THE EUROPOL PODCAST
OFFICIAL TRANSCRIPT

The King of Malware

Introduction

Marijn S., Europol/Dutch Police
It was one big infection factory.

Europol Narrator
Welcome to the Europol podcast, the official podcast of the EU's law enforcement agency. In this series, we shine a light on some of the biggest operations Europol has supported, and how we continue to fight crime.

The King of Malware.

Action Day at Europol HQ

Europol Narrator
On a cold day in January 2021, 30 of Europe's leading cybercrime specialists gathered at the Europol headquarters in The Hague. Today, however, was no ordinary operational meeting. This was the culmination of two years of careful planning and research. Their task was the takedown of one of the most lethal and destructive botnets of the last decade, EMOTET.

Bogdan B., Europol
This one was smooth, went very smooth. It was, as an example of coordination, I would say in 2 hours, 3 hours, we had a plan setup and we followed each step that it was accomplished and it went perfectly.

Europol Narrator
Bogdan is one of the cyber specialists who was at Europol that day.

Bogdan B., Europol
Hi. My name is Bogdan. I'm a specialist working at AP Cyber and one of the, Europol, staff that have been assigned to work on this investigation.

Europol Narrator
These specialists had one chance to implement a new and innovative approach they had developed to take down a botnet this dangerous. This would allow them to dismantle the infrastructure used by the criminals before they did any more damage. It turned out that Operation Ladybird, as it was called, was a great success. But it took a lot of preparation in the years before the takedown to get to that historic day.

This episode, we'll hear from specialists like Bogdan, and take a closer look at the evolution of EMOTET in the seven years before the takedown. We'll investigate how it earned the title of the King of malware, and how the police finally outsmarted the hackers.

Contextualising the problem

Europol Narrator

In recent years, our lives have become more and more entwined with technology. One of the greatest challenges now facing modern law enforcement is the growing prevalence of cybercrime and specifically, malware attacks. Malware is short for malicious software. It is intentionally designed to damage computers and systems, and to facilitate criminal activities such as theft or fraud.

The story of this particular type of malware, called EMOTET, begins in 2014. This is when it was first spotted as a banking Trojan. It aimed to hide inside computers and steal banking credentials from the machines it was installed on. It was consistently ranked number one by internet monitoring groups as the 'most wanted' malware.

Here's Bogdan, explaining EMOTET in more detail:

Bogdan B., Europol

Emotet was and is a prolific malware that was used by cybercriminals to infect computer systems, and basically was used as a base layer for deploying other types of malware that could have, and have impacted, systems and lives of citizens and companies. It was used to, after the initial infection, to deploy different types of malware such as ransomware, for example.

Europol Narrator

That means that EMOTET gave the cybercriminals unauthorised access to computer networks. Then, this access was sold to other top-level criminal groups. These criminals could carry out illicit activities such data theft and extortion through ransomware.
Each case began with the same entry point: a harmless looking email.

So what caused EMOTET to be crowned "the king of malware"? Why was it so dangerous?

EMOTET could be hidden inside emails, either in an attached document or in a malicious hyperlink included in the email. If the victim opened that attachment or clicked that link, EMOTET was in their computer. It was installed without the victim even knowing.

Any devices using the same network as the infected device were vulnerable. EMOTET was able to travel between machines that were using the same network.

Robert Schaap works in a national high-tech crime unit of the Dutch police.

Robert S., Dutch Hi-Tech Crime Unit

My name is Robert Schaap and I'm an advisor in public private partnerships, and they're trying to well, have the private sector engaged in our investigations.

Europol Narrator

And he explains more about how the EMOTET malware spread.

Robert S., Dutch Hi-Tech Crime Unit

One of the ways that the botnet propagated itself was that it used to the email boxes of the bots, the email boxes of the of the people using their laptops to spread new emails to all the contacts of that person. So one infectious computer would send out a lot of emails to people in their contact list. They get an email from somebody they trust, so they open it. But then there's an EMOTET text package attached to that email and they get infected.

So that's the way that it's also used to spread the malware itself.

Europol Narrator

This is where the malware began to show how dangerous it was. While you are unlikely to open an email from an unknown sender, if the email appears to be from a friend or family member then you are much more likely to be tricked into opening it. This then spreads EMOTET further, as it gains access to more and more computer networks.

Once EMOTET infects a victim's computer, this would become part of a larger network of compromised machines. Together, the infected computers functioned as one entity and formed what is known as a 'botnet'. This is essentially an army of zombie computers that can be remotely controlled by criminals.

The criminals ran the botnet using 'command and control servers', which is a network of servers that the infected computers regularly connect to, checking for their new EMOTET commands. The hackers would then send commands to the servers, which would be disseminated to the infected computers.

EMOTET was spreading rapidly around the world. And if, in its cyber-travels, EMOTET infected a machine with a lot of internet bandwidth, they could add it to this command and control network.

Marijn is a specialist who joined Europol's Cybercrime Centre in summer 2022. Prior to this, he worked in the same unit as Robert on the EMOTET takedown.

Marijn S., Europol/Dutch Police

My name is Marijn Schuurbiers.

Europol Narrator

And he explains further:

Marijn S., Europol/Dutch Police

Even your own computer will be upgraded to be become part of the botnet infrastructure because sometimes it has automatically noticed that the infection is on a heavy machine with a lot of Internet bandwidth and calculation.

They say, OK, this is not only worth to steal the data, which is on the machine, but we could use it actually as an important server. And so then did the infection-affected machine is upgraded into the botnet into its infrastructure and will become just a command and control server in the whole factory, rather than only a simple bot.

Europol Narrator

And EMOTET's operators used the botnet to send *more* EMOTET.

They told infected machines to send more automated emails from the victim's email account. This would spread EMOTET further. They were sent to victims' entire contact lists, meaning the malware could proliferate at an alarming rate.

With no borders to cross and no documents to check, in just a few clicks EMOTET could travel across the globe. As it travelled, it could steal more banking information from the machines it was infecting.

Even antivirus software couldn't stop it. EMOTET has a 'polymorphic' design – meaning that each time the malware opened up, it changed its code. The antivirus couldn't recognise EMOTET's code as a risk, because the machine thought it was just another innocent file on your computer, like a word document or image.

So the EMOTET malware was able to hide from detection, and could automatically proliferate itself by sending spam emails. Between 2014 and 2017, EMOTET had infected hundreds of thousands of machines worldwide.

But it was in 2017 that EMOTET evolved into a much more lucrative operation.

Robert S., Dutch Hi-Tech Crime Unit

They're going back to their core business. They used to be a banking Trojan, but it is actually they're very good in getting infections. It's an infection factory. And now monetizing that is easier by selling it on than trying to steal your money from a bank account. So it's just an evolving economy.

2017 evolution

Europol Narrator

Rather than just stealing bank credentials, a serious crime in itself, EMOTET could now act as an open door for other hackers. This could provide access, for example, for ransomware, which locks all relevant computer files until a sum of money is paid. Or for spyware, that steals information from a computer. All the while, the botnet continued to grow as computers worldwide were bombarded with EMOTET-carrying spam, day after day.

With this new capacity, and EMOTET having successfully spammed its way into so many computers, EMOTET had truly earned the name "the king of malware".

Businesses and individuals around the world found themselves the victims of these criminal efforts.

One estimate put the global damage done by EMOTET at around USD 2.5 billion. This generated millions for EMOTET's operators.

Response by Europol and Law enforcement

Europol Narrator

So what was law enforcement doing to respond to this threat?
The police needed to target EMOTET at its source. If the command and control servers could be compromised or taken offline, no commands could be sent to the EMOTET botnet. That stops the criminals telling EMOTET to do their bidding, and that ends the criminal operation.

However, as this was a crime that spanned multiple countries, it was time for Europol to step in to coordinate the action.

Bogdan B., Europol

It's very important for the international coordination to have direct discussion between the countries, to know each other, to understand, everyone what is working on. And at Europol we organised these meetings; in person, virtually. We brought together, I think, more than 100 different investigators, digital forensic examiners, cryptocurrency experts, analysts.

So they would get together, they will discuss on common findings, then investigations there, what we need to do next in the cases. We use these meetings as a platform to coordinate, further steps.

Europol Narrator

With this international collaboration, the specialists involved observed that EMOTET's servers were set up in three tiers. This meant that finding the core command and control servers, housed in tier 3, would require tracing the malware through tiers 1 and 2. These tiers consisted of hundreds of servers located all around the world, from Argentina to South Africa to Taiwan.

In order to legally gain access to these tier 1 systems, private sector companies and law enforcement realised that it was actually beneficial for them to allow themselves to become infected by EMOTET. This would give them access to the EMOTET infrastructure.

Marijn S., Europol/Dutch Police

The way virtually the industry works is that they infect themselves; because how are able to wiretap legally a tier one system - which basically the private sector cannot - but there's one exception if the tier one server is themselves, because you can wiretap yourself as much as you want, right?

So what they do sometimes is like if they have themselves infected with a general malware but do that on a bigger machine, just as I explained earlier that and that's the emotet malware will detect, hey, this is an interesting machine. Maybe to have it upgraded into an upgraded to a tier one server that happens that and then the private sector started monitoring that Tier one system and see where the communications to the tier two layers went.

Europol Narrator

By wiretapping themselves and getting upgraded into the botnet, law enforcement could slowly build a picture of the botnet by seeing who and what their hacked server was trying to connect to. And this is where investigators hit their first roadblock. They found the core of the EMOTET botnet - tier 3 - but it wasn't great news. There were a total three core command and control servers in tier 3, and they were all housed in Russia.

With no way to lawfully access the servers, investigators needed to wait patiently for an opportunity to strike.

But in late 2020, something changed. Why the criminals did this isn't clear, but they decided to move two of the three Russia-based command and control servers. And not to just anywhere – they moved them to the Netherlands.

Dutch law enforcement was now able to lawfully access these two command and control servers. Their activities caused a few hours of downtime – but the criminals thankfully didn't notice. The investigators were now *in*.

The Takedown

Europol Narrator

After a few months of laying in the EMOTET network undetected, the investigators had found a way to take down the malware. To do this, they came up with a plan.

Bogdan B., Europol

We agreed on an operational action plan together that had mainly three pillars. So first was identification and of the suspects of the associates are behind it. Secondly, to identify, monitor, seize and take down the criminal infrastructure. And third, it was the, to seize the financial assets of these suspects.

And each of these pillars have been assigned to be led by specific countries, by specific country.

Europol Narrator

As part of the first pillar in their plan, the investigators had managed to uncover the identity of one of the server admins. They tracked him to an address in Ukraine. Crucially, this led them to the key to the third command and control server, meaning all three servers behind EMOTET were now under the control of law enforcement.

Robert S., Dutch Hi-Tech Crime Unit

Only when the third key was collected, then the whole process of feeding their own binaries to the bots started because we wanted to have all bots.

Europol Narrator

So what did the team do next? They made their innocuous law enforcement binaries available to the network of infected machines. A binary is essentially a file containing a command for the computers in the botnet. These commands would then replace the original malicious payload. A malicious payload, or malware, is a file that the hackers were using to give instructions to computers under their control.

Marijn S., Europol/Dutch Police

From a technical and from a legal perspective, we did not even send the bots that new binary, that updated binary, to have it reconnected to basically police infrastructure. But we basically put it on the servers that we were under our control in a legal way, we confiscated them, we hacked into them.

The bots themselves, they are programmed that each day or each certain amount of hours, they will connect to the command and control server to see if there is any updated malware for them. If there is updated malware, they will pick it up themselves.

Europol Narrator

The law enforcement specialists working on the case now directed all EMOTET requests to a ‘sinkhole’ – a dud IP address controlled by law enforcement. So when the thousands of infected machines connected to the control servers to receive their latest instructions 15 minutes later, they would all receive this final instruction and be sent to the sinkhole instead.

And so in 2021, after more than 7 years of cyber-attacks, EMOTET was taken down.

Bogdan B., Europol

EMOTET was a great example of how law enforcement coordination, at this level should work. All the countries, all the members of the investigative teams from the countries have been fully committed from day one to cooperate. They have understood from the beginning that such a case cannot be run by one specific country, because of the data, because of the entities, because of the number of the suspects investigated.

So they all contributed resources, human resources, technical resources to the common goal.

Conclusion

Europol Narrator

So, is the king of malware dead?

Robert S., Dutch Hi-Tech Crime Unit

As it looks. Where the botnet is down and where the perpetrators are at the moment is still under investigation.

Europol Narrator

That means that EMOTET is still a threat.

This time, however, law enforcement has the benefit of experience. Europol effectively coordinated multiple countries and carried out a seamless takedown. This means that the next time they need to carry out an EMOTET takedown, the response will be even more effective than before.

So if you don't want to be a victim of malware, always update your computer when prompted. Don't open email attachments or click on hyperlinks unless you're absolutely sure of where they came from.

Thanks for listening. If you enjoyed the podcast please subscribe on whatever platform you're using, and tell your friends on social media about us. You can also follow us on twitter via @Europol.