unparalleled visibility and intelligence on global Internet traffic, and Arbor’s Pravail solution helps provide the context and enforcement flexibility to identify and stop advanced attacks at every stage in the lifecycle.

By integrating global intelligence into a comprehensive monitoring and protection platform, Pravail customers can more quickly and efficiently see, understand and enforce policy across the enterprise network. These capabilities act as a force multiplier, allowing operations and security to address advanced threats and reduce the risk to the enterprise.

For more information on Arbor’s Pravail solutions for enterprise network protection against malware, visit our website: www.arbornetworks.com/solutions/enterprise.

References

3. ZDNet.com, “Medicaid Hacked: Over 181,000 Records and 25,000 SSNs Stolen,” April 8, 2012.