Information & Security: An International Journal

Vasil Rizov, v.39:1, 2018, 43-50 https://doi.org/10.11610/isij.3904

INFORMATION SHARING FOR CYBER THREATS

Vasil RIZOV

Abstract: An organization that has faced an attack acquires valuable information on cyber threats that may be shared with others. This information can help an organization to identify, assess, monitor, and respond to cyber threats. Organizations that share cyber threat information can improve their own security postures as well as those of other organizations. Information sharing among private and public entities is a powerful mechanism to better understand a constantly changing environment and learn in a holistic way about serious risks, vulnerabilities and threats, as well as solutions.

This article provides a review of the benefits and challenges of coordinating and sharing cyber threat information, the strengths and weaknesses of different information sharing models, and the importance of building trust between actors and handling sensitive or classified information. Organizations have to establish information sharing goals and scope of information sharing activities, identify cyber threat information sources, develop rules that control the distribution of threat information, and make effective use of threat information in support of their overall cyber security practices.

Keywords: cyber security, cyber threat, information sharing, information security, classified information.

Introduction

The high-profile cyberattacks of the last two years appear to be indicative of a broader trend: the frequency and ferocity of cyberattacks are increasing. While considerable debate exists with regard to the best strategies for protecting various cyber systems and promoting cyber security, one point of general agreement amongst cyber security actors is the perceived need for enhancement and timely exchange of information concerning cyber threats.

This article will review the benefits and challenges of coordinating and sharing the cyber threat information, the strengths and weaknesses of different information sharing models, and the importance of building trust between actors, as well as the handling of sensitive or classified information.

What is threat information? Threat information is any information related to a threat that might help an organization for protecting itself against a threat or detect the activities of potential or actual threat actor.

A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the government through an information system via unauthorized access, destruction, disclosure, or modification of information, and denial of service.

In this respect, cyber threat information is any information that can help an organization identify, assess, monitor, control, and respond to cyber threats.

An organization that has faced an attack holds as a sequence of that attack valuable information to share with others. Information sharing between private and public stakeholders is a powerful mechanism for better understanding of the constantly changing environment and for learning in a holistic way about serious risks, vulnerabilities and threats, as well as solutions to them.

The purpose of this study is to help organizations establish information sharing goals, scope information sharing activities, identify cyber threat information sources, develop rules that control the distribution of threat information, and make an effective use of threat information in support of their overall cyber security practices.

Organizations that share cyber threat information can improve their own security postures as well as those of other organizations. By sharing cyber threat information, organizations can identify the types of systems and information being targeted, the techniques used to gain access and, what is even more important – indicators of compromise. This is important both within the private sector and between the private sector and the government.

Threat information sharing provides access to threat information that might otherwise be unavailable to an organization. Using shared resources, organizations are able to enhance their security posture by leveraging the knowledge, experience, and capabilities of their partners in a proactive way. The approach, where *one organization's detection becomes another's prevention*, is a modern sophisticated concept that strengthens the organizations' security in advance.

An organization can use shared threat information in many ways. Some uses are operationally oriented, such as updating enterprise security controls for continuous monitoring with new indicators and configurations so they can detect the latest attacks and compromises. Others are strategically oriented, such as using shared threat information as inputs when planning major changes to an organization's security architecture.

Threat information exchanged within communities which are organized around the finance sector can be particularly beneficial because the member organizations often face actors that use common Tactics, Techniques, and Procedures (TTPs) which target the same types of systems and information. Cyber defense is most effective when organizations collaborate successfully to deter and defend against well-organized, capable actors. By working together, organizations can also build and sustain trusted relationships that are the foundation of secure, responsible, and effective information sharing.

These are some of the *benefits* of cyber threat information sharing:

- *Shared Situational Awareness.* Information sharing enables organizations to leverage the collective knowledge, experiences, and analytic capabilities of their sharing partners within a community of interest, thereby enhancing the defense capabilities of multiple organizations. Even a single contribution – a new indicator or observation about a threat actor – can increase the awareness and security of an entire community.
- *Enhanced Threat Understanding.* By developing and sharing threat information, organizations gain a better understanding of the threat environment and are able to use threat information to inform their cyber security and risk management practices. Using shared information, organizations are able to identify affected platforms or systems, implement protective measures, enhance detection capabilities, and more effectively respond and recover from incidents based on observed changes in the current threat environment.
- *Knowledge Maturation.* When seemingly unrelated observations are shared and analyzed by organizations, they can be correlated with data collected by others. This enrichment process increases the value of information by enhancing existing indicators and by developing knowledge of threat actor TTPs that are associated with a specific incident, threat, or threat campaign. Correlation can also impart valuable insights into the relationships that exist between indicators.
- *Herd Immunity.* The principle of herd or community immunity comes from biology, where it refers to protecting a community from a disease by vaccinating many, but not all, of its members. Similarly, organizations that act upon the threat information they receive by re-mediating threats to themselves afford a degree of protection to those who are yet unprotected (i.e., who have either not received or not acted upon the received threat information) by reducing the number of viable attack vectors for threat actors, thus reducing vulnerability.

- *Greater Defensive Agility.* Actors continually adapt their TTPs to attempt to evade detection, circumvent security controls, and exploit new vulnerabilities. Organizations that share information are often better informed about changing TTPs and can rapidly detect and respond to threats, thereby reducing the probability of successful attack. Such agility creates economies of scale for network defenders while increasing the costs of actors by forcing them to develop new TTPs.

Major *types of cyber threat information* include: indicators of compromise; tactics, techniques, and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents.

- *Indicators* are technical artefacts or observables (an observable is an event, benign or malicious, on a network or system) that suggest an attack is imminent or is currently under way, or that a compromise may have already occurred. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, or the suspicious Domain Name System (DNS) domain name.
- *Security alerts*, also known as bulletins, advisories, and vulnerability notes, are brief, usually human-readable, technical notifications regarding current vulnerabilities, exploits, and other security issues. Security alerts could originate from sources such as the Bulgarian Computer Emergency Readiness Team (GOVCERT-BG), Information Sharing and Analysis Centres, other Security Incident Response Teams (SIRTs), commercial security service providers, and security researchers.
- *Tactics, techniques, and procedures* describe the behaviour of an actor. Tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor's tendency to use a specific malware, attack tool, or delivery mechanism.
- *Tool configurations* are recommendations for setting up and using tools that support the automated collection, exchange, processing, analysis, and use of threat information. For example, tool configuration information could consist of instructions on how to install and use a rootkit detection and removal utility, or how to create and customize intrusion detection signatures, router access control lists (ACLs), firewall rules, or web filter configuration files.
- *Threat intelligence reports* are generally documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organi-

zation. Threat intelligence is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making processes.

Many organizations already produce and share threat information internally. For example, an organization's security team may identify malicious files on a compromised system when responding to an incident and produce an associated set of indicators (file names, sizes, and hash values). These indicators are then shared with system administrators who configure security tools, such as host-based intrusion detection systems, to detect the presence of these indicators on other systems. Likewise, the security team may launch an email security awareness campaign in response to an observed rise in phishing attacks within the organization.

Among these practices for information sharing within an organization it is important 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.

While there are clear benefits to sharing threat information, there are also a number of challenges to consider when participating in cyber threat information sharing:

- *Establishing Trust.* Nothing else but the trust is at first. Trusted relationships form the basis for information sharing but require effort to establish and maintain. Ongoing communication through regular in-person meetings, phone calls, or social media can help accelerate the process of building trust.
- *Achieving Interoperability.* Standardized data formats and transport protocols are important building blocks for interoperability and help enable the secure, automated exchange of structured threat information among organizations, repositories, and tools.

  Adopting specific formats and protocols, however, can require significant time and resources, and the value of these investments can be reduced if sharing partners require different formats or protocols.

- *Protecting Sensitive but Unclassified Information.* Disclosure of sensitive information, such as intellectual property, trade secrets, or other proprietary information can result in financial loss, violation of sharing agreements, and loss of reputation. The unauthorized disclosure of information may disrupt an ongoing investigation, jeopardize information needed for future legal proceedings, or disrupt response actions such as botnet takedown operations. Organizations should apply handling designations to shared information and implement policies, procedures, and technical controls to actively manage the risks of disclosure of sensitive but unclassified information.

- *Protecting Classified Information.* Information received from government sources may be marked as classified, making it difficult for broader number of organizations to use. It is also expensive and time-consuming for organizations to request and maintain the clearances needed for ongoing access to classified information sources. In addition, many organizations employ non-Bulgarian citizens without security clearances. Some of them originate from countries that are not part of an Agreement on the mutual protection on classified information, and are not permitted access to classified information.

There are many reasons why entities may opt not to participate in cyber information sharing, including the potential liability that could result from sharing internal cyber threat information with other private companies or the government.

More broadly, the legal issues surrounding cybersecurity information sharing – whether it is with regard to sharing between two private companies or the dissemination of cyber intelligence within the government are complex.

It is important to create a legal framework for sharing cyber information. The issues of *what*, *with whom*, and *for what* (for what purposes) that information can be shared are necessary to be defined. Also, it is necessary to determine the whole scope and overall goals of cyber security legislation itself.

Clarifying Which Government Agency Leads the Efforts on Cyber Information Sharing

Once a legislative proposal has generally authorized broader cyber security information sharing between the public and private sectors, the legislation may need to resolve what entity in the government needs to be the liaison between the public and private sector with regard to such information sharing.

While currently GOVCERT-BG serves as the central repository and distributor of cyber intelligence for the government agencies, the State Agency for National Security (SANS) should serve as the entity that receives classified information related to cyber security.

Increasing the Amount and Quality of Government Cyber Information Disclosed to the Private Sector

Beyond clarifying the government authority which is tasked with receiving and disseminating cyber information, another central issue for cyber security proposals is ensuring that the underlying information which is disseminated by the government is both extensive and helpful. While the government has wide authority to disclose cyber intelligence within its possession, that authority is not limitless and is necessarily tied to laws such as Classified Information Protection Act and the Penal Code that

restrict the government's ability to release sensitive information within its possession. More broadly, delays in the dissemination of cyber intelligence arguably may severely diminish the effectiveness of such information.

To increase the speed at which cyber threat information is distributed and the volume of cyber intelligence that is disclosed, *two main strategies* are contemplated by various cybersecurity proposals.

First, cybersecurity legislation should require the government to create capabilities to distribute cyber intelligence in "real time" to other government agencies and even to the private sector. For example, this could be establishing real time or instantaneous "automated" distribution of cyber information being facilitated through the creation of a universal electronic format for cyber information.

Second, authorizing additional access to classified cyber intelligence within the possession of the government by the private sector. For example, the Security Council to mandate SANS for establishing procedures to allow the intelligence community to share classified cyber threat intelligence with the private sector, requiring the issuance of security clearances for those who may need access to cyber intelligence.

Risks, vulnerabilities and threats are global. Actually, sharing of information at national level does not fully address the problem. As governments develop effective information exchanges at national level, they pave the way for wider collaboration and deployment at international level.

The private sector is encouraged to be more transparent and to share information responsibly, to use information sharing to improve security voluntarily in order to avoid regulatory interest and strong regulatory action which might be counter-productive.

Academia and research could work to identify, describe, and quantify the benefits and costs of participating in such information sharing platforms.

Cyber defense will be most effective when organizations collaborate successfully to deter and defend against well-organized, capable actors. By working together, organizations can also build and sustain trusted relationships that are the foundation of secure, responsible, and effective information sharing.

Notes

1. Christopher S. Johnson, Mark L. Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150, October 2016, accessed April 4, 2018, https://doi.org/10.6028/NIST.SP.800-150.

2. Paul Chichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide," NIST Special Publication 800-61, Revision 2, August 2012, accessed April 4, 2018, https://doi.org/10.6028/NIST.SP.800-61r2.
3. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 2014, accessed April 2, 2018, www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
4. Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, CRS Report R43941 (Washington, D.C.: Congressional Research Service, March 16, 2015), accessed April 2, 2018, https://fas.org/sgp/crs/intel/R43941.pdf.
5. *National Cyber Security Strategy "Cyber Resilient Bulgaria 2020,"* adopted by the Council of Ministers of Republic of Bulgaria with Decision # 583 of 18 July 2016.
6. George Sharkov, "From Cybersecurity to Collaborative Resiliency," SafeConfig'16, Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Vienna, Austria, October 24, 2016, https://doi.org/10.1145/2994475.2994484.
7. ENISA, Symantec Inc., and Landitd Ltd., *Good Practice Guide on Information Sharing*, June 13, 2009, accessed April 4, 2018, https://www.enisa.europa.eu/publications/good-practice-guide.

About the Author

Vasil RIZOV is a security expert, researcher and consultant. With more than 25 years of experience in information and physical security, he has special interest is in human aspects of security and in cybersecurity.