Global Cyber Intelligence

Near Real-Time Global Border Gateway Protocol Insights

Attacks against Border Gateway Protocol (BGP) are becoming a frequent, preferred method for advanced attackers to steal passwords and interrupt communications. Adversaries can use man-in-the-middle (MitM) tactics and other attack vectors to exploit BGP routing, including impersonating trusted sources to obtain certificates, stealing valuable data, adding malicious implants into the seemingly normal traffic, eavesdropping, and analyzing traffic. Additionally, adversaries can deploy denial-of-service or black-holing attacks, create detours through malicious networks, or hijack traffic away from legitimate hosts to one controlled by the attacker.

SAIC's Global Cyber Intelligence (GCI) services deliver the internet's BGP data in near real-time and augment it with analytics to identify when adversaries are attempting to deploy these types of attacks. GCI delivers immediate alerts on malicious or suspicious activity, as well as timely bulletins, reports, and summary data for customers to operationalize their BGP data and proactively protect themselves from cyber-attacks.

SAIC®

"DEFENDING FORWARD" IS BECOMING INCREASINGLY CRITICAL AS ATTACKS INCREASE IN SOPHISTICATION. WE CAN NO LONGER BE REACTIVE, WAITING FOR AN ADVERSARY TO HIT OUR PERIMETER.

Capability Highlights

- The only solution that delivers the entire internet's BGP data in tactically useful timeframes
- Access to BGP data from the largest number of core internet peering points
- Unmatched speed of delivery with verified accuracy
- Availability of indexed and non-indexed internet routing tables (darknet)
- Provides the richest BGP data of your prefixes
- Provides streaming data focused to areas of responsibility
- Alert analytics delivery that can be incorporated into any SIEM environment
- Visualization tool for seeing routing changes
- A hosted analytics platform to allow full exploration of the data
- Automated- and data scientist-supported bulletins with analysis of alerts or anomalous conditions

PROOF OF CONCEPT

In 2020, SAIC conducted a proof-of-concept with a branch of the military to demonstrate the value of GCI in providing the ability to see and defend the enterprise by seeing suspicious and nefarious actions in "gray" space. SAIC identified multiple instances of malicious attacks against military subnets, including the use of bogons and man-in-the-middle attacks, as well as thousands of cases of data routing from a blacklisted country. Without SAIC's visibility into the internet's BGP data, these incidents may have gone undetected.

GCI collects BGP data from numerous peering points on five continents and compares it with data from other sources to ensure accuracy. The global extent of this data provides analysts with an understanding of cyberspace critical infrastructure and visibility of adversarial assets and activity. Defensive Cyber Operators (DCO) can use the GCI alerts to rapidly counter attacks. Offensive Cyberspace Operations (OCO) analysts can extend these capabilities to disrupt our adversaries in a non-attributable way. With our geospatial visualization tool, customers can explore how their traffic transits across the internet, a vital capability for high-priority missions.

GCI provides the stream of BGP data directly to customers so they can fuse with other datasets and perform their own analysis. The stream can be split into subsets of data so analysts can focus on the routes relating to their area of responsibility. In addition, we provide a comprehensive analytics platform to identify anomalies and execute alerts and reports. Analytic methods range from explicit rules identifying categories of anomalous routes or prefix announcements, to the identification of illegitimate autonomous systems, to studies of large-scale traffic bursts to understand underlying patterns. GCI alerts and reports give the exact nature of anomalies, enabling operators to take immediate action without further investigation.

While there is good visibility on data transiting your own networks, visibility vanishes once the packet enters the open internet, compromising the integrity of communication. SAIC's GCI addresses this by:

- Providing timely, high-resolution visibility of your traffic routes on the open internet for enhanced cyber operations planning and execution
- Detecting and reporting surreptitiously rerouted traffic adversaries can collect to deny communications or execute Denial of Service (DoS) attack
- Alerting on traffic routed through hostile countries or bogus Autonomous Systems
- Categorizing successive route changes with adversary actions
- Supporting attribution investigations
- Monitoring blacklisted sites
- Detecting BGP reroutes that cause latency and disruption
- Supporting black hole identification and investigation
- Supporting risk analysis aligning routes to adversary locations with vulnerabilities and known exploits
- Conducting risk assessment for planned and on-going operations
- Supporting the identification of spoofed TCP/IP data from an adversary, improving defense and forensic analysis
- Providing verifiable data for carrier accountability of Service Level Agreements

Contact

Russell Smith
703.676.4398
russell.j.smith@saic.com

Nancy Wright Grady, PhD
865.604.6733
nancy.w.grady@saic.com

Arthur Wachdorf
210.789.0707
arthur.l.wachdorf@saic.com

21-0401