Criminals blowing up German ATMs arrested after joint action

11 December 2019

Authorities in Hungary and Germany, with the active support of Eurojust and Europol, have dismantled a criminal gang, suspected of blowing up three automated teller machines (ATMs) in the eastern part of the German State of Hesse. In a coordinated joint action, approximately 20 premises were searched in Hungary and Germany and pieces of evidence, as well as assets originating from the crime, have been seized. Three out of eight suspects were arrested in Germany. Five more suspects have been interrogated, four in Hungary and one in Germany.

From 2016 onwards, the organised criminal group (OCG) has been suspected of blowing up or trying to explode cash machines in the State of Hesse, with an estimated illegal profit of EUR 285 000, and causing heavy damage to the surroundings of the ATMs. The OCG operated by breaking open the front part of the ATM and pouring explosive gas into the exit port of the machine, where the money usually comes out. With a pipe or a tube, the gas was subsequently passed into the safe of the machine and then ignited, with the explosion opening the vault of the ATM.

A Eurojust-supported joint investigation team was set up in the summer of this year between the Hungarian and German authorities. Eurojust further organised two coordination meetings, the second meeting to prepare for the joint action.

The operation was led by the Public Prosecutor's Office (PPO) of Hajdú-Bihar County in Hungary and the German General Prosecutor's Office of Frankfurt am Main, together with the National Bureau of Investigation of the Rapid Response and Special Police Services (KR NNI) and the police department of Mittelhessen in Gießen, Germany. Europol supported the Hungarian authorities on the ground in Hungary, with one officer, as well as two German investigators, taking part in the actions in Hungary.

Photo © Polizeipräsidium Mittelhessen

Measuring real-driving car emissions: Council agrees on its position

Member states' ambassadors meeting in the Council's permanent representatives committee today agreed on a negotiating mandate concerning the proposal to

amend regulation (EC) N° 715/2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information.

The proposed regulation is intended to provide a sound legal basis for applying pollutant-specific conformity factors when assessing the conformity of light passenger and commercial vehicles with EU tailpipe emission limits.

The agreed text :

- sets the **conformity factors** to be used when measuring the real-driving emissions (RDE) of light passenger and commercial vehicles at the same levels as in the Commission proposal;
- requests the Commission to **review** technical developments relating to the accuracy of portable emission measurement systems (PEMS) every two years and, if appropriate, table a **new legislative proposal** with a view to revising downwards the conformity factors.

Next steps

Following today’s agreement and once the European Parliament has also agreed on its position, the two co-legislators will begin negotiations with a view to the swift adoption of the proposed regulation at first reading.

Background

Pollutant-specific tailpipe emission limits are part of the EU vehicle type-approval legal framework. Over time, they have led to significant drops in emissions of exhaust particles both in terms of mass and number, as well as to a decrease of polluting elements, such as hydrocarbons and carbon monoxide. However, nitrogen oxide (NOx) emissions from diesel engines, in particular those installed in light passenger and commercial vehicles, have not been reduced as much as expected with the introduction of European emission standards, in 1991. One of the reasons behind this insufficient decline of emissions is the fact that emissions in real-world driving conditions tend to be significantly higher than those measured during the previous type-approval tests. Given this discrepancy between emissions measured in laboratories and those measured in real-driving conditions, the Commission introduced in 2016 a new measurement methodology – the **real-driving emissions (RDE)** test procedure. In order to take into account statistical and technical uncertainties of measurements carried out by means of portable emission measurement systems (PEMS), the Commission introduced the so-called “**conformity factors**“. On 13 December 2018, the General Court of the EU annulled partially the relevant Commission regulation, considering that conformity factors could legally be established only by the European Parliament and the Council as co-legislators. The General Court ordered however that the effects of the annulled parts of the Commission regulation be maintained until the adoption of new legislation replacing them by the two co-legislators. The General Court’s ruling has been appealed against by the Commission, Germany and Hungary. If these appeals are dismissed, the two co-legislators will have to enact the proposed regulation within 12 months from

the date of that dismissal.

The agreed text will be made available here on 12 December 2019.

International crackdown on RAT spyware, which takes total control of victims' PCs

Joint Eurojust-Europol press release

29 November 2019

A hacking tool that was able to give full remote control of a victim's computer to cybercriminals has been taken down as a result of an international law enforcement operation targeting the sellers and users of the Imminent Monitor Remote Access Trojan (IM-RAT).

The investigation, led by the Australian Federal Police (AFP), with international activity coordinated by Eurojust and Europol, resulted in an operation involving numerous judicial and law enforcement agencies in Europe, Colombia and Australia. The seamless cross-border interaction between the various authorities was supported on law enforcement level through the Joint Cybercrime Action Taskforce (J-CAT) and on judicial level through the European Judicial Cybercrime Network (EJCN).

Coordinated law enforcement activity has now ended the availability of this tool, which was used across 124 countries and sold to more than 14 500 buyers. IM-RAT can no longer be used by those who bought it.

Search warrants were executed in Australia and Belgium in June 2019 against the developer and one employee of IM-RAT. Subsquently, an international week of actions was carried out this November, resulting in the takedown of the Imminent Monitor infrastructure and the arrest at this stage of 13 of the most prolific users of this Remote Access Trojan (RAT). Over 430 devices were seized and forensic analysis of the large number of computers and IT equipment seized continues.

Actions were undertaken this week in the framework of this operation in the following countries: Australia, Colombia, Czechia, the Netherlands, Poland, Spain, Sweden and the United Kingdom.

A powerful computer highjacking tool

This insidious RAT, once installed undetected, gave cybercriminals free rein

to the victim's machine. The hackers were able to disable anti-virus and anti-malware software, carry out commands such as recording keystrokes, steal data and passwords and watch the victims via their webcams. All that could be done without a victim's knowledge.

This RAT was considered a dangerous threat due to its features, ease of use and low cost. Anyone with the nefarious inclination to spy on victims or steal personal data could do so for as little as US$25.

Victims are believed to be in the tens of thousands, with investigators having already identified evidence of stolen personal details, passwords, private photographs, video footage and data.

Daniela Buruiana, National Member for Romania at Eurojust and Chair of its Cybercrime Team, said: *'The cybercriminals selling and using the IM-RAT affected the computers of tens of thousands of victims worldwide. We would like to thank all the judicial and law enforcement authorities involved for the excellent results achieved in this operation. These authorities have shown an extremely high level of commitment and legal and technical expertise. Effective cooperation and coordination among all the relevant actors are vital in overcoming the obstacles to investigations due to the global scale and technical sophistication of this type of crime.'*

Steven Wilson, Head of Europol's European Cybercrime Centre (EC3), said: *'We now live in a world where, for just US$25, a cybercriminal halfway across the world can, with just a click of the mouse, access your personal details or photographs of loved ones or even spy on you. The global law enforcement cooperation we have seen in this case is integral to tackling criminal groups who develop such tools. It is also important to remember that some basic steps can prevent you falling victim to such spyware: we continue to urge the public to ensure their operating systems and security software are up to date.'*

Avoiding RAT-ing

The public and businesses can follow simple steps to help protect themselves from such malware, including:

- Update your software, including anti-virus software;
- Install a good firewall;
- Don't open suspicious e-mail attachments or URLs – even if they come from people on your contact list; and
- Create strong passwords.

For more advice on how to protect yourself against Remote Access Trojans, check Europol's crime prevention advice.

International crackdown on RAT spyware, which takes total control of victims' PCs

Joint Eurojust-Europol press release

29 November 2019

A hacking tool that was able to give full remote control of a victim's computer to cybercriminals has been taken down as a result of an international law enforcement operation targeting the sellers and users of the Imminent Monitor Remote Access Trojan (IM-RAT).

The investigation, led by the Australian Federal Police (AFP), with international activity coordinated by Eurojust and Europol, resulted in an operation involving numerous judicial and law enforcement agencies in Europe, Colombia and Australia. The seamless cross-border interaction between the various authorities was supported on law enforcement level through the Joint Cybercrime Action Taskforce (J-CAT) and on judicial level through the European Judicial Cybercrime Network (EJCN).

Coordinated law enforcement activity has now ended the availability of this tool, which was used across 124 countries and sold to more than 14 500 buyers. IM-RAT can no longer be used by those who bought it.

Search warrants were executed in Australia and Belgium in June 2019 against the developer and one employee of IM-RAT. Subsquently, an international week of actions was carried out this November, resulting in the takedown of the Imminent Monitor infrastructure and the arrest at this stage of 13 of the most prolific users of this Remote Access Trojan (RAT). Over 430 devices were seized and forensic analysis of the large number of computers and IT equipment seized continues.

Actions were undertaken this week in the framework of this operation in the following countries: Australia, Colombia, Czechia, the Netherlands, Poland, Spain, Sweden and the United Kingdom.

A powerful computer highjacking tool

This insidious RAT, once installed undetected, gave cybercriminals free rein to the victim's machine. The hackers were able to disable anti-virus and anti-malware software, carry out commands such as recording keystrokes, steal data and passwords and watch the victims via their webcams. All that could be done without a victim's knowledge.

This RAT was considered a dangerous threat due to its features, ease of use and low cost. Anyone with the nefarious inclination to spy on victims or

steal personal data could do so for as little as US$25.

Victims are believed to be in the tens of thousands, with investigators having already identified evidence of stolen personal details, passwords, private photographs, video footage and data.

Daniela Buruiana, National Member for Romania at Eurojust and Chair of its Cybercrime Team, said: *'The cybercriminals selling and using the IM-RAT affected the computers of tens of thousands of victims worldwide. We would like to thank all the judicial and law enforcement authorities involved for the excellent results achieved in this operation. These authorities have shown an extremely high level of commitment and legal and technical expertise. Effective cooperation and coordination among all the relevant actors are vital in overcoming the obstacles to investigations due to the global scale and technical sophistication of this type of crime.'*

Steven Wilson, Head of Europol's European Cybercrime Centre (EC3), said: *'We now live in a world where, for just US$25, a cybercriminal halfway across the world can, with just a click of the mouse, access your personal details or photographs of loved ones or even spy on you. The global law enforcement cooperation we have seen in this case is integral to tackling criminal groups who develop such tools. It is also important to remember that some basic steps can prevent you falling victim to such spyware: we continue to urge the public to ensure their operating systems and security software are up to date.'*

Avoiding RAT-ing

The public and businesses can follow simple steps to help protect themselves from such malware, including:

- Update your software, including anti-virus software;
- Install a good firewall;
- Don't open suspicious e-mail attachments or URLs – even if they come from people on your contact list; and
- Create strong passwords.

For more advice on how to protect yourself against Remote Access Trojans, check Europol's crime prevention advice.

Criminals blowing up German ATMs arrested after joint action

11 December 2019

Authorities in Hungary and Germany, with the active support of Eurojust and

Europol, have dismantled a criminal gang, suspected of blowing up three automated teller machines (ATMs) in the eastern part of the German State of Hesse. In a coordinated joint action, approximately 20 premises were searched in Hungary and Germany and pieces of evidence, as well as assets originating from the crime, have been seized. Three out of eight suspects were arrested in Germany. Five more suspects have been interrogated, four in Hungary and one in Germany.

From 2016 onwards, the organised criminal group (OCG) has been suspected of blowing up or trying to explode cash machines in the State of Hesse, with an estimated illegal profit of EUR 285 000, and causing heavy damage to the surroundings of the ATMs. The OCG operated by breaking open the front part of the ATM and pouring explosive gas into the exit port of the machine, where the money usually comes out. With a pipe or a tube, the gas was subsequently passed into the safe of the machine and then ignited, with the explosion opening the vault of the ATM.

A Eurojust-supported joint investigation team was set up in the summer of this year between the Hungarian and German authorities. Eurojust further organised two coordination meetings, the second meeting to prepare for the joint action.

The operation was led by the Public Prosecutor’s Office (PPO) of Hajdú-Bihar County in Hungary and the German General Prosecutor’s Office of Frankfurt am Main, together with the National Bureau of Investigation of the Rapid Response and Special Police Services (KR NNI) and the police department of Mittelhessen in Gießen, Germany. Europol supported the Hungarian authorities on the ground in Hungary, with one officer, as well as two German investigators, taking part in the actions in Hungary.

Photo © Polizeipräsidium Mittelhessen