Автоматизация в промышленности 2022. №02
www.avtprom.ru

DOI: 10.25728/avtprom.2022.02.10

К.Н. Круглов (Kaspersky ICS CERT)

АТАКИ, использующие доверенную корпоративную инфраструктуру для КРАЖИ учетных данных В сетях АСУ

Проанализированы атаки шпионских программ с ограниченным числом целей и коротким временем жизни каждого образца вредоносного ПО, которые нацелены, в том числе на промышленные предприятия. Показано, как SMTP-сервисы (отвечающие за отправление писем) используются для фишинговых рассылок и сбора украденных данных. Приведены рекомендации для обеспечения надлежащей защиты промышленного предприятия, его партнерской сети и бизнеса в целом.

Ключевые слова: шпионские программы, вредоносное программное обеспечение, промышленные предприятия, фишинговые рассылки, доверенная корпоративная инфраструктура.

***Круглов Кирилл Николаевич** - старший разработчик-исследователь, Kaspersky ICS CERT.*

Kruglov K.M. Credential theft attacks through trusted infrastructure in automatic control networks

The paper analyses spyware attacks with limited number of targets and short lifecycle of each malicious software sample, which may be aimed at industrial enterprises. It shows how SMTP services responsible for posting are used for phishing delivery and the collection of stolen data. The recommendations are made on ensuring the reliable protection of industrial enterprise, its partner network and the whole business.

Keywords: spyware, malware, industrial enterprises, phishing delivery, trusted corporate infrastructure.