Cybercrime: On the Trail of the Internet Extortionists

Each year, criminals make billions by attacking computer systems and extorting their victims. Those behind the misdeeds are seldom caught. […]

Von **Kai Biermann**, **Astrid Geisler**, **Herwig G. Höller**, **Karsten Polke-Majewski** und **Zachary Kamel**
10. Juni 2021, 5:19 Uhr

Petro Ponomarenko* wants his money back. And his computers. He needs the money for his child, who is suffering from a heart ailment. And he needs the computers to earn a living, even if they are old. "I bought everything on flea markets like eBay," he says. He claims to have used them to perform a bit of maintenance on servers belonging to regular customers, for $40 to $80 a month each. For other customers, he says, he has helped install new programs or transfer data from one computer to another. A kind of digital janitor: That's the image he would like to portray.

Investigators from Germany and the United States, though, believe that Petro Ponomarenko is a key player in one of the most significant instances of digital extortion in recent years. They believe the 48-year-old is a central player in a worldwide criminal network. Even just having found Ponomarenko is a huge success for investigators. Authorities, after all, are almost never able to track down those involved in cyber-extortion operations. Mostly, in fact, they can't even figure out who is behind them.

A team of reporters from DIE ZEIT and the public broadcaster Bayerische Rundfunk was able to establish contact with Petro Ponomarenko. He insists he is innocent, saying he was working on one of his computers when police clad in bullet-proof vests forced their way into his apartment. They searched his numerous PCs and confiscated a significant amount of cash. "They said that the servers were being used to control a dangerous extortion software," he says. "I didn't know anything about it."

On Jan. 26, 2021, police raided a decrepit, prefab concrete residential building in the Ukrainian city of Kharkiv, where Ponomarenko has an apartment. The police filmed the operation, a video which DIE ZEIT has obtained. It shows them hammering on a steel-reinforced door in the darkened hallway and yelling "Police!" One of the officers manages to break down the door with a crowbar. Inside, the police find a computer, its side panel removed and the fan still on. They also discover other computers, loose hard drives in a plastic container, mobile phones, a workbench with a soldering iron, power strips, keyboards and tools. A server with several drives stands in a cabinet.

For the investigators, the raid was the climax of a complicated, multi-year investigation. And finally, they found themselves standing in the machine room of the extortion network behind the malware Emotet, a program that has been used to blackmail companies, institutions and private persons – a total of more than a million victims.

On the day of Petro Ponomarenko's arrest in Kharkiv, police in the Netherlands also seized servers in several data centers. In Germany, 60 police officers were involved in the operation. Investigators from Lithuania, France, Britain, Ukraine, the U.S. and Canada also helped out. Together, they managed to gain control of Emotet and disarm the software.

With that, the international team of investigators was able to land a blow against one of the most lucrative and least risky crimes in the world. According to a 2019 survey performed by the technology association Bitkom, German companies alone estimate they have suffered damages of up to 10.5 billion euros due to extortion using stolen and encrypted data. Last year, the insurance giant Alliance ranked such cybercrimes as the most serious risk facing companies.

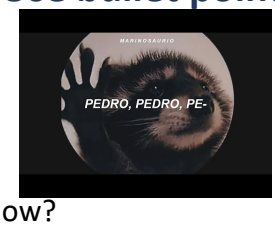
There are dozens of malware programs like Emotet out there, all operated by criminal groups. They usually adhere to a similar pattern: The perpetrators sneak into their victims' computers by way of innocuous-looking email attachments or take advantage of security loopholes in widely used software programs. Malware is thus able to infiltrate the targeted computer network, snoop around, copy data and then encrypt the system such that nobody but the attackers themselves can access it. The cybercriminals only provide the decryption code once ransom money has been paid – and not always even then. Frequently, they will threaten to make the information they have stolen public: customer lists, company secrets, internal financial information and personal data.

For the victims, each attack translates to significant losses of money and data, along with a damaged reputation. Just recently, a pipeline operator in the U.S. had to suspend operations due to a cyberattack. In another attack, extortionists published notes from hundreds of therapy sessions to put pressure on a Finnish chain of psychiatric clinics. The University Hospital of Düsseldorf, meanwhile, had to close down its emergency room and cancel several operations following an attack, because doctors no longer had access to patient files and were unable to prescribe procedures. Copper manufacturer KME in Osnabrück paid a ransom of 1.27 million euros to be able to continue operations. In January, the internet service provider Netcom in Kassel lost access to its entire internal administration, accounting department, email system and the data of 32,000 customers. The town of Neustadt am Rübenberge had trouble paying out parent leave allowances.

It is extremely difficult to track down the perpetrators of such crimes. They never meet in person and frequently only know each other under assumed names. And each is only responsible for a single link in the chain. One writes the programs, another disseminates them, a third sets up and maintains the series of servers used to access the victims' computer systems. Still another negotiates with the victims and, finally, someone is responsible for moving the extorted money through dark channels to recipients around the world.

[…]

Task: Answer the questions in English. Use bullet points and mark the respective paragraphs in the text.



1) Describe Petro Ponomarenko.
2) Give a picture of the police raid.
3) What pattern do the cybercriminals often follow?
4) Name three different victims of cybercrime and how they were affected by the attacks.
5) Why is it hard to track down the individual criminals?