DDoS SPECIAL

CIO Review

CIOREVIEW.COM
NOVEMBER 20 - 2015

Company of the Month

David Williamson, CEO
EfficientIP

LookingGlass Cyber Solutions

Integrating DNS Defense and Intelligence Driven Security

Chris Coleman,
CEO

$ 15US

CIO REVIEW
44790, S Grimmer Blvd.
#202, Fremont, CA-94538

CIO Review 20 MOST PROMISING DDoS SOLUTION PROVIDERS - 2015

Integrating DNS Defense and Intelligence Driven Security

By Judy Cristin

A full-fledged investigation is underway at a telecommunications internet service provider—despite the provider's network having normal Internet traffic from their supported customer networks, a few of their public Internet facing authoritative Domain Name Servers (DNS) are receiving high, inbound processing loads at arbitrary intervals. It didn't take long for the network engineers to unravel the cause—a Distributed Denial of Service (DDoS) attack against their DNS infrastructure resulting in slow response times or network resolutions becoming unavailable.

While globally considered a significant threat to today's enterprises, the impacts that most concern CIOs about unrelenting DDoS attacks are the potentially crippling financial losses and the tarnished brand reputation. The recent 'State of the Internet' report by Akamai supports concerns about the DDoS attack dilemma by highlighting the fact that, "For the past three quarters, there has been a doubling in the number of DDoS attacks year over year." In a world of increasing threats, the ultimate challenge for enterprises and service providers is to stop cyber-attacks early before they cause harm.

Chris Coleman, CEO

> "Our solutions are distinctively architected to discover, understand, manage, and mitigate threats both inside and outside an organization's infrastructure in an effective and efficient way

Offering unparalleled visibility into the threats that exist across the Internet, LookingGlass Cyber Solutions' unique portfolio of threat intelligence-driven solutions effectively combats the cyber challenge. Befitting the name and by focusing a threat intelligence lens on the challenge, the CEO of LookingGlass, Chris Coleman states, "Our solutions are distinctively architected to discover, understand, manage, and mitigate threats both inside and outside an organization's infrastructure in an effective and efficient way".

Having more than two decades of rich leadership experience with cutting edge cyber security technology, Coleman discusses the way the firm's product portfolio allows security professionals to gain an understanding of the overall threat landscape, the threats specific to a customer's public infrastructure, and the risks exposed by third party relationships. He highlights that the firm's architecture and product portfolio addresses the full scope required to collect mass Internet intelligence and threat data, aggregate, correlate, and manage that information. To mitigate threats, their solutions then deliver that information into network defense solutions, specifically DNS Defender-which is critical to not only protecting an infrastructure from DDoS attacks but also blocking communication with known malicious command and control servers.

The First Line of Defense

In the industry, it's often said that you can't stop threats if you don't have visibility of the threat landscape including potential risks posed by your third parties. With their outside-in perspective of the Internet and associated threats, LookingGlass has seen how the threat landscape has continued to evolve. Let's take a look at LookingGlass' threat intelligence-driven solutions to understand how these solutions can provide cyber security advantages.

As a global botnet monitoring system, LookingGlass' Virus Tracker works by reverse engineering malware and identifying the domains located on the Internet that the malware attempts to contact and communicate with. "By registering those domains before the malware authors can, or by re-registering domains after they have expired, Virus Tracker is able to masquerade as the command and control servers that control the malware communication channels," says Coleman. This information is not only collected and aggregated by their flagship ScoutVision platform but can also be ingested in a machine readable format by their DNS Defender application to shut down command and control connections as well as by protecting the customer's DNS infrastructure from malformed DNS requests and DDoS attacks against that same infrastructure. How concerning is the malware problem? Since Virus Tracker identifies more than three million new unique malware infections per day, we'd say the malware problem is very serious.

With alarming DDoS and malware statistics like these, CIOs know it's critical to leverage big data technology solutions to help their security professionals stay ahead of the challenging threat landscape. That's why many turn to ScoutVision which leverages fast, scalable technologies to gather, ingest, aggregate, normalize, enrich and analyze over 140 sources of threat data (including Virus Tracker) to create a comprehensive understanding of threat intelligence.

The threat intelligence ingested to ScoutVision is layered on top of continuous monitoring and assessment of Internet intelligence risks and activity for enhanced threat visibility and understanding. ScoutVision's back-end system continuously monitors the Internet and the public facing, advertised network space of customers, their trusted third party suppliers, and their industry peers. This outside-in perspective allows ScoutVision to identify how networks may be attacked to deliver early warning and notification of attacks targeting LookingGlass customers and their peer organizations.

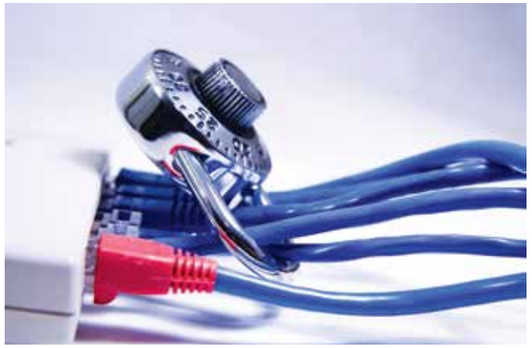
> "By registering those domains before the malware authors can, or by re-registering domains after they have expired, Virus Tracker is able to masquerade as the command and control servers that control the malware communication channels"

It's important to understand how threats are impacting an organization so to operationalize intelligence ScoutInterXect correlates network telemetry inside the organization with global threat indicators and Internet intelligence. By getting a complete view of how corporate owned assets are interacting-both historically and in real time-with threats and threat actors located beyond an organization's perimeter, incident responders and forensic investigators gain a critical outside-in perspective.

Threat Mitigation-Taking Action to Secure the Network

Over 90 percent of DDoS attacks target the DNS and the Internet DNS servers which can result in significant loss of connectivity. DNS servers operate on well-known ports that are always kept open to respond to devices attempting to resolve domains, making it an extremely easy target.

LookingGlass addresses DDoS attacks and malware with two solutions. DNS Defender is a DNS protocol specific caching, load balancing and DNS firewall so by inserting DNS Defender in front of their DNS infrastructure, organizations can help effectively mitigate DNS DDoS attacks.



During a 2013 DDoS attack, a telecommunications and Internet service provider decided to install DNS Defender in their data center. "During this period, they were able to see botnet attacks pass through their infrastructure and DNS Defender successfully blocked those attacks, preventing any further performance impact on the DNS servers," affirms Coleman.

The Dynamic Threat Defense solution integrates DNS Defender with ScoutVision to prevent the first contact between a spear phishing email or a malware infected host and the command and control server located on the Internet by eliminating the DNS resolution. With automated threat detection via ScoutVision, organizations are able to migrate from a manual rules provisioning process to comprehensive, automated threat mitigation for thousands of rules without administrator's involvement.

The firm's Dynamic Threat Defense (DTD) solution stops malware outbreaks, spear phishing attacks, and drive-by-downloads by integrating Scout Vision's machine-readable threat intelligence (MRTI) with the protocol-specific DNS firewall as an integrated network security solution. The DTD solution offers granular policy enforcement with malicious domain tagging, blocking, URL redirection, and logging—complete with an integrated suite of DNS management and analytic tools. DTD delivers superior protection while overcoming the cumbersome integration challenges of multi-vendor mitigation solutions based on traditional firewalls.

> "Our mission is to deliver the most advanced and comprehensive threat intelligence driven solutions so security teams have the best chance of finding and mitigating threats early before they do damage"

The Edge

Offering both cloud based and on-premises solutions, LookingGlass extends its global sales, marketing, and professional services capabilities through its experienced and valued channel and system integration partners. Through its ScoutConnected Partner Program, the company enables partners to integrate complementary security capabilities with the ScoutVision platform. ScoutConnected provides the technical interfaces based on OpenTPX—API, structure, schema—and training to enable third party threat and Internet intelligence to be ingested into or exported out of ScoutVision. A LookingGlass contribution to the open source community, OpenTPX is a comprehensive framework to share machine-readable threat intelligence combining network security operations data with threat intelligence, analysis and scoring data at Internet performance and scale. The threat data is then processed and prioritized to create actionable threat intelligence that customers can use directly or feed into other security information and event management tools or network appliances.

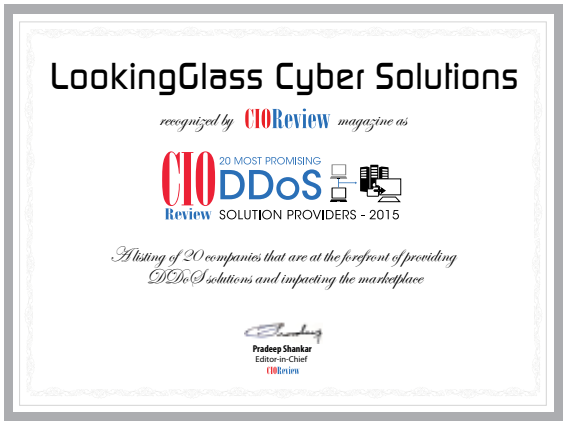
LookingGlass' public and private partnerships enable exclusive access to some of the largest DDoS sensor networks in the world which is useful in identifying ongoing DDoS attacks. This Threat Intelligence Analysis and Management coupled with Dynamic Threat Defense continue to bring in critical advantages across multiple sectors such as financial services, healthcare, government and telecommunications.

"Our mission is to deliver the most advanced and comprehensive threat intelligence driven solutions so security teams have the best chance of finding and mitigating threats early before they do damage," affirms Coleman. CR

CIOReview
The Navigator for Enterprise Solutions
DDOS SPECIAL NOVEMBER- 20- 2015 CIOREVIEW.COM

20 Most Promising DDoS Solution Providers 2015

As the Internet continues to grow and prosper, hacker attacks continue to increase in severity and frequency. Today, the technologies and applications distributed across the diverse enterprise environments are inviting multiple types of security issues, with Distributed Denial of Service (DDoS), being the major one. There has been a phenomenal rise in the DDoS attacks over the past several years. The methods and techniques being used for DDoS attacks are evolving, with attackers looking for new ways of 'freezing' their victims' operations. Further the lack of attack information, along with non-standard evaluation and testing approaches are hindering an effective prevention of DDoS attacks. In this scenario, companies are adopting multiple measures to mitigate threats. But, beyond having the right protective systems in place and ensuring sufficient overflow capacity is available, an effective strategy depends on an active, well-informed incident response. It's also important to work with a DDoS mitigation service to plan and prepare, so that the enterprises are ready to respond effectively in case of any attack. There are scores of solution providers in the market offering denial of service mitigation and prevention solutions with multiple features including high-speed border filtering, deep packet inspection to distinguish between spoofed and legitimate traffic, and more. To simplify and help CIOs navigate the DDoS solutions landscape, CIO Review presents a special edition on DDoS. A distinguished panel comprising of CEOs, CIOs, VCs, analysts including CIO Review editorial board has decided the "20 Most Promising DDoS Solution Providers 2015" in the U.S., listing the best vendors and consultants who provide key technology solutions and services related to DDoS.



Company:
LookingGlass

Description:
LookingGlass Cyber Solutions is the leader in threat intelligence and dynamic threat defense with the most extensive sources of threat and Internet intelligence plus intelligence-driven network security and threat mitigation.

Key Person:
Chris Coleman, CEO

Website:
lgscout.com