Автоматизация в промышленности 2024. №07
www.avtprom.ru

DOI: 10.25728/avtprom.2024.07.04

Н.А. Басынин (Positive Technologies)

Вредоносное ПО: исследование поведения и каналов распространения

Рассмотрено, какие типы вредоносного программного обеспечения (ВПО) чаще всего используются в кибератаках, а также по каким каналам злоумышленники доставляют вредоносы. Приведен анализ действий вредоносных программ, эти действия сопоставлены с техниками MITRE ATT&CK. Предложены меры, которые помогут защититься от атак с использованием ВПО.

Ключевые слова: вредоносное программное обеспечение, кибератаки, киберзащита, легитимные функции операционной системы, электронная почта, шифровальщики, шпионское ПО.

Басынин Никита Алексеевич *– аналитик исследовательской группы Positive Technologies.*

Список литературы

1. Тренды фишинговых атак на организации в 2022–2023 гг. https://www.ptsecurity.com
2. Вредоносное ПО в корпоративной сети: угрозы и способы обнаружения. https://www.ptsecurity.com
3. Актуальные киберугрозы: III квартал 2023 г. https:// www.ptsecurity.com

Basynin N.A. Malware: investigation of behavior and dissemination channels

The paper investigates malware types most frequently used in cyberattacks and its most popular delivery channels. Malicious actions are analyzed and compared to Mitre Att&ck techniques. Measures to be taken for malware prevention are proposed.

Keywords: malware, cyberattacks, cyber security, legitimate OS functions, email, encryptors, spyware.