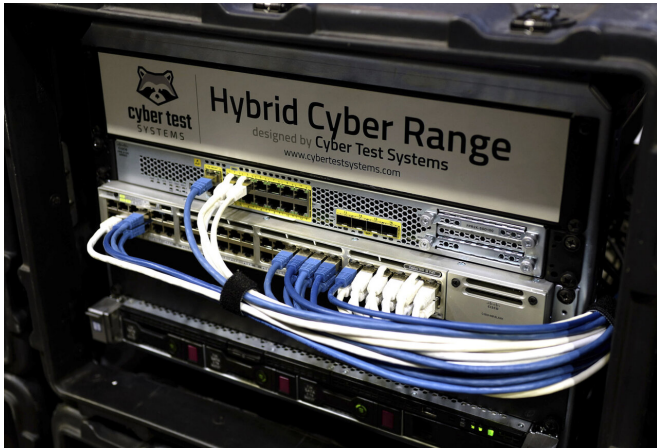


# France to boost cyberdefense after hospital malware attacks

18 February 2021, by Sylvie Corbet



In this Jan.22, 2019 file photo, cables are plugged into a device by Cyber Test Systems at the Cybersecurity Conference in Lille, northern France. French President Emmanuel Macron is unveiling on Thursday a plan to better arm public facilities and private companies against cybercriminals as ransomware attacks struck two hospitals earlier this month, amid an upsurge of similar attacks in the country. (AP Photo/Michel Spingler, File)

French President Emmanuel Macron on Thursday unveiled a plan to better arm public facilities and private companies against cybercriminals following ransomware attacks at two hospitals this month and an upsurge of similar cyber assaults in France.

The attacks at the hospitals in Dax and Villefranche-sur-Saone prompted the transfer of some patients to other facilities as the French health care system is under pressure from the coronavirus pandemic.

Macron discussed the attacks with officials and workers from both hospitals, saying the incident "shows how the threat is very serious, sometimes vital."

"We are learning about these new attacks, some coming from states as part of new conflicts between nations, others coming from mafias," the French leader said during a videoconference. Some attacks have "criminal" or "lucrative" motives, others are used to "destabilize" countries, he added.

Macron referred to a massive hack of U.S. federal agencies last year and to the stealing of vaccine documents from the European Medicine Agency in November.

He stressed the need for international cooperation among police and criminal justice agencies after Ukrainian authorities said they had crippled a ransomware gang known as Egregor earlier this month following a joint action by the United States, France and Ukraine.

Macron's office said the government will earmark about 500 million euros (\$603 million) to help boost cyberdefense systems in the public and private sector.

The National Cybersecurity Agency of France (ANSSI) reported that ransomware attacks surged 255% in 2020 compared to the previous year. All sectors and geographical areas of the country were included, but the increase particularly concerns the health care sector, the education system, local authorities and digital service providers, ANSSI said.



French President Emmanuel Macron gestures during a national cybersecurity strategy meeting at the Elysee Palace in Paris, Thursday, Feb.18, 2021. French President Emmanuel Macron on Thursday unveiled a plan to better arm public facilities and private companies against cybercriminals following ransomware attacks at two hospitals this month and an upsurge of similar cyber assaults in France. (Ludovic Marin, Pool via AP)

During ransomware attacks, cybercriminals infect computer networks with malware that scrambles data until victims pay a ransom.

The hospital in Villefranche-sur-Saone, located north of the city of Lyon, said its phone system went down during a cyberattack on Monday that forced a preemptive shutoff of the internet service and other networks to keep the ransomware from spreading.

The hospital also had to postpone surgeries planned for the following day. but said patient safety was preserved.

The Dax hospital in southwestern France reported a similar attack last week. Without phones and computers working, health care workers had to use pen and paper for record keeping.

The French cybersecurity agency is helping to investigate the attacks.

ANSSI said Monday that an attack similar to one used by Russian hackers targeted software

distributed by the French company Centreon, resulting in the breach of "several French entities" from late 2017 to 2020.

"This campaign bears several similarities with previous campaigns attributed to the intrusion set named Sandworm," ANSSI said in a statement Monday.

[Sandworm is a Russian military hacking group](#) that U.S. officials and cybersecurity researchers blame for the most damaging cyberattacks to date, including the June 2017 NotPetya attack that targeted businesses that operate in Ukraine. It caused at least \$10 billion in damage globally, most notably to the Danish shipping multinational Maersk.

Sandworm is also accused of trying to interfere in France's 2017 election in a hack-and-leak operation, in trying to sabotage the opening ceremonies of the 2018 Winter Olympics in South Korea and in triggering power outages in Ukraine in December 2015 and December 2016.

© 2021 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

APA citation: France to boost cyberdefense after hospital malware attacks (2021, February 18) retrieved 19 April 2021 from <https://techxplore.com/news/2021-02-france-boost-cyberdefense-hospital-malware.html>

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.*