IstroSec

Data Sheet

Ransomware Response

To minimize the impact of an ongoing ransomware attack in your organization, it is critical to react swiftly. In case you have been hit by a ransomware, contact us 24/7 on phone number +421 917 699 002 or by sending an email to incident@istrosec.com. IstroSec experts will ensure fast and effective remediation of the cyber security incident at hand.

This service includes

- Initial triage
- Containment to prevent further spread of ransomware
- Identification of the ransomware strain, attack group behind it, scope of the attack and analysis of the need to communicate with the attacker or pay the ransom
- Acquisition of digital evidence for digital forensics analysis, law enforcement agencies or cyber insurance companies
- Monitoring of the DarkWeb for the presence of leaked data
- Deployment of security tools to ensure security monitoring of the client's network for the duration of the incident
- Hardening of clean network segments to prevent further attacks
- If client decides to communicate with the attackers:
  - Leading the negotiations to lower the ransom and to avoid potential communication mistakes leading to unsuccessful exchange with the attacker
  - Assistance with validation and usage of the ransomware decryptor
  - Analysis of the decryptor provided by the attacker
- Identification of the vector of compromise including digital forensics for the purposes of cyber insurance and law enforcement agencies
- Identification of secondary infections within the organization
- Building resiliency to prevent this ransomware attack from resurfacing

Why IstroSec?

Combined experience of more than 70 years

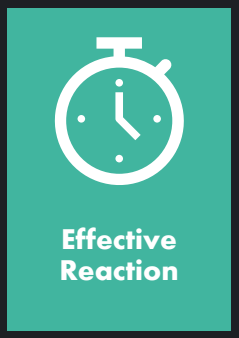
Access to experts in all domains of information security, including penetration testers, forensic analysts, malware analysts, trainers and more

Systematic improvement of information security according to frameworks enriched with the experience of IstroSec experts with advanced security incidents

Certified experts to ensure compliance with security standards and legislation - IstroSec experts have been operating in public administration (NIS Directive, GDPR and others) as well as in the private sector (ISO 27001, NIST, HIPAA and others)

Why Choose Us?

IstroSec's experts have long-standing experience with ransomware attacks, identification of the problem at hand and its effective remediation. They utilize proprietary methodology validated by countless incident response engagements and tools for effective ransomware response (including response to threats related with ransomware), minimizing its impact and damage done to client's assets and acquisition and preservation of digital evidence for law enforcement agencies, the regulators or insurance companies.



Facilitating Ransom Payments Using Cryptocurrencies

If there is no other option than to pay the ransom, IstroSec can facilitate the communication with the attacker by deploying professional negotiators with psychological training to ensure:

- There is no miscommunication that could potentially lead to total loss of data
- Smooth ransom payment to maximize the probability of attacker providing the decryptor
- The chance of publishing leaked data is minimized

Effective Reaction

When ransomware is deployed in the target organization, it is necessary to react within hours. It is critical to identify high-priority actions and perform such actions immediately. IstroSec's experts have the necessary experience with crisis management in these situations and can assist with coordination or lead the response actions.

Providing Support to Target Organization

Not all organizations have the necessary tools to support effective response to ransomware attacks. IstroSec has proprietary tools at your disposal that can be readily implemented within your infrastructure to enable effective containment and analysis of the attack.

Expertise in Cyber Security Incident Response, Malware Analysis and Digital Forensics

IstroSec's experts have proven best-in-class expertise in incident response, digital forensics and malware analysis confirmed by responding to several nation-state APT attacks, responding to attacks targeting Fortune 500 companies and by four IstroSec specialists being members of the winning team of LockedShields 2016, the world's most advanced cyber security incident response exercise.

IstroSec's incident response specialists are also holders of internationally accepted certificates, such as GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) and others.