IstroSec

Data Sheet

Threat Hunting and Compromise Assessment

During threat hunting, we actively search for suspicious activity or remnants of any potential malicious activity within the clients' infrastructure. Nowadays, attackers and their efforts to penetrate the target infrastructure are increasingly sophisticated. Their attacks are often overlooked by modern commercial solutions like EDR or AV until it is too late.

> *"We focus on activities that could signal the presence of malicious actors, potentially vulnerable systems, bad IT hygiene habits such as unnecessary admin privileges, plain-text passwords, etc."*

Prerequisites

- Access to SIEM, EDR or other log collectors
- Ability to make queries on endpoint data
- Read access and the ability to work with logs of end devices
- Optional: Previous outputs of penetration tests, audits, incidents and the like

Basic Threat Hunting Contains:

- Checking for IoCs in network communication (if possible).
- Automatized control of clients' key systems, whether they contain some IOCs from the **Istro**Sec's database.
- Formulation of threat-hunting hypothesis based on standard attacks against customer type of organization, additional service - development of Customer Threat Landscape.
- Identification and analysis of possible sources of relevant data to the hunting hypothesis.
- Automatic control of endpoint logs and outlining suspicious events.
- Creating and inventory of clients' programs, their version, vulnerabilities for their version (if possible via Clients tools).
- Access to relevant data sources (implemented technologies or implementation of our tools).
- Basic identification of outliers present within Clients' infrastructure.

Full Threat Hunting Contains Also:

- Consultation based on clients' capabilities and proposing the implementation of free/commercial tools for monitoring.
- Help with implementing monitoring tools within Clients' infrastructure, and their initial setting based on clients' need.
- Detailed manual analysis of monitoring tool's output.

Deliverables:

- Report containing an executive summary, technical details, and recommended actions on identified issues
- Queries used to hunt with.

IstroSec

Data Sheet

Why Us?

Experience and knowledge

IstroSec specialists have experience with threat hunting using a variety of commercial, free and proprietary tools. Furthermore, they have experience with adversaries from script kiddie level all the way up to state-sponsored APT groups. They know the tactics, techniques, and procedures of attackers and have the knowledge necessary to enable you to make decisions based on the data on current cyber threats.

Expertise in threat hunting

IstroSec specialists have expertise in threat hunting 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 IstroSec 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: Organization in sector lucrative for adversaries

Service provided: Threat hunting

Solution: Compromise assessment and threat hunting after publishing a zero-day vulnerability

The manufacturer of one of the deployed software products has issued a warning on a serious zero-day vulnerability. There are indications of current abuse of this vulnerability by attackers to breach the infrastructure. The IstroSec threat hunting team was instructed to verify whether the organization has been compromised. Therefore, the team collected available vulnerability data from the vendor and from sources within the IT security community to determine the threat hunt strategy and indicators of compromise that were the starting point of the threat hunt. The team mapped out the client's environment with an emphasis on identifying available sources of information about what is happening in the infrastructure, such as logs of vulnerable applications, logs of network traffic, logs from the local DNS server, system logs of devices and logs of deployed SIEM solutions. Error records consistent with attempts to exploit the vulnerability have been found in the logs of the vulnerable application.

Based on time correlation, suspicious connections were identified in the network communication logs. The reputation of the source IP addresses has been checked against the threat intelligence sources, but no record has been available yet. The full packet capture record of network communication was not available. At the same time, statistical analysis of network traffic showed that the device began to perform more DNS queries than before the moment of suspicious activity, which could indicate beaconing and the created C2 channel by an attacker. An EDR solution was operatively installed on the device with suspicious activity to help identify the beacon process and acquire samples of related files.

The team recommended declaring a security incident and calling in forensic and malware analysts. The threat hunt continued to play a supporting role in resolving the incident. Suspicious IP addresses have been blocked on the perimeter firewall. Malware analysis identified the samples as a DNS beacon from the CobaltStrike suite. Forensic analysis revealed activity aimed at stealing login data from the time before deployment of an EDR solution on the device. As part of the ongoing threat hunting, the activity of all user accounts found on the secured device was checked in the SIEM logs. It turned out that one administrator account logged in to several internal servers after compromise, and the user himself did not confirm such activity. Based on this, it was recommended to change all user passwords and reset the Kerberos service during the containment phase of the incident.