IstroSec

Data Sheet

Malware Analysis

Most cyber-attacks involve malicious software, or malware. There are very often ransomware and other cyber-attacks where backdoors are introduced into the victim's networks in order to establish remote access. In other instances, they infect victims with different kinds of spyware. Also phishing attacks often rely on infected attachments or they contain a link to a specially crafted website infected with malware.

> *In the case of targeted or advanced cyber-attacks, it is not sufficient to rely solely on routine antivirus scans during the response, and malicious code needs to be analyzed in more detail.*

Reasons you may need more detailed malware analysis

- A targeted or advanced cyber-attack is assumed
- Relatively new or unknown malware sample that goes undetected by standard antiviruses
- To assess the risk and potential impacts of the attack it is required to identify all features, capabilities, and configuration of the malware sample
- Identification of similar attacks and campaigns. Planning and readiness for attackers' next steps
- Threat intelligence and defensive intelligence customized for the client
- Identification and removal of persistence and all the artifacts created by the malware without the need of reinstall the operating system; especially in cases when standard antiviruses found only a small portion of the artifacts or none of them

Malware Analysis Services

- Static and behavioral analysis - identification of malware type and family, its basic characteristics and behavior
- Create list of indicators of compromise - IOCs, which could be used during incident response, forensic analysis, monitoring and threat hunting
- Determination, whether malware sample was customized to target a particular victim or if it is part of standard mass campaigns
- Extraction of configuration (if applicable)
- Analysis of the malware features, identification of the malware functionalities
- Attribution of the malicious code to threat actor or campaign (if possible)
- Advanced malware analysis and reverse engineering - complete analysis of features and functionality including bypassing of the obfuscation techniques and anti-analysis protection. Research of similar and/or related cases, malware intelligence
- Development of the special inoculation programs, which prevent infection with the malware samples used during the cyber attack
- Development of the special programs and removal tools which will delete the artifacts created by the malware during the cyber attack

Why IstroSec?

Experience and knowledge

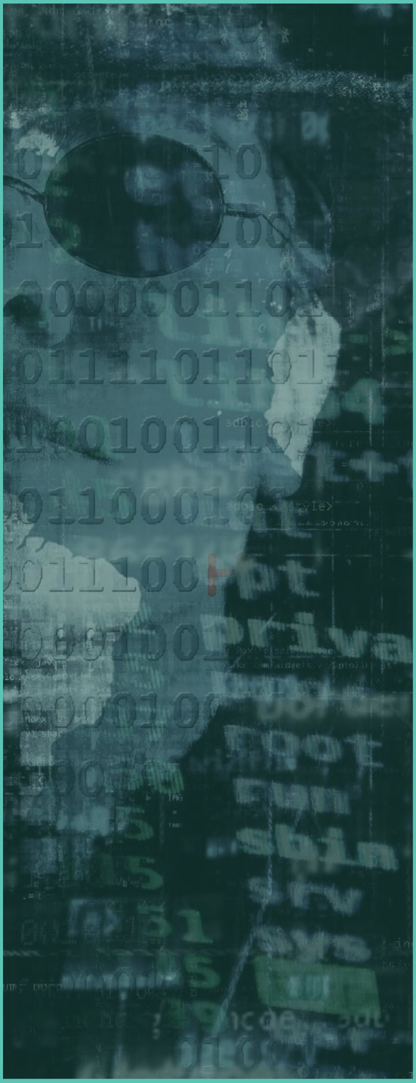
Our certified experts have many years of experience. They have analyzed hundreds of malware samples including samples used in advanced and targeted cyber-attacks and APT attacks against government and global private companies. They know the tactics, techniques and procedures of attackers and have the necessary knowledge to enable datadriven decisions based on analysis of malware deployed during an incident.

Expertise in malware analysis

In addition to malware analysis, our experts also carry out their own research in the field of malware, training, prevention, and threat intelligence. They have also developed several community open source tools and published their results in many papers, case studies, and conferences in Europe and the United States, including DEFCON and BlackHat. Four of our experts were part of the winning LockedShields 2016 team.

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 studies

Company type: Government

Service: Malware analysis

Solution: Advanced malware analysis, research of related threats, creation of IOCs

Our researchers found a malware sample masked as a document originated from one governmental institution. Malware analysis revealed the phishing campaign infecting its victims with Cobalt Strike. This tool is often used by penetration testers as well as advanced attackers with the purpose of take control and remote access to the compromised machines.

Based on extracted Cobalt Strike configuration our analysts found a command-and-control server. Together with our malware intelligence research they found more servers which have been used in attacks against government, or, they have been prepared by attackers for future attacks in this campaign. We provided IOCs to the governmental CSIRT in that country. Then, it was possible to discover other victims of the attackers and prevent the further attacks using the revealed attacker's operational infrastructure.

Company type: Large commercial IT development company

Service: Malware analysis (+forensic analysis and incident response)

Solution: Advanced malware analysis, malware intelligence, development of malicious artifact removal tool

Devices in client's possession were affected by unusual high CPU load. It was caused by running processes masked as some Windows services. However, these services were not legitimate. Antivirus check detected some of them as a cryptocurrency miner, but their removal was not successful - they had been re-created again very soon. Malware analysis identified several persistence techniques used by that malware. Followed by malware intelligence research, the analysts discovered more malicious artifacts used in this attack, but already removed by the attackers. With knowledge of those artifacts the analysts were able to reconstruct all stages of the attack. They also identified the initial access of the attackers - an exploitation of the vulnerability in a web application. Then they developed a malicious artifacts removal tool for all artifacts, persistences and several backdoors. Together with data from threat intelligence the analysts found other similar attacks and estimated the volume of this global campaign and attackers' profit.