VareseNews

Once, they damaged people, today data. The business of cybernetic seizures

Pubblicato: Lunedì 22 Novembre 2021

It’s a global business, the new frontier of economic warfare among the great powers. In Italy during the first half year of 2021 the hacker attacks exceeded the amount of 3.6 million.

At the night of 9th July 1973 **Paul Getty III**, a sixteen-year-old boy, was kidnapped in Rome, between Piazza Navona and Trastevere where he usually sold handmade little necklaces. The authenticity of the kidnapping has long been questioned because of the teenager’s personality and lifestyle. It was thought that the unruly chic hippy, heir of one of the richest families in the world, who was on familiar terms with drugs, had staged a kidnapping in order to get money out of his grandfather **Paul Getty II**. The latter declared from London that he wouldn’t pay even a penny for the ransom. “I have many grandchildren, if I pay for one of them, I will have to pay for all of them”

The turning point came on 14th November when an envelope with a tuft and an ear (sent 28 days before by post) was delivered to the newsroom of the Italian newspaper *Il Messaggero.*

Eight days after, a phone call informed the telephone operator of the Italian newspaper *Il Tempo*: “There are some photos of Paul on the highway Roma-Napoli, near Valmontone. Five polaroid photos inside a box. The photos of the boy without an ear.” There was also a message: “The richest family in the world

show to be also the most criminal, like Cain." And the kidnappers threatened other mutilations.

Finally, from his mansion the grandfather gave up. The teenager's mother started to negotiate with the kidnappers. On the 12th December an emissary of Getty's handed over the money: **1.7 billion liras**. Seventy-two hours later the boy was set free between Basilicata and Calabria, near Lauria.

THE NEW BUSINESS OF "KIDNAPPING"

After 50 years, **the "kidnapping" in the age of economy, based on the value of data**, have changed targets and technologies. Comparing to the careful selection of the richest people at that time, nowadays we all are a potential market for "kidnappers".

In April 2021 a minor publisher of school books of the Midwestern **USA** was attacked by a **hacker**, named **Woris**, who threatened to block all online service activities for the primary schools, the company's most important customers, if they didn't pay a ransom of **$1.75 million**. To increase the pressure, Woris threatened to get in touch with the families to inform them about his intention to pass pedophile information in order to create fake identities with which they would create documents, which would allow them to access schools as if they were relatives or parents.

The hacker worked with the support of **DarkSide**, a Russian group which provided hacking services to criminals all over the world. It's disarming to read the tone of the service chat conversations used for the "customers". Woris wrote: "I was proud seeing my soul's wickedness when I made up the fake story about the pedophiles." And then: "The control panel of your customer service is difficult to use and makes me waste lot of my precious time.

At this moment, even **hackers with mediocre technical skills** can become a threat to the national security of the Countries, since thanks to services like the ones of **DarkSide**, since closed and substituted with others like **BlackMatter**, the intellectual barrier at the entrance is extremely low. Just like Microsoft provides software-as-a-service, in the same way **criminal gangs provide technical assistance to hackers**, negotiate with those who got hacked, **process the payment in cryptocurrencies**, provide personalized communication campaigns to put pressure and, if needed, block secondary systems so as to facilitate the ransom demand. They do have **a price list, which goes from a commission of 25%** for **up-to 500,000 dollar** ransom **to 10% for amounts over $ 5 million.** During the years of COVID, **cybernetic seizures' activities** have exponentially increased, becoming an extremely structured "**business**". Some people "punch" the safety net, some others have the task to **take control of systems and data**, some provide the technical support to handle the laundering of the ransom; some others even deal with the relations with the media and handle the dealing with the security authority.

HOW A CYBER ATTACK WORKS

The first thing happening is that the victim receives a message on the screen with some instructions and mild threats, in which it is explained that computers, servers and data have been encrypted and all the back-up copies deleted.

To **decrypt the information**, you have to access a site through a given special key. The following

message is that every attempt to recover or autonomously unlock the data implies the danger of damaging them permanently and making them invisible. Furthermore, you are informed that your confidential data have been stolen and duplicated in order to be sold and broadcast to other organisations, which may threaten to publicize them. **And then the negotiations for the "release" start.**

WHY ARE THE ORGANISATIONS LOCATED IN RUSSIA?

One of the reasons these organisations are often located in **Russia** is that all the people and institutions based in the **States of the former Soviet Union** are protected from the attacks, to avoid Putin's claws being activated against them. Basically, it is a lethal partnership. The **Muscovite authorities** declared in public that they **will not prosecute cybernetic criminals** for attacks performed beyond their borders. After the tax havens, also the online crime free zones arrived.

IN ITALY THE NUMBER OF ATTACKS EXCEEDED THE AMOUNT OF 3.6 million.

What do the American pipeline, Olympus, the global Japanese company in biomedical technology, the Italian region of **Lazio**, and the San Giovanni Hospital in Rome **have in common?** They all have been victims of attacks in 2021. Between the '70s and the '90s almost **600 cases of kidnapping** took place in Italy for the purpose of extortion. During the first half year of 2021, **hackers' attacks exceeded the amount of 3.6 million in Italy only.** This is a **93% boom compared to the one of the same period of the previous year**, when the intrusions reached the amount of 1.9 million . Globally speaking, **Kaspersky**, a leading company in cybersecurity, **has detected 1.5 billion attacks against devices, Internet of Things** (IoT) during the first half of this year. Not only from Russia, obviously. This business has become global and this is the new frontier of economic warfare among the great powers. Facing this evolutionary scenario, we all are called to have a strong awareness of attitude, protection and prevention systems at all levels.

"**The problem is not the problem. The problem is your attitude about the problem. Do you understand?"**, Jack Sparrow.

Translated by Riccardo Cigna and Giada Colnago

Reviewed by prof. Robert Clarke