KASPERSKY SECURITY BULLETIN

Healthcare security in 2021

02 DEC 2020 3 minute read

2020 roundup and our predictions

The pandemic has turned 2020 into a year of medicine and information technology. The remarkable surge in the criticality level of medical infrastructure, coupled with feasible across-the-board digitalization, led to many of our last year's predictions coming true much sooner than expected.

As we foresaw, there has been an increase in attacks on medical equipment in countries where the digital transformation of healthcare is only just beginning. Interest in medical research has, of course, increased too among cybercriminals in particular groups specializing in targeted attacks. This was spurred primarily by the development of a COVID-19 vaccine and its potential significance for the global community. The biggest hullabaloo was around the WellMess campaign, which, according to Western intelligence agencies, sought to steal information about vaccines being developed in Canada, the UK and several other countries.

The topic of healthcare has become one of the most popular baits for attacks of varying complexity: from no-frills emails with malicious attachments through phishing to targeted attacks. To deceive users, attackers faked statements and documents from various medical bodies, including the WHO, and promised medicines and vaccines.

Since the outbreak of the pandemic, groups such as DoppelPaymer and Maze, known for targeted ransomware attacks, have announced that they will not pursue medical organizations in the current climate. All the same, healthcare is regularly targeted by cybercriminals. Recall that at the very start of the pandemic a hospital in the Czech Republic with one of the country's largest COVID-19 testing facilities suffered a cyberattack. 2020 also saw the first confirmed case when a patient died due to delays in receiving emergency care after medical equipment was infected by ransomware. According to public sources, 10% of all organizations hit by targeted ransomware between January and September 2020 were hospitals and other medical institutions. In late October alone, more than two dozen US hospitals were attacked as part of a large-scale Ryuk and other targeted ransomware campaigns. Despite the fact that some groups did indeed refrain from going after medical facilities, others pursued them with redoubled vigor.

With the digital security of medical organizations in the spotlight, especially after the above-mentioned Czech hospital incident, the infosec industry is focused on providing maximum support to healthcare systems. This led — at the very start of the pandemic — to the formation of the CTI League, a voluntary organization of cybersecurity experts seeking to protect medical organizations and help them respond to cyber incidents. Hospitals have been assisted too by security software developers, including Kaspersky, which provided medical organizations with free access to its products.

Predictions for 2021

- Attacks on COVID-19 vaccine and drug developers, and attempts to steal sensitive data from them, will continue. The world is not only fighting the disease, but witnessing a race between pharmaceutical firms, in which any significant breakthrough will likely result in targeted attacks on the company that made it.
- In countries with highly developed public healthcare, organizations in the private medical sector, most of which are small and medium-sized businesses (SMBs), will face attacks. Protecting patient data and infrastructure is fairly expensive and thus difficult for SMBs to implement at the best of times, let alone during an economic crisis.
- Health-related cyberattacks will be used as a bargaining chip in geopolitics — attribution of attacks entailing serious consequences or aimed at the latest medical developments is sure to be cited as an argument in diplomatic disputes.
- Next year will see a stream of reports about patient data leaks from cloud services. Medical organizations' transition to cloud infrastructures and storage of personal information in them is already creating additional risks. Given our correct prediction last year that interest in user health data would grow, healthcare institutions must devote serious energies to protecting their cloud infrastructures right now.
- Medicine as a bait topic will be with us next year and remain current at least until the end of the pandemic. The human factor is one of the most important components of many attacks, and information about new regulatory restrictions, potential treatments and patient health will

continue to attract user attention. Leaked medical records will also become part of the hook in targeted attacks, since accurate patient information will make fake messages far more credible.

The focus on digital security in hospitals offers hope that 2021 will be the year when cybersecurity and healthcare join forces. Past experience has shown that painful lessons such as the Wannacry epidemic in 2017 and the coronavirus pandemic in 2020 are the very thing that incentivizes organizations to pay more attention to infrastructure security.

DATA LEAKS DATA THEFT MEDICAL THREATS PHISHING RANSOMWARE TARGETED ATTACKS

Authors

Expert MARIA NAMESTNIKOVA

Healthcare security in 2021

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

// LATEST POSTS

BlueNoroff: new Trojan attacking macOS users

SERGEY PUZAN

Kaspersky Security Bulletin 2023. Statistics

AMR

IT threat evolution in Q3 2023. Mobile statistics

ANTON KIVVA

IT threat evolution Q3 2023

DAVID EMM

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR

30 NOV 2023, 4:00PM 70 MIN

Responding to a data breach: a step-by-step guide

ANNA PAVLOVSKAYA

CYBERTHREAT TALKS

14 NOV 2023, 4:00PM 60 MIN

2024 Advanced persistent threat predictions

IGOR KUZNETSOV, DAVID EMM, MARC RIVERO, DAN DEMETER, SHERIF MAGDY

CYBERTHREAT TALKS

09 NOV 2023, 6:00PM -60 MIN

CYBERTHREAT TALKS

12 SEP 2023, 4:00PM 60 MIN

Overview of modern car compromise techniques and methods of protection

ALEXANDER KOZLOV, SERGEY ANUFRIENKO

2023 APT Landscape Unveiled: Trends, Challenges, Solutions

DMITRY GALOV, DAN DEMETER, MOHAMAD AMIN HASBINI, DAVID EMM

// REPORTS

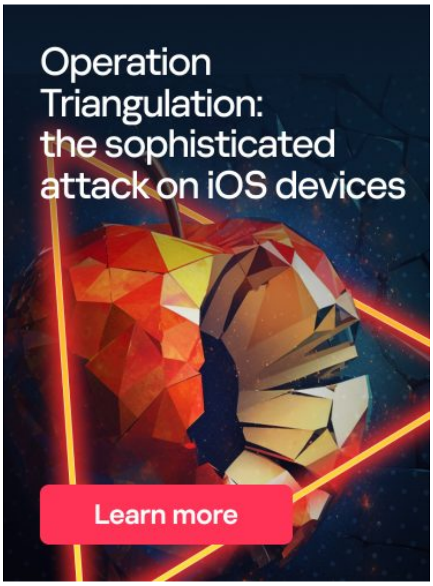
HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

A cascade of compromise: unveiling Lazarus' new campaign

How to catch a wild triangle


Operation Triangulation: the sophisticated attack on iOS devices
Learn more

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

Subscribe

□ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

Threats

Categories

Archive

Webinars

Statistics

Threats descriptions

All tags

APT Logbook

Encyclopedia

KSB 2023

© 2023 AO Kaspersky Lab. All Rights Reserved.
Registered trademarks and service marks are the property of their respective owners.

Privacy Policy License Agreement Cookies