Jet CSIRT (Computer Security Incident Response Team) uses ICS Threat Intelligence Malware Data Feed from Kaspersky

kaspersky BRING ON THE FUTURE

Kaspersky ICS CERT

Jet Infosystems

csirt.jet.su

Systems integrator

- One of the top 3 largest integrators in Russia according to CNews Security 2019
- 24 years on the IT market
- 1,800+ employees
- 250+ cybersecurity experts
- 300+ comprehensive projects annually

Jet Infosystems is one of the largest IT companies in Russia. The company has been active in the information technology market since 1991, implementing complex and unique projects throughout Russia. With a staff of over 1,800, Jet Infosystems has 10 offices and divisions in Russia and the CIS, and also handles projects abroad. The company's main focuses include the design and implementation of computing systems, network infrastructure, engineering systems and multimedia, custom engineering; development, implementation and maintenance of software solutions and enterprise level business applications, information security services, IT outsourcing and technical support.

Its information security service portfolio includes the design, implementation, maintenance and technical support of specialized solutions and consulting. Jet Infosystems' key objective is to implement and create solutions to provide businesses with real security.

Task

In 2018, Jet Infosystems launched Jet CSIRT (Computer Security Incident Response Team).

Jet CSIRT merges two of the company's key services: monitoring and responding to information security incidents, and operating and maintaining security tools. This ensures the company can handle client security issues with an individualized approach 24x7.

The Jet CSIRT team boasts 40 experts responsible for over 200 contracts for expert services. Jet CSIRT's clients span a number of different industries, including large industrial enterprises.

To ensure the highest quality protection of industrial infrastructures and investigation of industry-related information security incidents, it's essential to have specific data on industrial control systems (ICS) cyber threats. Malicious programs detected on ICS computers are often unique and almost never found on other computers in corporate networks.

Jet Infosystems needed to find a reliable supplier of this data for its Computer Security Incident Response Team, so it analyzed the market to find a company with a global presence and experienced team of ICS threat researchers. In addition, Jet Infosystems was looking for a fair MSSP model and convenient licensing policy.

"At a certain point, our Computer Security Incident Response Team started focusing on the high-quality enrichment of incidents with data on cyberthreats to industrial control systems. After analyzing the market, we concluded that Kaspersky was best positioned to help".

Aleksey Malnev, Head of Jet CSIRT, Jet Infosystems

Expertise
Kaspersky helps industrial enterprises, regulators and government agencies combat attacks and threats targeting critical infrastructures. Kaspersky ICS CERT (Industrial Control Systems Cyber Emergency Response Team) was specially formed for this purpose.

Data quality
ICS Threat Intelligence Malware Data Feed is regularly updated with information received via the Kaspersky Security Network (KSN) exclusively from ICS computers protected by Kaspersky products.

Comprehensive approach
Kaspersky helps implement comprehensive approaches to cybersecurity at all levels, from security analysis and training for employees, to advanced ICS protection technologies and incident response.

Solution

Jet Infosystems chose Kaspersky as its data provider for Jet CSIRT after determining that Kaspersky is the only market player meeting all the company's needs that also has truly unique data on cyber threats relevant to industrial enterprises.

The constantly updated flow of information on threats in industrial automation systems informs industrial information security services about cyber threat risks and their consequences, and helps decision-making regarding measures to protect against cyber attacks before they start and prevent incidents.

The threat data contains indicators of compromise (IoC) that help:

- detect attack attempts against industrial automation systems;
- identify malware infections in industrial automation systems, including when responding to computer incidents;
- enrich data on threats and malware detected in industrial automation systems.

Collection and processing

The data feed is regularly updated based on information received from APCS computers protected by the Kaspersky Security Network (KSN). All the data received is verified and qualitatively improved using a variety of technologies, including analysis based on statistical criteria, analysis by Kaspersky expert systems (sandboxes, heuristic analysis, similarity analysis, behavior profiling, etc.), verification by analysts and white list verification.

Data use scenarios

Detecting attacks

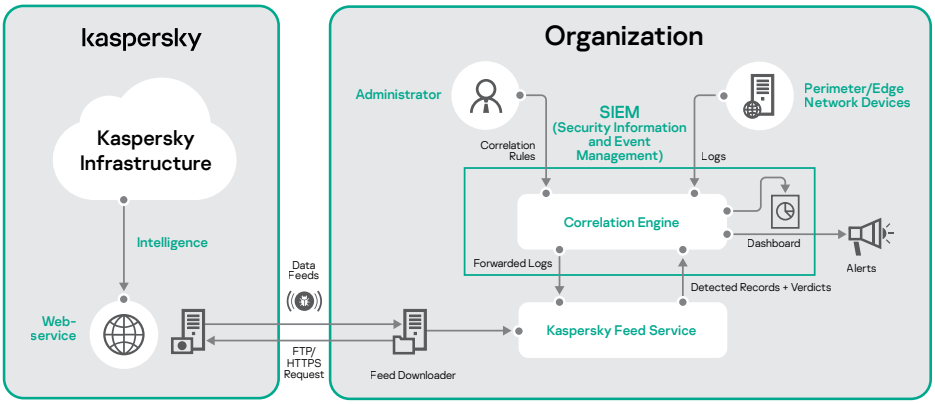
ICS Threat Intelligence Malware Data Feed provides an additional layer of protection against malware by detecting malicious programs and attempted attacks on systems via correlation with SIEM system data collected from network perimeters, tail nodes and file sandboxes.

Detecting cases of infection

Threat data is provided in open JSON format for use by various data analysis and comparison systems, or can be reformatted into any other data format. Thus, the threat data can be used to identify attacks and cases of ICS computer malware infection during cyber incident investigations.

Enriching threat data

In the course of cyber incident investigations, specialists often need additional information about detected threats to help link disparate facts about cyber incidents to obtain a more complete picture.



Results

ICS Threat Intelligence Malware Data Feed was connected to Jet CSIRT systems as planned without any difficulties with the support of Kaspersky specialists.

Now after several months, Jet CSIRT specialists can confidently say that they made the right choice, as pilot tests have demonstrated the successful registration of a number of the latest industrial threats. Now Jet CSIRT offers even higher quality expert services for industrial enterprises.

www.kaspersky.com

#Kaspersky
#BringontheFuture

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization - including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics