Kaspersky Crimeware Intelligence Reporting

kaspersky BRING ON THE FUTURE

Evolving threats

The world of crimeware threats is constantly evolving. Crimeware refers to malicious programs specifically designed to commit financially-motivated cybercrime. The most infamous example is ransomware – programs which block access to data or disrupt a computer's performance. There are no limits to the imagination of cybercriminals who are coming up with ever-more sophisticated ways to gain and monetize their access to their target's systems, accounts and data.

Introduction

Financially-motivated cybercrime is not limited to specific industries. And while attacks on financial infrastructures like ATMs and PoS (Point of Sale) devices continue, all enterprises in every sector are at risk from ransomware. Over the last couple of years, there has been a blurring of boundaries between different types of threats and different types of threat actors. This includes the emergence of advanced persistent threat (APT) campaigns focused not on cyberespionage, but on theft – stealing money to finance other activities that the ATP group is involved in. We should not underestimate the growing sophistication of crimeware threats.

Kaspersky Crimeware Intelligence Reporting enables organizations to inform their defensive strategies by providing timely information on malware campaigns, attacks targeting financial institutions and information on crimeware tools used to attack banks, payment processing companies and their specific infrastructures.

The service delivers:

Detailed descriptions of popular, widespread and highly-publicized hyped malware

Information on dangerous, widespread malware campaigns

Researcher notes/early warnings, including information on new and updated malware threats

Detailed descriptions of threats targeting financial infrastructures and the corresponding attack tools being e developed or sold by cybercriminals on the Dark Web in various geographies

Service benefits

Crimeware actor profiles. Including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with mapping to MITRE ATT&CK

Privileged access. Receive technical descriptions about the latest threats during ongoing investigations, before release to the general public

Retrospective analysis. Access to all previously issued private reports is available throughout your subscription

Access to technical data, including an extended list of IOCs, available in standard formats including openIOC or STIX, and access to our YARA rules

RESTful API. Seamless integration and automation of your security workflows

Tools used to attack financial organizations

Researcher notes / early warnings

Malware descriptions

Malware campaigns

Kaspersky Crimeware Intelligence Reporting

Learn more

www.kaspersky.com