



Episode 10

---

HEALTHCARE:  
**A CYBERSECURITY  
HEALTH CHECK**





## Cyberattacks against the medical and hospital sector exploded at the end of 2019.

Organizations operating in the private medical services industry were the first victims of this tidal wave. Following this, hospital centers the world over were subject to particularly meticulous cyberattacks from cybermafia groups. It is important to fully understand the particularities of this sector and analyze in depth the pathways for improvement so that we can confront this new threat to the healthcare industry.





# A HISTORY OF THE MOST NOTEWORTHY ATTACKS OF 2019

**⚠️ 2019 is full of notable cyberattacks against the medical sector. Chronological analysis sheds light on patterns and systemic weaknesses that must be grasped to better understand how to protect organizations.**

## **April 2, 2019: Brookside ENT and Hearing Center offices - USA**

In the beginning of April, the Brookside ENT and Hearing Center medical offices were infected with ransomware (apparently via phishing). All patient data was encrypted, and recovery efforts failed. The two doctors who practiced in the offices decided not to pay the ransom. Without any patient data and with a severely damaged reputation among

its patients, the offices closed their doors on April 30, 2019. Hundreds of patients were forced to redo their various medical exams in other establishments, which took a serious financial toll on the poorest of them.





### **July 8, 2019: Premier Family Medical - USA**

Premier Family Medical is a major medical services provider in Utah. It consists of roughly 10 medical establishments covering a wide variety of services. In July 2019, ransomware encrypted the data of more than 320,000 patients, apparently by taking advantage of a loophole in the SMBV1.0 protocol to take over an Active Directory domain controller. Once again, no one knows for certain whether the data was sold on the dark web. The impact on the organization's image was disastrous, and the patients do not know whether their medical data will be exploited.

### **August 10, 2019: Wood Ranch Medical - USA**

The attack on Wood Ranch Medical in California is another striking example of a devastating and malicious act that caused a business to shut its doors. On August 10, 2019, the servers were infected by ransomware that encrypted all the organization's patient data and backups. In the days following the attack, the organization tried hopelessly to restore the data via their backups without paying the ransom, as the amount demanded was astronomically high and impossible to pay. The data of 5,835 patients was

altered and potentially available to the attackers, though Wood Ranch Medical assured the public that the encrypted data was not stolen to be sold on the Darknet. Nevertheless, no one can be sure of the future of this data. Laid low by the attack, Wood Ranch Medical closed its doors on December 17, 2019, and [left an explanatory message on its website](#).

### **October 1, 2019: Hôpital de la Tour Blanche & Hôpital de Vierzon - France**

This attack is noteworthy in that it simultaneously targeted the Hôpital de la Tour Blanche, located in the commune of Issoudun, and the hospital in the commune of Vierzon. Following this attack, the director of the Issoudun hospital center declared that targeting hospitals was a conscious decision on the part of certain mafia groups. The attack apparently began with a phishing attempt involving an attachment that installed a Trojan horse. Fortunately, this infection did not affect patient data, and only blocked administrative data and emails. Nevertheless, the attack severely disturbed the activities of the two hospitals for several days.







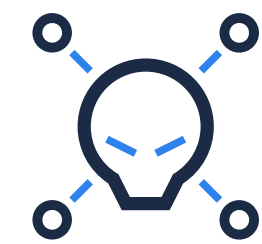
### **October 1, 2019: DCH Health System hospitals - USA**

On October 1, 2019, the three hospitals in the DHC group in Alabama were infected by the Ryuk ransomware. This ransomware is known to use Active Directory for lateral movement and privilege escalation. In a matter of hours, numerous systems at the three hospitals were infected. The DHC group decided not to accept additional patients, but also chose not to transfer currently hospitalized patients so as not to compromise the lives of those who were critically ill. On October 7, 2019, the DHC group announced that they had paid the ransom so that they could once again access their data. While it seems clear that it is best to pay a ransom if the critical state of a patient requires it, this also sends a bad message to mafia groups who seek to extort funds via ransomware and effectively encourages this activity.

### **November 15, 2019: Rouen CHU - France**

In the early evening of November 15, 2019, the CryptoMix Clop ransomware spread throughout the computer system of the Rouen CHU. It encrypted computers, using the Active Directory address book to deploy its malicious payload on the servers and workstations of the CHU. The group TA505 is well known for using this malicious code and for being extremely organized in its attacks. In this case, the point of infection is chosen at random, and the infection first targets downloaders and remote access Trojan horses (RATs). Then a latent mode waits for the right moment (for example, when an attack route opens in Active Directory) to infect the victim's machines in record time. The ransom demanded can reach €300,000. The TA505 group was known for its criminal activities against victims in the world of banking and finance; this industry shift suggests that the group now views the health environment as a «profitable» target for its activities.





## MEDICAL SUPPLIERS ARE ALSO BEING TARGETED

### **The end of 2019 also revealed a new target favored by cybermafia groups: medical suppliers.**

The Danish company Demant is one of the largest producers of hearing devices and operates worldwide. In the beginning of September 2019, the company was targeted and affected by a coordinated cyberattack using a cryptovirus. On September 3, 2019, the company announced on its website that it had been the victim of a “critical incident” and felt obligated to stop its internal computer infrastructure. Demant did not wish to disclose the details of the attack but would later share information about a “cybercriminal” attack. Some Danish media organizations indicated that ransomware was used to infect the entire information infrastructure of Demant, which included production sites, ERP software, and file servers worldwide. Furthermore, the company indicated that “delays in the provision of products and an impact on

order-receiving capacity” should be expected. Recovering the IT system took several weeks and cost an estimated \$95 million, as indicated in the company’s communication to its investors. In addition, the company declared in a press release that “Roughly half of the estimated lost sales were linked to our bulk sales of hearing aids. This incident prevented us from exercising our activities during one of the most important months of the year, especially in the United States, which is our largest market.” The press release is available [here](#).





Beyond the financial losses directly linked to this incident, the fallout surrounding Demant's image was devastating and will prove a detriment to the company's activity for years.







# THE PARTICULARITIES OF HOSPITAL CENTER INFORMATION SYSTEMS

## **Widespread use of Microsoft Active Directory technologies**

Most hospital centers rely on Microsoft technologies, most notably the general usage of the Windows operating system and the Active Directory address book. Adoption of these technologies originates from a particular use case of the medical environment, namely that hospital personnel are by nature mobile. With the sudden massive arrival of digitized information in the 1990s, hospital centers and clinics based their information systems on solutions like Citrix and Terminal Server, which allowed:

- Increased mobility within establishments, along with continuous access to the establishment's data
- Authentication security management via remote session
- Facilitated activity across extremely different peripherals, including PCs, MacOS machines, tablets, and medical devices

These technologies are commonly based on a central Active Directory address book, which permits ICA and RDP sessions and the establishment of a central security policy that includes:

- Universal logins across all peripheral workstations
- Centralized passwords and a password policy for all systems
- Two-factor authentication: the first factor based on the password for the Active Directory account and the second factor generally carried on a certificate stored in a chip card





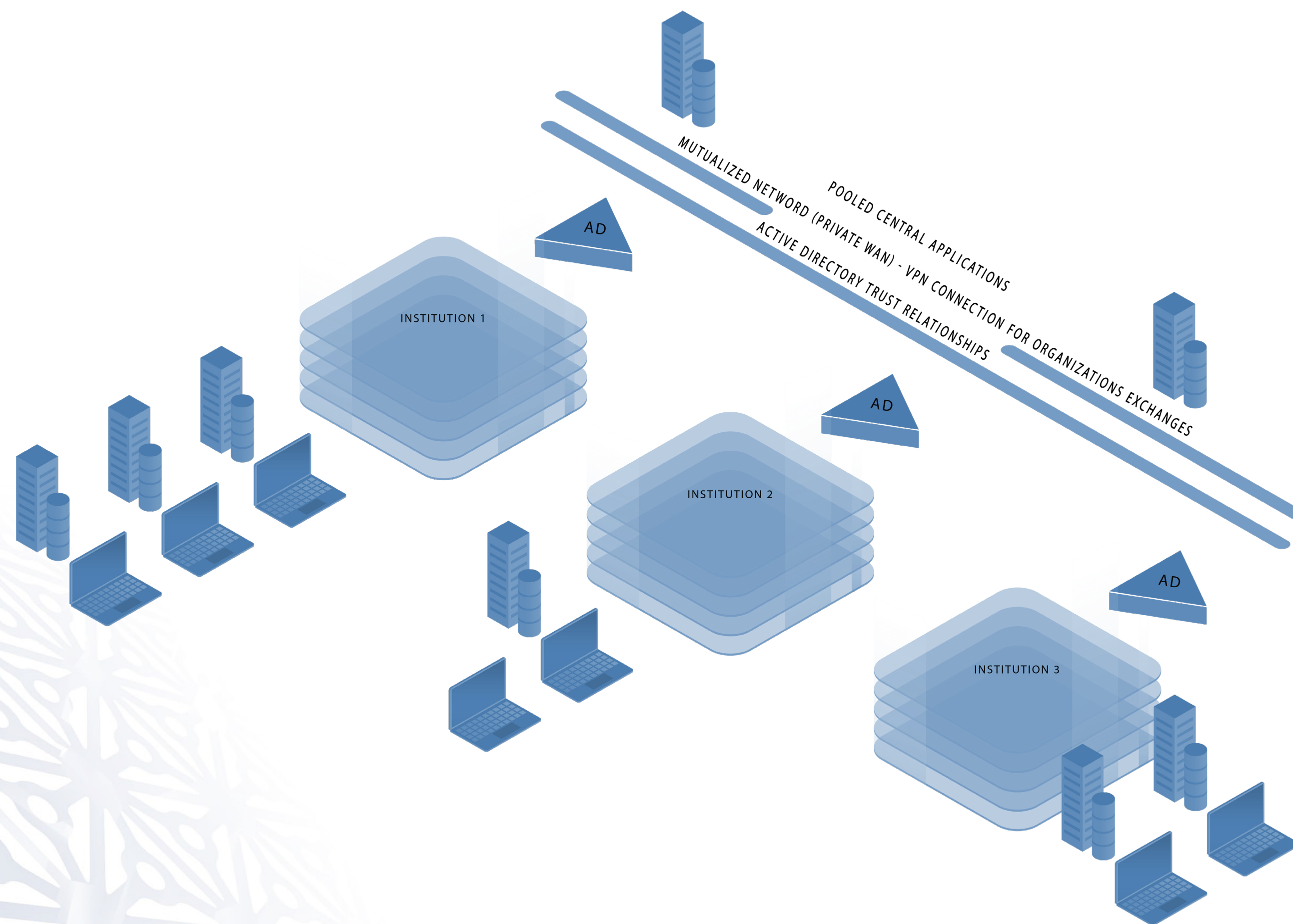


### **Medical health records**

The beginning of the 2000s saw the appearance of widespread reflection on the use of medical health records. In many countries, major advances allowed for more fluid exchange between practitioners, as well as increased traceability for clinical procedures. Most national organizations and bodies seeking to regulate patient data use in the medical sphere organized and enacted drastic security

measures with respect to the sharing and storage of this data. Unfortunately, in many cases, hospital establishments and clinics did not have the financial or personnel means to put such policies into practice. Additionally, the deployment experienced delays despite the daily investment of hospital IT personnel.





## ▲ One underlying tendency: merging hospital centers and clinics

To face up to the increasingly significant investments necessary in the healthcare field, hospitals and clinics began to merge into larger and larger entities. These mergers allowed for the development of economies of scale, notably in the IT infrastructure investments necessary to healthcare professionals. The idea was to have one central organization in charge of streamlining and managing the equipment and software of the different establishments. Globally, this policy proved effective in terms of cost, but it also gave rise to new risks in the IT infrastructure of healthcare establishments—bounce attacks and infection via joint network.

**The shared IT architecture of these healthcare establishment groups can be summed up as follows:**





In a group, the IT architectures are managed by one central team, but the history of different deployments does not allow the centralization of all software. Typically, Active Directory address books that existed before the merger remain present at the different sites, but agreements can be made so that practitioners can be mobile and intervene in the different sites without having to memorize several passwords and security contexts.

Furthermore, in this architecture, one establishment often takes responsibility for hosting one section of the Information System for the rest of the community. For example, Establishment No. 1 could be in charge of hosting the accounting software because the central institution has decided that if they retain only a single type of software for the three establishments, it should be the one historically used by Establishment No. 1. Finally, it is possible that Establishment No. 2 employs IT personnel who are particularly qualified with respect to database environments. Thus, one could decide that all the database applications serving the entire community should be hosted and managed by Establishment No. 2.

**Lastly, there is a significant informatics complexity in the different levels of management and responsibility:**

- Central IT Body – generally in charge of the network, address books, security, and managing new centrally deployed applications
- IT Body Establishment – generally in charge of historical applications within the establishment and the hosting of certain software components that serve the community

This type of architecture and organization is particularly sensitive to ransomware-style attacks that target the Active Directory address book and the file servers. With limited means, healthcare establishments are the perfect target for attacks organized by cybermafia groups, who know how to exploit the weaknesses of this configuration and profit from multifaceted management.







## A PHILOSOPHICAL ASPECT EXPLOITED BY CRIMINAL GROUPS

### The lure of savings and efficiency

Historically, cybercriminal groups exploited “mass” methods without really targeting their victims. These included phishing, automated scripts, mass firewall scans, etc. The trend has now evolved toward precise targeting of victims achieved by using personalized leverage. Malicious attackers must also obtain high yield. We sometimes forget that this is an industry, and as such has the same characteristics as «classical» industry: investment, deployment, and return on investment.

In the last two years, cybercriminal groups have set their

sights on specific targets—first of all potential high-yield victims, which is to say private businesses with high profit margins (e.g. the banking sector, the financial sector, the pharmaceutical sector, etc.) We are now seeing an evolution toward targets without significant financial standing but which can cause great psychological harm; that is, healthcare establishments.





### Life or death

Imagine the following scenario: a person with an illness goes to a hospital facility for a diagnosis, and once their medical checkup is done, it is decided that they need to be operated on the next day. During the night, a cryptovirus encrypts all the patient's data--the blood tests, the notes from the anesthesiologist, the surgery protocol, etc. Their life now depends on encrypted data. What should be done? Should the ransom be paid? Should the patient's life be risked to maintain an ideological stance (i.e. never pay a ransom, no matter the cost)? Is the data necessary for treating the patient guaranteed to be recovered once the ransom is paid?

None of these questions has a simple answer, and the psychological impact of taking risks on the health of a patient is complicated to determine. Cybercriminal groups have

perfectly detected this weakness anchored in our modern societies. By targeting healthcare facilities, they operate in a sector where money is secondary in philosophical terms and the leverage for forcing ransom payment is greater than just the financial statements of a given organization. We do not take risks with human life, and we judge it "priceless." But cybercriminal groups see in this dogma the right price for their mafia actions.



## Conclusion

As we've seen, healthcare facilities have their own unique IT characteristics, notably a historical IT environment based on Microsoft technologies using classic components—Active Directory address books, TSE and Citrix servers, and Windows file servers. These infrastructure components are especially vulnerable to cryptovirus attacks. What's more, the tendency toward concentration in the sector is structured around interconnectivity between several facilities previously separated but now sharing IT resources (networks, address books, applications, etc.). An attack on one facility can infect an entire group.

This environment must be made secure via an ensemble of good practices:

1. Establish and put into practice a security plan for Active Directory address books that are already present. Ransomware uses Active Directory to escalate privileges and deploy malicious code across the whole facility. Obsolete Active Directory designs need to be revisited and the security deviations that appear in address books over time need to be monitored in real time.

2. Generalize the deactivation of obsolete file access protocols such as SMB V1.
3. Assure that no user is local administrator for their workstation to avoid facilitating the attackers' task. Doing so will implement a minimum standard of cyber-hygiene for the initial network access points.
4. Verify that the servers hosting RDP and ICA terminal services are well patched, as recent types of attacks targeting these protocols are frequently used by cybercriminal groups.
5. Finally, ensure that functional backups exist and are stored separate from the facility's traditional network.

**We invite you to consult the Alsid website ([www.alsid.com](http://www.alsid.com)) to discover how the Alsid solution for AD can help you start to modernize your security plan.**





