Russian Cops Bust Key Members Of World's Busiest Cybercrime Gang: Sources

By Thomas Brewster

Published: 2016-02-08 · Archived: 2026-04-29 08:06:06 UTC

In November, Russia's FSB quietly led an operation to take down the world's most active cybercriminal groups, the operators of the banking malware Dyre, according to a number of sources with knowledge of the matter.

Little is known about the investigation, which is ongoing, or who was arrested. One source claimed the apprehended suspects were in the top echelon of the Dyre crew. The hackers were stealing tens of millions of dollars from businesses and banks, stealing as much as $1.5 million in individual attacks. They were responsible for a quarter of all financial cybercrime in 2015 and Dyre was the most active of all banking malware variants, according to IBM .

FORBES understands the arrests took place across 18 and 19 November. IBM and Dell Secureworks both told FORBES the Dyre malware disappeared from their respective radars on 18 November. Either the Dyre infrastructure has been wiped out or is idle.

Western police agencies have been left out of the loop, despite the malware affecting a significant number of American and European businesses. A spokesperson for the UK's National Crime Agency said: "We are aware that arrests have been made and an active investigation remains, with enquiries ongoing. However, we cannot comment further."

Europol said it could not comment as it only worked with European partners, whilst the FBI had not returned requests for comment. All have previously stated difficulties working with Russian law enforcement in cyber investigations. The FSB also had not responded to a request for comment.

Russian security firm Kaspersky was said to have assisted the investigation and is expected to reveal more at its annual analyst summit in Tenerife this week. Kaspersky said it did not comment on law enforcement investigations, however.

News of the arrests comes shortly after Reuters reported that a film studio in Moscow, 25th Floor, had been raided as part of the investigation. But there was no evidence anyone at the company had been charged or was involved in Dyre. Intriguingly, the firm was producing a film called Botnet, a thriller loosely based on a 2010 case in which 37 people were charged for a $3 million cybercrime.

Since their emergence in 2014, variants of the Dyre malware have together, at the very least, stolen tens of millions of dollars. In April last year, IBM said in incidents at the start of 2015 organizations were losing between $500,000 and $1.5 million to attackers. Bank of America , Citibank, JP Morgan Chase , Royal Bank of Scotland and Wells Fargo were amongst 1000 banks, electronic payments and digital currency providers the Dyre operators targeted.

The malware was typically sent in an email attachment to employees. Once the attachment was opened, Dyre used a number of tactics to pilfer company funds. First, it would wait until a banking website was opened and inject a fake page, stealing the logins as the employee typed them. The hackers would then log in and move the money around various accounts, attempting to launder the stolen funds.

Alternatively, another page would open, advising the user that more security information was required, such as a PIN code or a date of birth. Finally, the hackers targeted businesses that often carried out large wire transfers, throwing up fake websites that asked them to call a number owned by the criminals to supply information about the transfer. They would then redirect the transfers, via a number of global banks, to their own accounts.

Last year, the Dyre masterminds upped their game. Security firm Trend Micro said it had seen a 125 per cent increase of Dyre infections worldwide in the second quarter of 2015 compared to the previous period.

Europe was worst hit, home to 39 per cent of total infections, just above North America on 38 per cent, according to Trend. Despite emanating from Russia, there appear to be close to zero infections in the country. Often, cybercriminals in Russia evince a patriotic streak, though it's unclear why. Last year, researchers linked one of the FBI's Most Wanted cybercriminals, Yevgeniy Bogachev, to state espionage activity.

Dyre was also noted for its ability to evade popular "sandboxes", where programs are run in a contained environment to check for malicious behaviour before being allowed to load on the main system. It was also used to download additional malware payloads, such as the Cryptowall ransomware.

Then the action in November came and Dyre was seemingly no more. "Seeing as it was not the first time the servers were quiet, we assumed it was a time out the gang was taking from its activity," said Limor Kessem, senior cybersecurity evangelist at IBM.

"But Dyre did not come back. After going dark on activity, we hardly saw any new infections from that day. The servers that update bots with new configurations were disconnected from the Internet alongside the servers that dispatch real time web injections.

"There was a short phase where the redirection attack servers were still up, but they too were disconnected about week later and have remained silent since."

This is unlikely to be the end of the Dyre malware, however. It's now likely the software will be adopted and tweaked by hackers, as the source code for Dyre was recently made freely available, according to one source.

Updated on 9 February to include confirmation from the NCA it was aware of arrests.
