# International coalition dismantles Russian-led Qakbot and Conti ransomware network



International law enforcement agencies have successfully disrupted a crucial malware operation led by Russian cybercriminals following a coordinated global effort that included agencies from the UK, Canada, Denmark, the Netherlands, France, Germany, and the United States. The operation resulted in the issuance of international arrest warrants for 20 suspects, predominantly residing in Russia, while the U.S. has released indictments against 16 individuals associated with the notorious Qakbot and Danabot malware families.

Among those charged is Rustam Rafailevich Gallyamov, 48, noted for his pivotal role in these cybercrime enterprises, alongside Aleksandr Stepanov and Artem Aleksandrovich Kalinkin, both identified by their aliases, JimmBee and Onix, respectively. The U.S. Department of Justice has highlighted the indiscriminate nature of these attacks, which have targeted not only private institutions but also governmental agencies, and have increasingly sought to destabilise nation-states. This month, the high-street retailer Marks & Spencer became a prominent victim, underscoring the escalating risk faced by entities of all sizes.

The German Federal Criminal Police Office (Bundeskriminalamt or BKA) spearheaded the European component of this investigation, which also included public appeals to locate 18 individuals linked to the Qakbot malware. The investigation has particularly spotlighted Vitalii Nikolayevich Kovalev, a 36-year-old from Volgograd, who is already on the U.S. wanted list. Kovalev is reportedly the architect behind the infamous Conti ransomware group, widely regarded as one of the most sophisticated criminal organisations in the cyber realm. His activities have made him one of the "most successful blackmailers in the history of cybercrime," as described by German investigators. They allege he has extorted vast sums from countless corporations, often under disturbing circumstances, such as those faced by healthcare institutions during the COVID-19 pandemic.

Operation Endgame, initially launched by German authorities in 2022, is shaping up to be a benchmark in international cybercrime mitigation efforts. BKA president Holger Münch emphasised Germany's distinct target profile, noting that the nation has found itself particularly attractive to cybercriminals. The BKA's comprehensive investigation looks into the suspects' ties to organised criminal enterprises and gang-related extortion, recognising that these activities often cross borders, complicating enforcement efforts.

The resurgence of ransomware aimed at critical infrastructures is alarming. Between 2010 and 2022, the Conti group notably intensified its focus on U.S. hospitals, demonstrating a predilection for exploiting vulnerabilities within sectors that serve essential public needs. As with many cybercriminal enterprises, the bulk of their operations remains within Russia, though some members are believed to operate from Dubai. While their extradition to face charges in Europe or the US appears improbable, the ongoing identification and pursuit of these criminals may lead to broader disruptions in their operations.

The BKA's initiative follows a series of successful operations across Europe and North America aimed at dismantling various malware networks, demonstrating that collaboration among nations can yield positive outcomes. For instance, the recent dismantling of multiple botnet operations including IcedID and Smokeloader, showcased a growing trend in law enforcement's coordinated response to cyber threats. This collaborative spirit is crucial, as cybercriminals evolve and adapt their strategies in response to enforcement measures.

As the situation evolves, the necessity for continued vigilance and cooperation among global stakeholders remains imperative in combating the relentless tide of cybercrime. The progressive measures being employed in operations like Endgame highlight both the potential and challenge inherent in addressing this digital menace that has infiltrated all facets of modern life.

## Reference Map:

* Paragraph 1 – [[1]](https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation), [[2]](https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation)
* Paragraph 2 – [[1]](https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation), [[3]](https://www.dw.com/en/europol-hits-malware-network-in-major-cybercrime-operation/a-69220251)
* Paragraph 3 – [[1]](https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation), [[4]](https://www.abc.net.au/news/2024-05-31/massive-international-operation-takes-down-ransomware-networks-/103917618)
* Paragraph 4 – [[3]](https://www.dw.com/en/europol-hits-malware-network-in-major-cybercrime-operation/a-69220251), [[5]](https://www.cybernews.com/security/nca-dismantles-huge-russian-cybercrime-network/)
* Paragraph 5 – [[2]](https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation), [[6]](https://www.cybersecurity-help.cz/blog/4674.html)
* Paragraph 6 – [[2]](https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation), [[7]](https://www.cyware.com/resources/threat-briefings/weekly-threat-briefing/cyware-weekly-threat-intelligence-may-05-09-2025)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation> - Please view link - unable to able to access data
2. <https://www.theguardian.com/technology/2025/may/23/russian-led-cybercrime-network-dismantled-in-global-operation> - European and North American cybercrime investigators have dismantled a major malware operation led by Russian criminals. The operation involved police from the UK, Canada, Denmark, the Netherlands, France, Germany, and the US. International arrest warrants were issued for 20 suspects, primarily residing in Russia, and indictments were unsealed in the US against 16 individuals. The charges include the alleged leaders of the Qakbot and Danabot malware operations, such as Rustam Rafailevich Gallyamov, 48, from Moscow, and Aleksandr Stepanov, 39, and Artem Aleksandrovich Kalinkin, 34, both from Novosibirsk, Russia. The operation highlights the increasing severity of cyber-attacks aimed at destabilizing governments and engaging in theft and blackmail. Notably, the UK retailer Marks & Spencer was among the recent victims of such attacks. The German crime agency, Bundeskriminalamt (BKA), led the European efforts, releasing public appeals to track down 18 suspects believed to be involved in the Qakbot malware family and Trickbot. The majority of the suspects are Russian citizens. Vitalii Nikolayevich Kovalev, 36, a Russian national already wanted in the US, is one of BKA's most wanted. He is allegedly behind Conti, considered one of the most professional and best-organized ransomware blackmail groups globally, with Kovalev described as one of the 'most successful blackmailers in the history of cybercrime' by German investigators. Using the pseudonyms Stern and Ben, BKA alleges he has attacked hundreds of companies worldwide and extracted large ransom payments from them. Kovalev, from Volgograd, is believed to be living in Moscow, where several firms are registered in his name. He was identified by US investigators in 2023 as having been a member of Trickbot. Investigators now also believe he was at the helm of Conti and other blackmail groups, such as Royal and Blacksuit (founded in 2022). His own cryptocurrency wallet is said to be worth around €1 billion. The BKA, along with international partners, identified 37 perpetrators and had enough evidence to issue 20 arrest warrants. The US attorney’s office in California simultaneously unsealed the details of charges against 16 defendants who allegedly 'developed and deployed the DanaBot malware.' The criminal infiltrations into victims’ computers were 'controlled and deployed' by a Russia-based cybercrime organization that has infected more than 300,000 computers worldwide, particularly in the US, Australia, Poland, India, and Italy. It was advertised on Russian-language criminal forums and also had an 'espionage variant used to target military, diplomatic, government, and non-governmental organizations,' the indictment states. 'For this variant, separate servers were established, such that data stolen from these victims was ultimately stored in the Russian federation,' it adds. Also on Europe's most wanted list as a result of the German operation is 36-year-old Russian-speaking Ukrainian Roman Mikhailovich Prokop, a suspected member of Qakbot, according to BKA. Operation Endgame was first instigated by the German authorities in 2022. BKA president Holger Münch said that Germany is particularly focused on cybercriminals. The BKA is investigating the suspected perpetrators’ involvement in gang-related activities and commercial extortion, as well as membership in an overseas-based criminal organization. Between 2010 and 2022, the Conti group focused specifically on US hospitals, increasing its attacks during the Covid pandemic. US authorities had offered reward money of $10 million to anyone who would lead them to its figureheads. Most suspects are operating in Russia, some also in Dubai. Their extradition to Europe or the US is unlikely, Münch of the BKA admitted, but their identification was significant and damaging to them, he insisted. 'With Operation Endgame 2.0, we have once again demonstrated that our strategies work – even in the supposedly anonymous darknet.'
3. <https://www.dw.com/en/europol-hits-malware-network-in-major-cybercrime-operation/a-69220251> - Europol has announced the dismantling of major malware networks in a significant cybercrime operation. The operation, dubbed 'Operation Endgame,' was initiated and led by France, Germany, and the Netherlands, with support from several other countries, including Britain, the United States, and Ukraine. The operation targeted botnets such as IcedID, Smokeloader, SystemBC, Pikabot, and Bumblebee, which play a major role in deploying ransomware. The sting resulted in 16 police searches across four countries and the seizure of over 2,000 domains. One of the main suspects earned at least €69 million ($74.5 million) in cryptocurrency by renting out criminal infrastructure sites to deploy ransomware. The operation underscores the growing international cooperation in combating cybercrime and the effectiveness of coordinated efforts in disrupting malicious activities online.
4. <https://www.abc.net.au/news/2024-05-31/massive-international-operation-takes-down-ransomware-networks-/103917618> - A massive international operation has successfully dismantled ransomware networks responsible for extorting hundreds of millions of dollars. Coordinated by the European Union's judicial cooperation agency Eurojust, the operation involved police agencies from Europe and America. Four 'high value' suspects were arrested during the raids—three in Ukraine and one in Armenia. The operation led to the takedown of more than 100 servers and the seizure of over 2,000 internet domains globally. The dismantled networks were responsible for spreading ransomware and other malicious software via infected emails, affecting millions of people worldwide. The operation highlights the growing threat of cybercrime and the importance of international cooperation in combating it.
5. <https://www.cybernews.com/security/nca-dismantles-huge-russian-cybercrime-network/> - The UK's National Crime Agency (NCA) has dismantled a significant Russian cybercrime network, resulting in 84 arrests and the seizure of $25 million. The operation targeted a network involved in large-scale cybercrime activities, including ransomware attacks and data breaches. The NCA's efforts highlight the ongoing challenges posed by cybercriminals and the importance of international collaboration in addressing cyber threats. The operation underscores the need for continued vigilance and cooperation among law enforcement agencies worldwide to combat cybercrime effectively.
6. <https://www.cybersecurity-help.cz/blog/4674.html> - Following Operation Endgame, a major botnet takedown in May 2024 that dismantled several major malware droppers, including IcedID, SystemBC, Pikabot, Smokeloader, and Bumblebee, law enforcement across North America and Europe launched a coordinated crackdown. This led to arrests, house searches, and other legal actions targeting users of the Smokeloader botnet, operated by a cybercriminal known as 'Superstar.' Through a pay-per-install service, Superstar sold access to infected machines, which customers used for activities like keylogging, webcam spying, ransomware attacks, cryptomining, and more. Romanian authorities, with support from French and British counterparts, dismantled a criminal group involved in a major online fraud operation. The group recruited hundreds of money mules to launder at least EUR 3 million, primarily obtained through fake business emails. Preventive measures have been taken against 13 suspects in Romania and 7 suspects in the UK were arrested.
7. <https://www.cyware.com/resources/threat-briefings/weekly-threat-briefing/cyware-weekly-threat-intelligence-may-05-09-2025> - Europol has successfully dismantled six DDoS-for-hire services used globally for cyberattacks. The operation involved arrests in Poland, seizure of domains in the U.S., and collaboration with Dutch and German authorities as part of Operation PowerOFF. These services, disguised as stress-testing tools, allowed non-technical users to launch DDoS attacks by renting infrastructure. The UN has introduced the UNIDIR Intrusion Path framework to assess cyber-attacks, complementing existing models like the MITRE ATT&CK framework.