Kaspersky raises alarm over increasing targeted attacks against pharmaceuticals

Global cybersecurity company Kaspersky reveals an alarming trend observed in the pharmaceutical industry – a year-on-year steady increase on the number of devices being attacked by cybercriminals. From 44% of machines infected in 2017 and a 1% increase in 2018, this year's number of detected attempts shows that nearly every 5-in-10 devices inside a pharmaceutical facility are now being targeted globally.

Amongst the countries which logged the most number of attacks are Pakistan (54%), Egypt (53%), Mexico (47%), Indonesia (46%), and Spain (45%). Four more countries from the Asia Pacific region cap off the top 15 nations with the highest percent of devices infected. These include India, Bangladesh, Hong Kong, and Malaysia with more or less 4-in-10 machines with detected malicious attempts.

"While it is a known fact that money-hungry cybercriminals can easily earn by attacking banks, we also observe that these hackers as well as cyberespionage groups are slowly paying a lot of attention towards the industry of advanced medicine," says Yury Namestnikov, Head of Global Research and Analysis Team (GReAT) Russia at Kaspersky. "They are slowly realising that pharmaceutical companies house a treasure trove of highly valuable data such as the latest drugs and vaccines, the newest researches, as well as medical secrets. The rise of internet-connected operational technology (OT) inside these pharmaceuticals also contributes to the widening attack surface inside this sector."

Among the Advanced Persistent Threat (APT) groups which have been waging sophisticated spying over pharmaceuticals globally include Cloud Atlas and APT10 also known as MenuPass.

"Based on our monitoring of several APT actors' movements in the Asia Pacific and globally, we figured that these groups infect servers and exfiltrate data from pharmaceutical companies. Their attack techniques and behaviour also prove that these attackers' apparent goal is to get their hands on intellectual properties related to the latest medical formulas and research results as well as the

business plans of their victims," adds Namestnikov.

Vulnerabilities in open source EMR-systems and its dangers

In his own research, Denis Makrushin, Security Architect at Ingram Micro, revealed the risks that come along with the steady migration of hospitals from paper-based data storage to electronic medical record (EMR) systems. Makrushin further notes that healthcare organisations, scrambling to digitise their data storage, see open source EMR web-portals as an easy and quick option, despite their known security challenges.

"We are seeing lesser printed or hand-written medical books inside hospitals and clinics worldwide with the advent of open source. Given their limited internal IT workforce, healthcare institutions opt to use convenient services such as OpenEMR, OpenMRS or similar web applications. This technology's rapid adoption triggers the rise of the threats against this widely-used services," says Makrushin,

OpenEMR and OpenMRS are open platforms for medical practice management. Any organisation can use this product for business without any restrictions. The source code of this product is also available for any developer. In addition, this software has certifications from trusted organisations (for example OpenEMR is ONC Complete Ambulatory HER certified).

"Their free and open nature make these EMR-applications highly sensitive to cyberattacks. There have been a lot of security patches released as researchers unmask one exploit after another. I, myself, have discovered vulnerabilities in these applications, hackers can inject malicious code at the initial stage of registration, and portray himself as a patient. From this, malicious actors can infect the portal's page and collect medical information from all users of the portal, including doctors and admins. These data can be easily exfiltrated," he adds.

To securely use this platform, Makrushin suggests healthcare facilities to:
• Conduct secure software development lifecycle (Secure SDLC)
– Regularly perform architecture analysis, conduct penetration testing, security code review on systems being use

• Control the attack surface
– Periodically update your installed software and remove unwanted applications
– Try to remove all exposure nodes that process medical data

• Raise security awareness for every person involved
– Conduct regular cybersecurity awareness training for all staff and even patients