TrickBot gang member arrested after getting stuck in South Korea due to COVID-19 pandemic

By Catalin Cimpanu

Published: 2023-01-19 · Archived: 2026-04-05 15:48:36 UTC

A Russian man was arrested last week at the Seoul international airport on accusations of developing code for the TrickBot malware gang.

The man, identified in local media reports only as Mr. A, was arrested trying to leave South Korea for his native home in Russia after he'd been stuck in the Asian country for more than a year and a half.

The suspect, who arrived in February 2020, was initially prevented from leaving after Seoul officials canceled international travel at the onset of the COVID-19 pandemic.

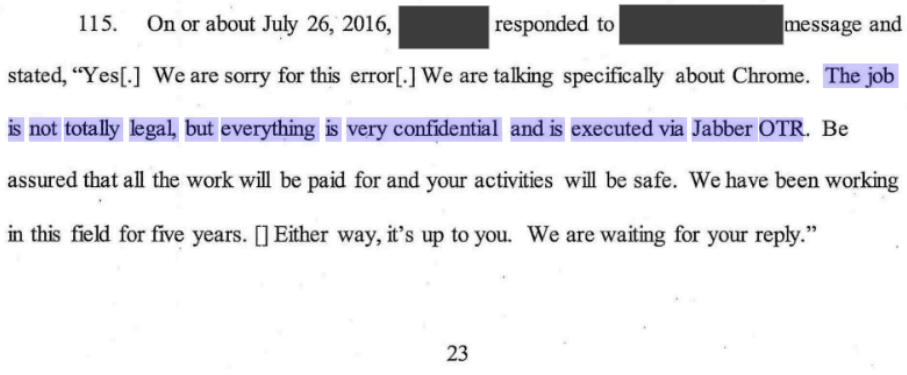
When air travel restrictions were lifted, the suspect's passport had expired, forcing Mr. A to live in a Seoul studio apartment until this summer while the local Russian embassy issued a replacement.

However, while the suspect was awaiting a passport replacement, US officials started an official investigation against TrickBot, a Russian-based malware gang that had used its botnet to facilitate ransomware attacks across the US throughout 2020.

While a takedown operation spearheaded by several security firms failed in October 2020, US officials had more success on a legal front, announcing the arrest of a 55-year-old Latvian woman named Alla Witte, who US prosecutors said worked as one of TrickBot's programmers.

Similar to Witte's indictment, a South Korean judge said Mr. A was charged for working with the TrickBot gang and developing a web browser-related component for the group after answering a job ad in 2016 — the same way Witte was recruited.

Documents in Witte's case cite private conversations between TrickBot members regarding the recruitment process. Per these conversations, the TrickBot gang was upfront with the people who applied and told them what they're doing was not legal.



115. On or about July 26, 2016, [redacted] responded to [redacted] message and stated, "Yes[.] We are sorry for this error[.] We are talking specifically about Chrome. The job is not totally legal, but everything is very confidential and is executed via Jabber OTR. Be assured that all the work will be paid for and your activities will be safe. We have been working in this field for five years. [] Either way, it's up to you. We are waiting for your reply."

23

Image: The Record

Per the same conversations cited in the Witte case, most who applied for the jobs realized they were doing "blackhat stuff."

Trickbot lead members said in private conversations to each other that they were looking for candidates who did the recruitment test without asking too many questions.

"If they ask additional questions, this person is not suitable," one message read.

CC8	[redacted]
CC8	[redacted] did the test task
CC8	Who else did it?
CC8	Why are you communicating with this one
CC8	[redacted] wrote to you
CC8	The main reason is that this functionality can be used for illegal activities/ blackhat (formgrabbing, injects) \n I do not do Blackhat
CC8	plus, [redacted] did not even do the test task
[redacted]	Later [redacted] changed his mind and [redacted] is ready to write in the evening. There is nothing to lose if [redacted] writes, right?
	Is [redacted] test task being checked?
CC8	let him create a Jabber
CC8	I will contact him there
CC8	until people finish the test task, do not exchange any Jabbers
CC8	We need to stop communicating with idiots
[redacted]	We are not in the main one, but in the external one. I got it.
CC8	it does not matter, they sent the test task
[redacted]	in short, describe the question they are asking, so I don't have to bother you later
CC8	If there is no result, we don't communicate any more
[redacted]	The majority understand that this is blackhat and asking for the commercial target .
CC8	if they ask additional questions, this person is not suitable
CC8	This is the gist

Image: The Record

South Korean news outlet KBS said the suspect was arraigned in a Seoul court on Wednesday, September 2, on an international arrest warrant and extradition request to the US.

Mr. A is fighting this extradition. His lawyer claimed that if his client is sent to the US, he "will be subjected to excessive punishment."

Recorded Future®

Know what matters.

Act first.

Get started

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

Source: https://therecord.media/trickbot-gang-member-arrested-after-getting-stuck-in-south-korea-due-to-covid-19-pandemic/