ITL BULLETIN FOR MAY 2017

CYBER-THREAT INTELLIGENCE AND INFORMATION SHARING

Chris Johnson, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

Cyber-attacks continue to increase in frequency and sophistication, presenting significant challenges for organizations that must defend their data and systems from capable threat actors. These actors range from individual, autonomous attackers to well-resourced groups operating in a coordinated manner as part of a criminal enterprise or on behalf of a nation-state. Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. Given the risks these threats present, it is increasingly important that organizations share cyber-threat information, and use the community's experience to improve their security posture.

Cyber-threat information is any information that can help an organization to identify, assess, monitor, and respond to cyber-threats. Examples of cyber-threat information include indicators (system artifacts or observables[2] associated with an attack), TTPs, security alerts, threat intelligence reports, and recommended security tool configurations. Most organizations already produce multiple types of cyber-threat information that are available to share internally as part of their information technology and security operations efforts.

By exchanging cyber-threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber-threat information from multiple sources, an organization can also enrich existing information and make it more actionable. This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information through the reduction of ambiguity and errors. Organizations that receive threat information and subsequently use this information to remediate a threat confer a degree of protection to other organizations by impeding the threat's ability to spread. Additionally, sharing of

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.
[2] An *observable* is an event (benign or malicious) on a network or system.

cyber-threat information allows organizations to better detect campaigns that target industry sectors, business entities, or institutions.

NIST has published Special Publication (SP) 800-150, Guide to Cyber-Threat Information Sharing, to assist organizations in establishing and participating in cyber-threat information sharing relationships. The publication describes the benefits and challenges of sharing, clarifies the importance of trust, and introduces specific data handling considerations. To show how sharing and coordination can increase the efficiency and effectiveness of an organization's cybersecurity capabilities, NIST SP 800-150 presents some scenarios that describe threat information sharing in real-world applications.

The goal of the new publication is to provide guidelines that improve cybersecurity operations and risk management activities through safe and effective information sharing practices, and help organizations to plan, implement, and maintain information sharing.

Basics of Cyber-Threat Information Sharing

NIST SP 800-150 introduces basic cyber-threat information sharing concepts including types of cyber-threat information and common terminology. The publication also examines potential uses for shared cyber-threat information and explores the benefits and challenges of threat information sharing.

Threat information is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include the following:

- ***Indicators*** are technical artifacts or observables that suggest an attack is imminent or is currently underway or that a compromise may have already occurred.
- ***Tactics, techniques, and procedures (TTPs)*** describe the behavior of an actor.
- ***Security alerts*****,** also known as advisories, bulletins, and vulnerability notes, are brief, usually human-readable, technical notifications regarding current vulnerabilities, exploits, and other security issues.
- ***Threat intelligence reports*** are generally prose documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organization. Threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.
- ***Tool configurations*** are recommendations for setting up and using tools that support the automated collection, exchange, processing, analysis, and use of threat information.

The primary goal of the publication is to foster similar threat information sharing practices across organizational boundaries – both acquiring threat information from other organizations, and providing internally-generated threat information to other organizations.

Threat information sharing provides access to threat information that might otherwise be unavailable to an organization. Using shared resources, organizations can enhance their security posture by leveraging the knowledge, experience, and capabilities of their partners in a proactive way. Allowing "one organization's detection to become another's prevention"[3] is a powerful paradigm that can advance the overall security of organizations that actively share threat information.

Organizations that share cyber-threat information will benefit by gaining situational awareness, which will, in turn, help to improve security posture and risk management practices. As seemingly unrelated observations are shared and analyzed, those can be correlated with data collected by others, helping to mature community knowledge. This improved community understanding helps organizations to remain better informed about changing TTPs and how to rapidly detect and respond to threats. Such agility creates economies of scale for network defenders while increasing actors' costs by forcing them to develop new TTPs.

While sharing threat information clearly has benefits, certain challenges remain. Some challenges that apply both to consuming and to producing threat information are:

- Establishing trust;
- Achieving interoperability and automation;
- Safeguarding sensitive information;
- Protecting classified information; and
- Enabling information consumption and publication.

NIST SP 800-150 identifies several information challenges that apply only to the consuming of threat information and other challenges that apply only if an organization wants to provide its own information to other organizations.

Establishing Sharing Relationships

NIST SP 800-150 recommends the following planning and preparation activities in relation to launching a threat information sharing capability:

- Define the goals and objectives of information sharing;
- Identify internal sources of threat information;
- Define the scope of information sharing activities;

[3] This phrase, which has been used in numerous presentations and discussions, was formulated by Tony Sager, Senior VP and Chief Evangelist, Center for Internet Security.

- Establish information sharing rules;
- Join a sharing community; and
- Plan to provide ongoing support for information sharing activities.

Throughout this process, organizations are encouraged to consult with subject matter experts both inside and outside their organization. Such sources include:

- Experienced cybersecurity personnel;
- Members and operators of established threat information sharing organizations;
- Trusted business associates, supply chain partners, and industry peers; and
- Personnel knowledgeable about legal issues, internal business processes, procedures, and systems.

An organization should use the knowledge and experience from these experts to help shape a threat information sharing capability that supports its mission and operates under its security, privacy, regulatory, and legal compliance requirements. Due to constantly changing risks, requirements, priorities, technology, and/or regulations, this process will often be iterative. Organizations should reassess and adjust their information sharing capabilities as needed based on changing circumstances. Such a change may involve repeating some or all the planning and preparation activities listed above.

Many organizations handle information that, by regulation, law, or contractual obligation, requires protection. This includes personally identifiable information (PII), controlled unclassified information (CUI), and other sensitive information afforded protection under the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the Health Information Portability and Accountability Act (HIPAA), the Federal Information Security Modernization Act (FISMA) of 2014, the Gramm-Leach-Bliley Act (GLBA) and other legislation, regulations, and guidelines. Organizations should identify and properly protect such information. An organization's legal team, privacy officers, auditors, and experts familiar with the various regulatory frameworks should be consulted when developing procedures for identifying and protecting sensitive information.

Participating in Sharing Relationships

NIST SP 800-150 provides guidance about how an organization's participation in an information sharing community will help to achieve the benefits described above. Several subsections explain sharing activities to consider, including:

- Engage in ongoing communication;
- Consume and respond to security alerts;
- Consume and use indicators;
- Organize and store indicators; and
- Produce and publish indicators.

Organizations just starting their threat information sharing efforts should initially choose one or two activities to focus on and then consider adding activities as their information sharing capability matures. Organizations should understand that threat information sharing *augments* — not replaces — an organization's fundamental cybersecurity capabilities, regardless of the maturity of their information sharing practices.

Ongoing Support for Information Sharing Activities

NIST encourages greater sharing of cyber-threat information among organizations, both in acquiring threat information from other organizations and in providing internally-generated threat information to other organizations. Implementing the recommendations that are described in the new publication enables organizations to make more efficient and effective use of information sharing capabilities.

To make cyber-threat information sharing process and procedures effective, they should be integrated into the organization's system life cycle. Each organization should provide ongoing support for information sharing activities. For this purpose, an organization should establish an information sharing plan. The plan should address the collection and analysis of threat information from both internal and external sources and the use of this information in the development and deployment of protective measures. A sustainable approach is necessary to ensure that resources are available for the ongoing collection, storage, analysis, and dissemination of cyber-threat information.

NIST SP 800-150 emphasize the importance of using standardized data formats and transport protocols to share cyber-threat information that makes it easier to automate threat information processing. The use of automation enables cyber-threat information to be rapidly shared, transformed, enriched, analyzed, and acted upon with less need for manual intervention.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov