THE CORONAVIRUS & CYBERSECURITY: 3 AREAS OF EXPLOITATION

Robert R. Ackerman Jr.

https://bit.ly/2SuXGTB

Engl.

The article by Robert R. Ackerman Jr. discusses the three main targets that hackers attacking during the coronavirus crisis. There is information about criminal, political, and strategic factors. These factors are combining to create a perfect storm for cyber infection.

The author supposes that in political exploitation there will be attempted compromises on critical infrastructure, such as power plants and petrochemical facilities, as well as active disinformation campaigns to sow confusion and undermine confidence in political leadership. Also he says that the DDoS attack on Health and Human Services is just the start.

According to the author, in criminal exploitation coronavirus-themed domain registrations are 50% more likely to be from malicious actors. The author considers that well-honed phishing attacks targeting hospitals and critical healthcare providers.

In strategic exploitation, the author shows that the most sophisticated attackers will take advantage of preoccupied organizations that have their guard down. They will plant malware inside a targeted company's infrastructure for later exploitation. In addition, the author illustrates that 40% of security breaches are now indirect, as threat actors increasingly target the weak links in the supply chain or business ecosystem.

Robert R. Ackerman Jr. concludes that every crisis and attending threat translates into a learning opportunity. These opportunities are lessons from which we can adapt new strategies and supporting technologies to evolve our digital economy and technology infrastructure to be better prepared the next time we face challenges.

Укр.

У статті Роберта Р. Акермана-молодшого описуються три основні цілі, які кіберзлочинці атакують під час кризи, яка пов’язана з пандемією коронавірусу. Наведена в статті інформація розкриває кримінальний, політичний та стратегічний фактори, які поєднуються для створення ідеального «шторму» для кіберзараження.

Автор припускає, що в політичній експлуатації будуть зроблені спроби компрометації критичної інфраструктури, такої як електростанції та

нафтохімічні споруди, а також активні дезінформаційні кампанії, щоб посіяти плутанину та підірвати довіру до політичного керівництва. Також він каже, що DDoS атака на охорону здоров'я та людські послуги – це лише початок.

За словами автора, у кримінальній експлуатації реєстрації доменів, пов’язаних з коронавірусом, на 50% частіше бувають від зловмисників. Автор вважає, що добре відточені фішингові атаки націлені на лікарні та критично важливих медичних постачальників.

У стратегічній експлуатації автор показує, що найбільш витончені нападники будуть атакувати організацій, які не мають свої охорони. Вони будуть проваджувати шкідливе програмне забезпечення всередині цільової інфраструктури компанії для подальшої експлуатації. Крім того, автор ілюструє, що 40% порушень безпеки зараз є непрямими, оскільки зловмисники все частіше націлюються на слабкі ланки ланцюга постачання або бізнес-екосистеми.

Роберт Р. Акерман-молодший робить висновок, шо кожна криза та пов’язана з нею загроза – можливість навчання. Ці можливості є уроками, з яких ми можемо адаптувати нові стратегії та підтримуючі технології для розвитку нашої цифрової економіки та технологічної інфраструктури для того, щоб бути краще підготовленими, коли ми знову зіткнемося з проблемами.

Автор анотацій: Рожко Владислав, група УБД-41