The cesspool of the internet is to be found in a village in North Holland

nrc.nl/nieuws/2021/04/02/the-cesspool-of-the-internet-is-to-be-found-in-a-village-in-north-holland-a4038369

Carola Houtekamer, Rik Wassens

Leeslijst Onderzoek

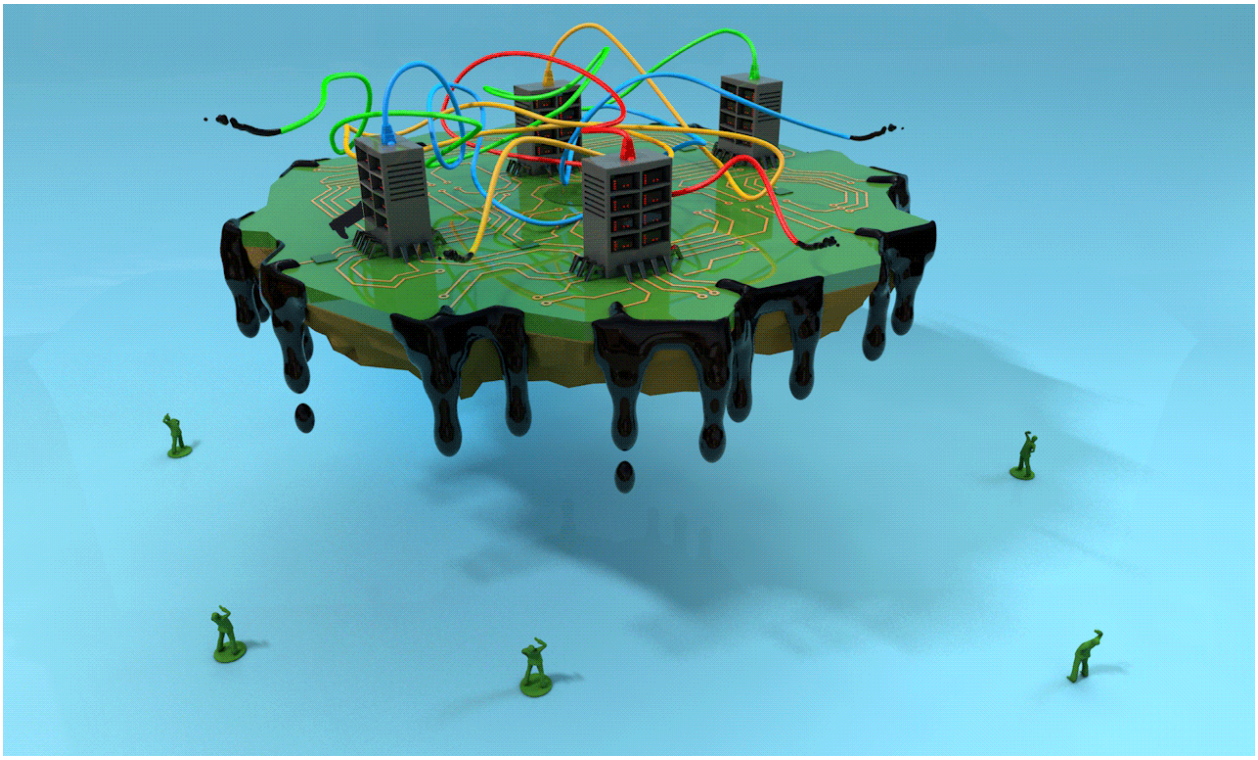
Hosting In the village of Wormer, there is a data centre run by two men from The Hague. For years they have been under investigation by the authorities in connection with cybercrime, malware and child pornography on their network. But that has not deterred the two men.

Leeslijst

- Auteurs
  - Carola Houtekamer
  - Rik Wassens
- Gepubliceerd op 2 april 2021
- Leestijd 19 minuten

Leeslijst

Zoom in Zoom in



Animation Roland Blokhuizen

At the beginning of 2012, the British internet activist and security expert Jart Armin received an email from the High Tech Crime Team of the Dutch police. Would he be willing to drop by to discuss the Dutch company Ecatel?

Finally, he thought. Armin was more than willing, because he was totally fed up with that company. For years he had seen how the internet was being polluted from Ecatel's network and for years he had been in conflict with the owners. His anti-cybercrime organisation Host Exploit had repeatedly placed Ecatel at the top of its list of the world's worst hosting companies, but with no result, apart from threats of legal action from the company.

So yes, he certainly did want to talk to the police. Hopefully, there would finally be a criminal investigation into the company and it would be shut down. At the end of February 2012, with a thick report under his arm, he flew from the UK to the Netherlands for a meeting in Driebergen. He was met by the police at the train station.

He spent the entire day talking to the police about all the malpractices at Ecatel. About the large volume of spam, malware and DDOS attacks originating from the network, the deluge of child pornography found on it and he spoke about a large Russian cybercrime organisation, the Russian Business Network, which, he said, used Ecatel's services. And about networks of hacked computers, the dubious sale of medicines and the malicious websites that try to install viruses in the computers of unwary visitors. A suspiciously large number of such cybercriminals are clients of Ecatel, he told the police, and they conduct their activities on the internet unhindered, despite complaints from network managers around the world.

At the end of the day, Armin received a bottle of jenever in thanks. „But the customs made me throw it away before the return flight. I couldn't even take a sip." He left behind his file with more than a hundred pages of evidence.

Nine years later, Armin is sitting in his pied-à-terre in Amsterdam opposite two reporters. „How is it possible that it still exists?" Because apart from a few name changes, everything is more or less the same at Ecatel. An incredible amount of hacking, child pornography and other harmful information and sites can still be traced to the network – most recently from *Vizier op Links*, a Dutch radical right-wing group that intimidates politicians and activists.

The only thing that has changed is the list of agencies that have taken an interest, with little success, in the activities of the company – the police, the Dutch Fiscal Intelligence and Investigation Service (FIOD), the Ministry of Justice and Europol. That list has only grown longer, research by *NRC* has shown. Meanwhile, Ecatel's owners continue to earn large sums of money from the cesspool of the internet in a data centre in the province of Noord-Holland.

Complex web

Several times a week, two distinctive individuals from The Hague arrive in a car at an industrial site in Wormer, a town about thirteen kilometres north-west of Amsterdam. They are Bap K., a 75-year-old man wearing tinted glasses, and his 34-year-old business partner in The Hague, Reinier van E., a large, bald, muscular figure in a tracksuit. They often bring two dogs with them to work. They bark at passers-by from the data centre's front garden.

The story begins on 13 May 2002. Bartholomeus Johannes K., then aged 56, forms a company that he calls Colinks, describing it as an 'automation service agency'. Bap, as he calls himself, was born in The Hague, lived for a while in South Africa, and now plans to earn his money in the rapidly growing hosting business. The Netherlands is a stable country and an excellent location for the business with its reliable energy network and the large deep-sea internet cables that come ashore in the country. Bap quickly hires Reinier van E., a teenager from The Hague, to take care of the technology.

Together they start a hosting company, with Bap handling the administration and Reinier the computers. For a fee, clients can rent a server from them on which to run their internet service. Bap and Reinier arrange the computers, the energy and the internet access – a little like a landlord letting a room – and the clients operate their own online business from that location. What customers do with their rented server is entirely up to them. Some cut up their space on the server into hundreds of units and sublet them to others.

In the ensuing years, Bap and Reinier build a complex web of private companies in various countries. Reinier has only just reached adulthood when he and Bap form the British limited company Ecatel, at an address in Kent that also houses hundreds of other shell companies. Their other hosting companies, or variations of them, are given names like Novogara, DataZone, Reba Communications, FiberXpress, B&R Holding, iQarus, Incrediserve and Linkup. Some of the companies carry on precisely the same activities from the same address, but under a different name. Some of the companies offer to sublet servers, as though the men were their own clients. Other companies surface – according to the authorities – belonging to the men – such as Quasi Networks and IP Volume, with anonymous directors in the Seychelles. Years after its establishment, a British company is registered in the name of the data centre's caretaker, who lives in a flat in Zaandam.

Almost from the beginning there are complaints about the two men. If equipment they order is not available they are immediately at the door with a complaint, one dealer wrote on a website in 2004. „Unfortunately not in a normal fashion, so I'm finished with them." Another grumbles that Bap and Reinier will not listen to complaints about spam – unwanted, bulk emails usually sent with the intention of persuading people to part with their money – originating from their servers. „And we have a whole laundry list of other junk that is hosted by those guys," someone writes. „I have already tried a number of times to contact them via their abuse reporting centre and helpdesk, but that's like sending mail into a black hole."

Attack with an axe

The crude style of doing business continues. After a dispute over an unpaid energy bill in 2011, Bap and Reinier leave a data centre in Alphen aan den Rijn to start one of their own. They move into the former Regional Computer Centre for Health Insurers in Wormer, twenty minutes north of Amsterdam. The unobtrusive building is hidden away at the end of a cul de sac on the local industrial site. The corridors and halls in the enormous computer centre are large and empty and only a small area of the building is occupied.

From the front, the data centre looks like a normal business, with a neat path leading up to a glass entrance with the bright-blue logo of DataOne above it. A handful of people are hired for the technology and maintenance.

But things are not so slick behind the façade, according to people who visited the company But things are not so slick behind the façade, according to people who visited the company. The muscular Reinier can often be found behind the stove in the enormous industrial kitchen frying a pan of eggs for himself. Items regularly catch fire in a barrel beside the waste containers. The atmosphere is usually cheerful, as the older Bap again starts bragging about flying adventures and all the women he has slept with. At their ease, the two discuss threatened legal actions. But the tone can change suddenly. “Then it is immediately a stream of curses, ‘fuck off, fucking this, fucking that’”, says one source.

One client tells of the time that the super-fit Reinier chased after him waving an axe. He had come to remove his computers and Reinier felt he was entitled to a large sum of cash. The client did not report the incident to the police because he himself had then given Reinier ‘a sharp nudge’ with his car.

Shielding clients

Bap and Reinier’s business model has also not changed over the years. That model is: know nothing, respond to no one, be obstructive.

And it works, because Dutch law states that a hosting company cannot be prosecuted for the actions of those who hire its servers. It is impossible for a hosting company to know the content of every byte on those servers. But hosting companies are required to take action if they are informed of the presence of illegal content. The question is how quickly and how actively they do so.

For a fee – generally in anonymous cryptocurrencies like bitcoin – customers are actually shielded by Bap and Reinier, according to sources. When the hoster receives an official request from the US to remove copyrighted materials – a DMCA takedown notice – the men do nothing about it, says a person who saw it happen. „DMCAs are just tossed in the wastepaper basket.” Subletters even advertise this ‘service’. „*DMCA ignored*” reads one advertisement offering space in the „*state of the art Ecatel DataCenter, located in*

Amsterdam”. Spammers who keep sending unwanted bulk mailings have no reason to worry, says anti-spam organisation Spamhaus. It stops briefly after a complaint, but „after three days” it resumes from another location in the network, says data analyst Carel Bitter, who sent a list with more than 1,500 reports of spam, malware and other malicious material originating from the men’s network.

The Dutch Centre of Expertise for Online Child Abuse (EOKM) also comes up against a brick wall in confrontations with the two men. When the EOKM’s hotline learns of dubious material on the duo’s network, it sends a notification to their company. It has been agreed in the sector that material must be taken offline after a notification. But it regularly occurs that the hotline first has to prove to the client of The Hague duo that the child in the image is actually a minor. If the notifications in fact arrive, that is, since the staff of the EOKM have found that they sometimes end up in the spam folder or that the hotline’s email address has suddenly been blocked. For reasons that are unclear, the web form that the two men drew up for reporting gruesome images is designed in such a way that the system can only handle five reports an hour. That is unworkable, according to the hotline.

Jovial tone

Foot-dragging and obstruction are the tactics they employ, agrees Jos Klaus, a lawyer who brought a case against Ecatel for a consortium of watchmakers in 2013. His clients had found that various fake versions of their expensive watches were being sold on sites hosted by the company. Communication with the company proved a struggle. Bap only replied to the first letter after a week, says Klaus. When Bap received the IP addresses that he had asked for, he replied that he would only accept the letter in Word format, not in PDF, says Klaus. „The reason was that he wanted to ‘cut and paste’.” Nothing more happened after that, leaving Klaus with no choice but to institute proceedings and Ecatel had to be ordered to remove the websites by the court.

Tim Kuik, director of copyright organisation BREIN, says he was told by the men that he had to stop sending legally formulated letters of complaint. „They wanted a meeting where I would tell them what was wrong in a jovial tone, and then they might look at it.” At the same time, they hid behind their web of companies. In 2017, Kuik had to issue a writ against the men to get them to provide information about one of their international companies. They denied any involvement and referred the matter to their caretaker, who was named as the company’s director. He appeared nervous as he told his story in court.

Throughout the years, the complaints keep on coming. Zeus, a large botnet used to steal bank details and to install ransomware on computers, is found to be running partly on servers managed by them. Football matches in the English Premier League are being

streamed via their network without the organisation's consent. Clients that have been turned away by legitimate internet companies switch over to Ecatel. A former employee of competitor LeaseWeb: „We would then see them resurfacing on Ecatel."

Cat-and-mouse game

The Dutch police's High Tech Crime Team knows that things are not right at Ecatel. Around the time of Jart Armin's visit to Driebergen in 2012, they turn up at the former computer centre in Wormer with notable frequency. International investigative services are regularly looking for a client of the two men and at their request the Dutch police have come to copy a server at the men's company.

Bap and Reinier are usually unconcerned about the arrival of the police. They feel invulnerable. On one occasion the police had arrived in response to a request from the US, says a source. Would they like a cup of coffee? A guided tour? During an inspection of a diesel generator, Reinier told the police with a smile that he had programmed it himself and given the electrician a few hundred euro to attach a seal to it.

There are other times when the visits proceed less smoothly and the police officers have to threaten to break down the front door unless it is quickly opened. But it remains a game of cat and mouse without any consequences. According to sources, the Public Prosecution Service had no interest in a serious criminal investigation to show malicious intent on the part of Bap and Reinier.

However, a growing number of agencies start to take an interest in Ecatel during this period. The company's name regularly crops up at meetings of a working group that oversees the 'notice and takedown' code of conduct. This voluntary code was drawn up by the internet sector in 2008 at the request of the government and provides that in the event of a report of child pornography or other banned material, hosting companies must immediately take the information offline.

The code of conduct works well, says the chair of the working group, Maarten Simon of domain registration agency SIDN, but the volume of child pornography in the Netherlands has remained appallingly high. „One name that always came up over the years was Ecatel. It had never endorsed the code of conduct and did not adhere to it. That undermined the code." Why is nothing being done about this, Simon asked at a meeting with representatives of the police, the prosecution service and the ministry of Justice. „It is difficult," they said. „If we issue an order to remove material, they remove it just in time." Alex de Joode, now a compliance officer with the internet hub AMS-IX, attended those talks. „Everyone said: we have to do something about them. But it was not a priority. It was apparently not an exciting project."

In 2015, the High Tech Crime Team approached professor of cybersecurity Michel van Eeten at TU Delft. „The top of the police force was sick and tired of being criticised at international police conferences about all the garbage standing on servers in the Netherlands," they said. „Everyone knows about Ecatel," they added. But it was all anecdotal evidence. Gossip, rumour and poor statistics. The question was whether we could prove which Dutch hosters were spreading the most garbage."

Van Eeten helped the police by providing a list in which he compared the volume of harmful activity from a network – child pornography, cyberattacks, spam and phishing – with the size of the company, he said via Teams. Ecatel was in the top ten. „But that doesn't actually help at all. You have to measure how willing a company is to remove the nasty material. And even that tells you nothing, because a consciously malicious hoster will in fact do his best to look good and will react to notifications, while in the background helping his client, by quickly relocating a site for example." You actually have to show that a company is consciously cooperating with criminal behaviour, says Van Eeten. „But that is very difficult to prove. This has frustrated the police for years."

Detection system

The state of affairs changed when Ferd Grapperhaus of the conservative party CDA took office as minister of Justice in 2017. It quickly became clear to everyone that Grapperhaus was thunderstruck by the Netherlands' position in the worldwide rankings of countries hosting child pornography. He was determined to do something about it. He told *The New York Times*, which had identified the men in Wormer in an investigation into three notorious child pornography websites: „I did not realise the extent of the cruelty, or how far it goes." Among the large quantities of photos of laughing children in sexy poses, the sites also contained explicit and violent images with babies and infants.

In March 2018, a large group assembled for a meeting chaired by the Dutch ministry of Justice and Security. The national public prosecutor for child pornography was present, as well as representatives of the working group for the hosting sector's code of conduct, the internet sector, the ministry of economic affairs, the EOKM, the police's child abuse team in Zoetermeer and professor Van Eeten from TU Delft.

Among the large quantities of photos of laughing children in sexy poses, the sites also contained explicit and violent images with babies and infants
Grapperhaus instituted a number of measures. A technical system for detecting child pornography – a *hashcheckserver* – would be set up that hosting companies could join. Images, discovered during criminal cases in the Netherlands and elsewhere, that were stored by hosting companies and appeared in the system would have to be removed immediately. Civil servants would explore the possibility of establishing a 'content authority' with powers to impose fines on recalcitrant hosters. The code of conduct would also be less voluntary in nature. Companies would have to respond to a notification from the child

pornography hotline without discussion within 24 hours and Van Eeten would be asked to monitor compliance by companies. At the urging of the Dutch House of Representatives, Grapperhaus would publish Van Eeten's list of companies that did not comply: *naming and shaming*.

This led to the appearance of a first public report at the end of 2020, in which the hosting company IP Volume came alternatively second and third in the rankings of the principal sources of child pornography in the Netherlands. Despite its registration in the Seychelles, the agencies all assumed that IP Volume operates from the Netherlands and is one of the maze of small internet companies built up around the two men from The Hague.

But Van Eeten was unable to tell how quickly IP Volume responded to notifications from the child pornography hotline. In a letter to parliament in October 2020, Grapperhaus explained that IP Volume „does not cooperate and even erects (technical) obstacles" to the hotline. The notifications are therefore being sent by the police in order to increase their „binding nature". But, Grapperhaus also observes, none of this really helps – IP Volume remains lax.

In the wake of his roundtable meeting, the minister instructs his officials to explore what measures can be taken under criminal law against malicious hosting companies. It proves very difficult. It not only has to be shown that a company is consciously facilitating the client, the exceptional international character of the internet is also an obstacle. The question is always who is responsible for the illegal content and whether the content is on a site that has been sublet or has been diverted to another country. What if the country where a client is registered will not cooperate with a criminal investigation? And what if the client cannot be found? The internet is everywhere and nowhere at the same time.

Theft of IP addresses

At the end of 2019, another agency appears on the list of authorities that are interested in the men from The Hague. That is the European police agency, Europol.

It becomes involved through the work of internet activist and investigator Ron Guilmette, who is watching angrily from the other side of the world in the United States. Guilmette is an internet veteran, who worked on the world wide web when it was still called ARPAnet in the 1980s. In the following decade, he observed with dismay as the fantastic scientific project, based on voluntary agreements between well-meaning parties, filled up with filth and spam. He has a particular hatred for spam. „It is a strange fascination," he says via Skype. „I simply wanted to preserve email for humanity. Spammers are destroying that."

In his nightly hunts for spammers, Guilmette came across something strange: a possible theft of an enormous series of IP addresses, with a street value in the millions of dollars. The addresses belonged to African companies and organisations, but seemed to be managed by

a small company in Wormer. He wrote outraged posts about it on mailing lists of network operators, but there was no reaction.

Together with a South African journalist, Guilmette worked out how the putative theft must have occurred. In a technical journal they described how an Israeli businessman had falsified the information about the ownership of the IP addresses at the internet authority for Africa. They described how the addresses ended up with a businessman in the Dutch province of Limburg and then came to be managed by Bap and Reinier's network.

It is no coincidence that the African addresses acquired in this dubious fashion reached the two men, said Guilmette via Skype. „Everyone, every website, every device connected to internet needs an IP address, otherwise the data doesn't arrive," he said. „But as everyone knows, the IP addresses are running out and are therefore worth a lot of money." Malicious individuals need even more IP addresses, he adds. „Their addresses are often blocked after some time and then they need new addresses for their spam and their attacks."

There was little follow-up to the articles, except that the African internet authority publicly acknowledged at the beginning of this year that there is something strange going on with those addresses and that it had lost 2.4 million IP addresses.

Frustrated, in September 2019 Guilmette personally contacted Europol about the company run by the two men from The Hague. They asked to meet him, together with the Dutch High Tech Crime Team and the FIOD. A Skype meeting was then arranged with a team of police officers and civil servants at which Guilmette laid out what he had discovered. „They wanted to know everything and said they would let me know what was being done with the information. But I never heard anything more from them."

Raid

On the morning of 22 September 2020, twenty cars and vans are lined up at the door to the data centre in Wormer. The car park is full. The FIOD is out in force. Bap and Reinier have to go with them, together with the caretaker, but he is released immediately after being questioned. He has not been seen since at the data centre.

A report of the visit later appears on the pubic prosecution service's website stating that the tax authorities had raided a '*bulletproof hoster*' with seven enterprises, including at least one based in the Seychelles. The public prosecution service believes that the business has avoided paying hundreds of thousands of euro in tax. „Many clients pay in bitcoin and that income was siphoned off through veiled constructions." The FIOD seized the company's records, 70,000 euro in cash and hundreds of thousands in bitcoins, as well as five cars and two tasers.

Was this the best strategy?

Every route had run into a dead end and no one at the agencies knew what to do any more, according to a number of sources. So it was decided to set the FIOD on them. Various individuals referred separately to the case of American gangster Al Capone. „He could also not be caught for anything but tax evasion."

Whether the cesspool has now been cleaned up remains to be seen. People say it was very quiet around the former computing centre for a while, but cars have recently been seen coming and going again.

Bap and Reinier would not comment on the raid. „How do you reach the conclusion that the report on the public prosecution service's website refers to me or to companies associated with me?" Bap said in a written reaction to *NRC*.

The FIOD seized the company's records, 70,000 euro in cash and hundreds of thousands in bitcoins, as well as five cars and two tasers
The men were unwilling to be interviewed by the reporters. But Bap did send three written replies to questions, in which he denied that his network has been used to send malware, manage a botnet or sell fake watches. Above all, he wanted to emphasise that he and his companies play no role in the spread of child pornography. „When anyone reports something that is prohibited by law, action is taken immediately," he wrote.

It is the child pornography hotline that is uncooperative, Bap asserts. It often sends false notifications with reference to images that are not on their servers and refuses to use a tool that he has had developed to report images. That tool can now handle more than five reports an hour, he wrote.

Bap feels that minister Grapperhaus was wrong to mention the name of IP Volume as a company that responds poorly to notifications of child pornography, blaming it on incorrect reports. „IP Volume has demanded a rectification from the minister." Furthermore, he is not the director of IP Volume, he wrote. The director is in the Seychelles. The fact that his business partner Reinier handles the correspondence for IP Volume „does not automatically mean that he is the director."

Little action

Surely someone must be able to put an end to these two men's activities, Ron Guilmette grumbles on Skype. „Two men who allow so much sleaze to appear on the world wide web. I simply don't understand it. It is really a lack of interest on the part of the internet community and the authorities. And that in a decent country like the Netherlands."

For the time being, the internet community is doing little. On the internet, which is in fact a network of smaller networks, not everyone is connected to everyone else. Neighbours have to pass on data. If the companies that give IP Volume access to the rest of the internet were

all to decide to stop doing so, the company could no longer operate on the internet. This is called *de-peering*, and it does occur very sporadically.

But it is highly controversial, says Guilmette. It flies in the face of the voluntary, decentralised structure of the internet. That is why the largest hub, the Amsterdam Internet Exchange, say they won't do it. A spokesman for the exchange: „We are only a highway, we have nothing to do with the content. You surely can't expect us to paternalistically review what such a party is hosting?"

The men have been listening a little more carefully recently, says Arda Gerkens, the director of the EOKM. The hotline has received 24 reports of child abuse this year. „That is significantly fewer than usual. Pressure works." But that pressure has to be maintained. Gerkens: „Every hosting provider faces this problem, some more than others. There are some that pull out all the stops to clean up their act as quickly as possible. Some could do better, but they do remove material without discussion within 24 hours. And then you have one that always causes trouble, and that is IP Volume."

They also listen a little to Spamhaus, says Carel Bitter. „Because if they are blocked, their data will no longer arrive." But the police should actually shut the place down, says Bitter. „It seems as though the public prosecution service does not have the will to conduct a proper investigation into this extremely bad host." Most of the cyber attacks do not affect Dutch targets. The victims of child pornography are generally not Dutch children. „The problem is apparently not serious enough."

Bitter wonders why a hoster is not required to know more about its clients. „Banks have to know who they are doing business with." An email address as a contact detail should not be enough.

Internet activist Jart Armin is also frustrated. „You know, I have had some real successes. We harried the Russian Business Network. We brought down the notorious hosting company McColo. I see the fact that Ecatel still exists as one of my greatest failures."

„Your self-image is simply wrong", he says. „I was at a conference on cybersecurity years ago and met your minister of justice," – he vaguely recognises a photo of one of Grapperhaus's predecessors, Ivo Opstelten. „I told him about Ecatel. 'That is incorrect,' the minister said. 'The Dutch internet is very clean. We check that every day.' You apparently still believe that."

Comments? **onderzoek@nrc.nl**
Illustrations: **Roland Blokhuizen**

About this article Use of initials

Bap K. and Reinier van E. are referred to by their initials because they are suspects in a criminal investigation. For this article, *NRC* spoke to dozens of people who knew the men and/or who work for the agencies concerned. The article is also based on a number of research reports, analyses by cybersecurity companies, reports by anti-spam organisations, court documents, Chamber of Commerce documents, email correspondence, photos and public information from internet databases.

Reactions

Bap K. denies that his and Reiner E.'s network is used to send malware, to control botnets or to sell dubious watches or medicines. The company's negative rating by Host Exploit was „part of a witch hunt". He points out that many legitimate security companies use their services and that their scanning traffic could be perceived as attacks. He and Van E. take action against child pornography.

K. also denies that Ecatel, or any other companies under his management, facilitate the relocation of bad clients. Clients that have been shut down do sometimes come back online via a subletter. "Every provider has this problem. Unfortunately, it is a fact of life." Ecatel ceased to exist in 2017, and K. already left its board of management in 2009, he stresses. Companies that still use Ecatel's name in its advertising in 2021 are „consciously spreading false information".

K. would not answer questions about why IP Volume forwards internet traffic to the IP addresses that were allegedly stolen from the African internet authority. K. says he is not the owner of the IP addresses and does not use them. „Those IP addresses belong to a party in Israel."

The public prosecution service and the Dutch police's National Unit said they were unable to comment on specific individuals or companies. The public prosecution service did say: „The core of the problem of bad hosting is that the existing European and Dutch regulation of hosters is limited and is driven mainly by commercial and economic considerations, privacy interests and freedom of speech. The hosting companies are seen merely as a conduit."

This also complicates criminal investigations, for which the hoster must be suspected of acting with intent. That is very difficult to prove, the public prosecution service wrote. The client and the hoster cannot automatically be summoned to release their communication, because a hoster is not responsible for the client. The police follow that principle.

Vizier op Links' website was hosted for sixteen days by a client of the data centre in Wormer. It removed the site from its network at the end of December because there were so many complaints about it.

The caretaker who worked at the data centre and became director of Ecatel in 2015 did not respond to questions from NRC.

Bad hosting

In 2010 Ecatel ranked first on the list of the world's 50 worst hosting companies compiled by anti-cybercrime organisation Host Exploit because of the scale of the pernicious activity carried on from the network. In 2012 it ranked fourth.

In 2012, the hackers' collective *Anonymous* launched an attack on Ecatel's network, under the name #OpEcatel. The pretext for the attack was the enormous volume of child pornography on the network and the company's inaction in response to notifications.

In 2013, a court ordered Ecatel to remove websites on which fake watches were being sold.

In 2015, Ecatel became embroiled in a lengthy conflict with the Premier League in the UK over claims of illegal streaming of football matches over Ecatel's network. Streams must be removed by court order within 20 minutes of a notification.

In 2020, IP Volume was in the top four of Dutch hosting companies on which the most child pornography could be found, according to TU Delft. Since a year, blocks of ip-addresses of Quasi Networks can be found there.

Translation by Hugh Quigley