CODEGUARDIAN™

POWERED BY

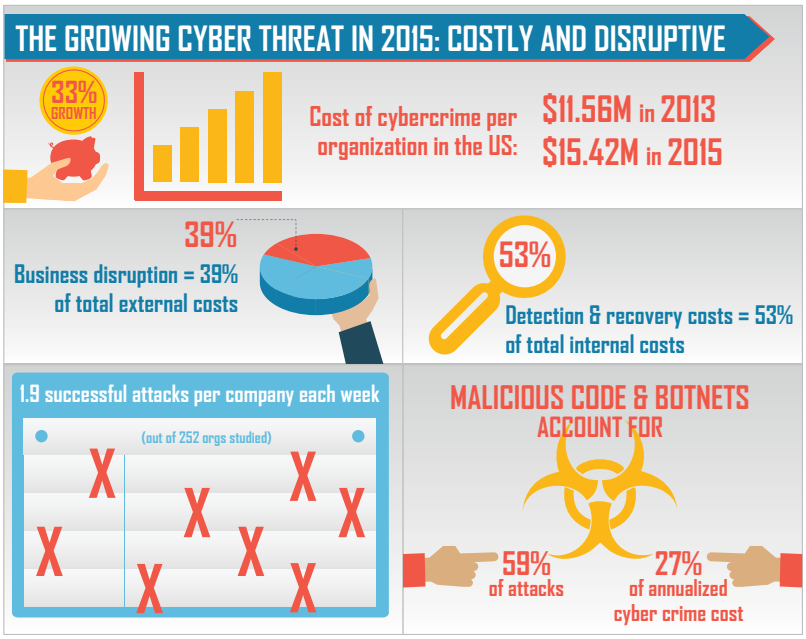
LGS INNOVATIONS

LISTEN · INNOVATE · DELIVER™

LGSCODEGUARDIAN.COM

Software Integrity to Secure Network Assets

Network hacks, data breaches, information theft, and other malicious network attacks are on the rise – and so is concern for overall network security strategy. Nearly one million malware threats are released worldwide every day, and it takes an average of 46 days to resolve a malicious attack, threatening critical operations, organizational reputations, and even the financial viability of many companies. Given the potential repercussions surrounding network attacks, it is imperative that organizations deploy a proactive, defense-in-depth strategy that addresses all layers of the network.



Source: Ponemon Institute, 2015 Cost of Cyber Crime Study: Global

LGS Innovations recognizes the importance of network-level software integrity as a component of the larger network security ecosystem. With a dedication to the evolution of enterprise support born from extensive experience deploying secure, mission-critical switching solutions, LGS Innovations offers CodeGuardian™: a solution that hardens network devices at both the software source code and binary executable levels to enhance overall network security.

Staying Secure in an Evolving Environment

Modern day netwrok-centric devices are customized embedded computers, and the software running on them is not protected by traditional IT security mechanisms such as virus scanners. This leaves routers and switches susceptible to the introduction of malware and other attacks, potentially causing:

- Compromise of network connectivity (including rejecting or redirecting traffic)
- Opening of the network to further attacks by compromising security policy on the network
- Exposure of the network to theft of sensitive data
- Interruption or corruption of network traffic
- Blocking of all traffic by rendering the network hardware inoperable

The LGS CodeGuardian solution mitigates larger enterprise risks at the source, enabling an enhanced security profile through:

- Independent verification and validation of source code
- Software diversification to prevent exploitation
- Secure delivery of software to LGS customers

While the telecommunications industry's growing reliance on a global software production process has raised questions about the software chain of custody and potential vulnerabilities introduced along the chain, CodeGuardian protects networks from intrinsic vulnerabilities, code exploits, embedded malware, and potential back doors that could compromise mission-critical operations. CodeGuardian promotes a proactive, defense-in-depth approach toward network security that continuously defines and implements value-add capabilities to address both current and future threats.

Independent Verification and Validation (IV&V) and Analysis of Source Code

CodeGuardian technology uses a proactive security approach through IV&V and operational vulnerability scanning and analysis of switch software within the network equipment portfolio, reviewing the source code for:

- Equipment software vulnerabilities: bugs and flaws contained in software, recommended and default system configuration, processes/best practices, and system documentation.
- System exploits: concepts or code that take advantage of vulnerabilities to gain initial access to the operations of a system.
- Embedded malware: code loaded onto a system to inflict damage, collect data, change the functioning of the system, or launch attacks at other systems.
- Back doors in software: code intentionally designed into a system that bypasses normal authentication checks in order to give access or control. Examples include field debugging capabilities, secret key strokes, special login sequences, or hidden login user IDs

CodeGuardian IV&V and vulnerability analysis addresses external interfaces such as:

- HTTPS Interface
- Login Interface
- NTP Interface
- Command Line Interface
- IP Port Usage
- SNMP Interface
- Data Packet Interface

Software Diversification to Prevent Exploitation

CodeGuardian technology also implements software diversification to randomize the executable program address space so that various instances of the same software, while functionally identical, are arranged differently on the binary level, making any address-dependent exploits ineffective on other diversified instances of the software. This prevents attackers from:

- Gaining access to information (data theft)
- Performing unauthorized actions or commands (privilege escalation)
- Preventing routine operation of a system (e.g. Denial-of-Service (DoS))

In order to perform an exploit against a target, an attacker will typically take advantage of a vulnerability in a system, which often requires knowledge of the underlying address layout of an application. CodeGuardian's diversification process mitigates this risk by analyzing and modifying the position of application components, thereby reducing the effectiveness of attacks based on the address layout of a standard, non-diversified version of the software.

Assured Supply Chain

To help ensure a secure software supply chain, CodeGuardian maintains a secure lab environment with an air-gapped network and restricted access. The secure lab has a complete build environment with source control, toolchain, build machines, and testing facility. The secure lab environment ensures the software that goes through the CodeGuardian analysis process is the same software delivered unaltered to the end customer through LGS distribution channels.

CODEGUARDIAN™

About LGS Innovations

LGS Innovations delivers mission-critical communications products, R&D, and supporting services to U.S. defense, intelligence, and civilian agencies, state and local governments, critical infrastructure operators, and commercial customers around the world. We create advanced solutions in wireless communications, signals processing and analysis, optical networking, photonics, routing and switching, and spectrum management.

These solutions drive mission success in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), cyberspace operations, and network assurance. By incorporating best-in-class commercial and custom technologies with a full suite of offerings in research and development, engineering, integration, and product applications, our solutions improve efficiency, reduce costs, and provide an information advantage to our customers.

LGS has a history and culture of innovation, and maintains strong ties to our Bell Labs legacy of inventive development. Our intellectual curiosity keeps us on the cutting edge of technology and leverages our 75-year history of creating next-generation communications solutions to support critical operations.

LGS Innovations is a U.S.-owned company headquartered in Herndon, Virginia, with offices across the U.S. and overseas. We employ more than 1,000 associates around the world, including 750 scientists and engineers. Do you have a passion for innovation? So do we. Learn more at www.lgsinnovations.com.

LGS INNOVATIONS

LISTEN · INNOVATE · DELIVER™

LGS INNOVATIONS
13665 Dulles Technology Drive, Suite 150
Herndon, VA 20171

TEL: 1-866-LGS-4243 (1-866-547-4243)
URL: www.lgsinnovations.com