IstroSec

Data Sheet

Defensive Intelligence

Nowadays, the most valuable commodity of organizations is data. The attackers are also aware of this fact, which reflects the expansion of various illegal markets and semi-public online forums that trade in personal and corporate data. By monitoring these markets and forums, it is possible to find out at what attacks the majority of the illegal hacking community is currently focusing on, what vulnerabilities they target, and what data has already been misused by attackers (internal documents, user data, etc.).

> *By entrusting the monitoring of these activities and data about your organization to IstroSec experts, you will be informed about current attacks relevant to your organization, vulnerabilities and ways to mitigate potential risk.*

Types of Intelligence

Targeted threat intelligence. Actionable intelligence feed relevant for customer organization. **Istro**Sec experts provide complex services from analysis of requirements, providing actionable threat feed and implement consumers on target organizations

Leak monitoring. **Istro**Sec experts will monitor clear web, deep web and dark web for leaks from customer organizations.

Threat briefings. **Istro**Sec experts will prepare intelligence report for top level and / or middle level management regarding current threats and exploited vulnerabilities in the wild relevant to threat profile of organization

The service contains:

- Monitoring of leaked data on clear, deep and dark web
- Providing an information channel relevant to the organization, containing up-to-date information on cyber threats on relevant verticals
- Providing actionable information on threats
- Preparation of a report for senior and middle management, containing a list of current threats and exploited vulnerabilities relevant to the organization

Report contains:

- Information on the vulnerability and how to fix it, or at least mitigate the risk of compromise, if a fix is not yet available
- The organization's data that was found leaked online
- An overview of APT groups focusing on the industry in which the organization operates and ways to mitigate the risk of compromise by these groups
- Indicators of compromise
- Tactics, techniques, and procedures of the attackers
- Recommendations of tools, configurations, and other measures to prevent current threats

European Cybersecurity Company.
Threat Intelligence. Incident Response. Cyber Advisory.

www.istrosec.com

Why Us?

Experience and knowledge

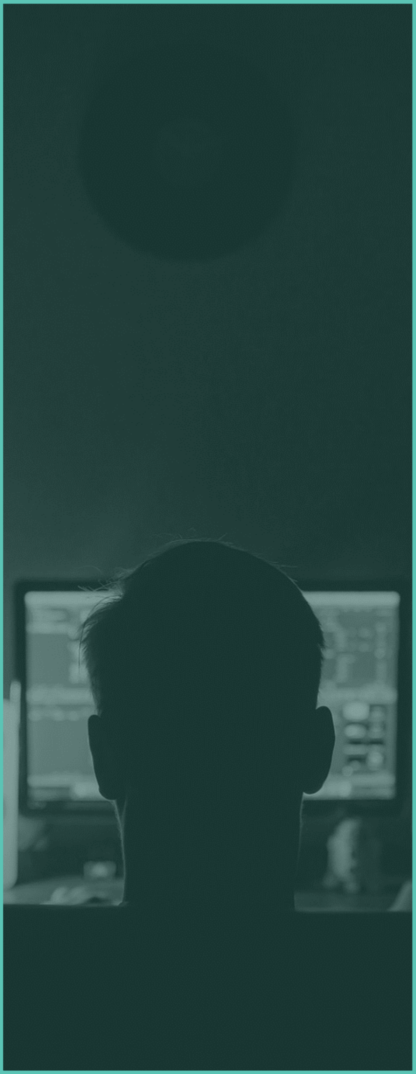
IstroSec specialists have experience with searching for, processing and analysis of data on cybersecurity threats. They know the tactics, techniques, and procedures of attackers and have the knowledge necessary to enable you to make decisions during incident response based on the data on current cyber threats.

Expertise in intelligence

IstroSec specialists have expertise in intelligence and many other areas, such as incident response, forensic analysis, and world-class malware analysis, which they have repeatedly demonstrated while dealing with state-sponsored cyber-attacks, attacks on Fortune 500 organizations, as well as the participation of four **Istro**Sec experts in the winning team of Locked Shields 2016 exercise.

Certified professionals

IstroSec experts are also holders of internationally recognized certificates in these areas. We hold certificates such as Certified Information Systems Security Professional (CISSP), Certified Information System Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) and more.



Case Study

Company type: Manufacturer in the electrical industry

Service provided: Intelligence

Solution: Online hacking forums monitoring

A vulnerability that was fixed in an update from the previous week has been released on GitHub. It was a vulnerability that could gain privileges at the system level. A post referring to the vulnerability and also to the list of devices where this vulnerability can be exploited was published on the hacking forum. Usually, attackers select victims based on the ratio of attack intensity to potential profit. They often start by looking at a list of organizations that have already been compromised and whose data is freely available on the dark web. They assume that if an organization has been compromised once, its cybersecurity practices are not very mature. Subsequently, they will begin to prepare a newly published vulnerability for use against such an organization.

As part of the monitoring of such hacking forums and other resources, the **Istro**Sec team observed that the incidence of reports of this vulnerability and the number of potential victims is increasing. An analyst at **Istro**Sec compared clients' data in a database and found that one of our customers was using systems that were vulnerable to this type of attack.

The customer was notified, and a threat report was prepared. The report contained:

- Information on the vulnerability and how to fix it, or at least mitigate the risk of compromise, if a fix is not yet available
- The organization's data that was found leaked to the site
- An overview of APT groups focusing on the industry in which the organization operates and ways to mitigate the risk of compromise by these groups