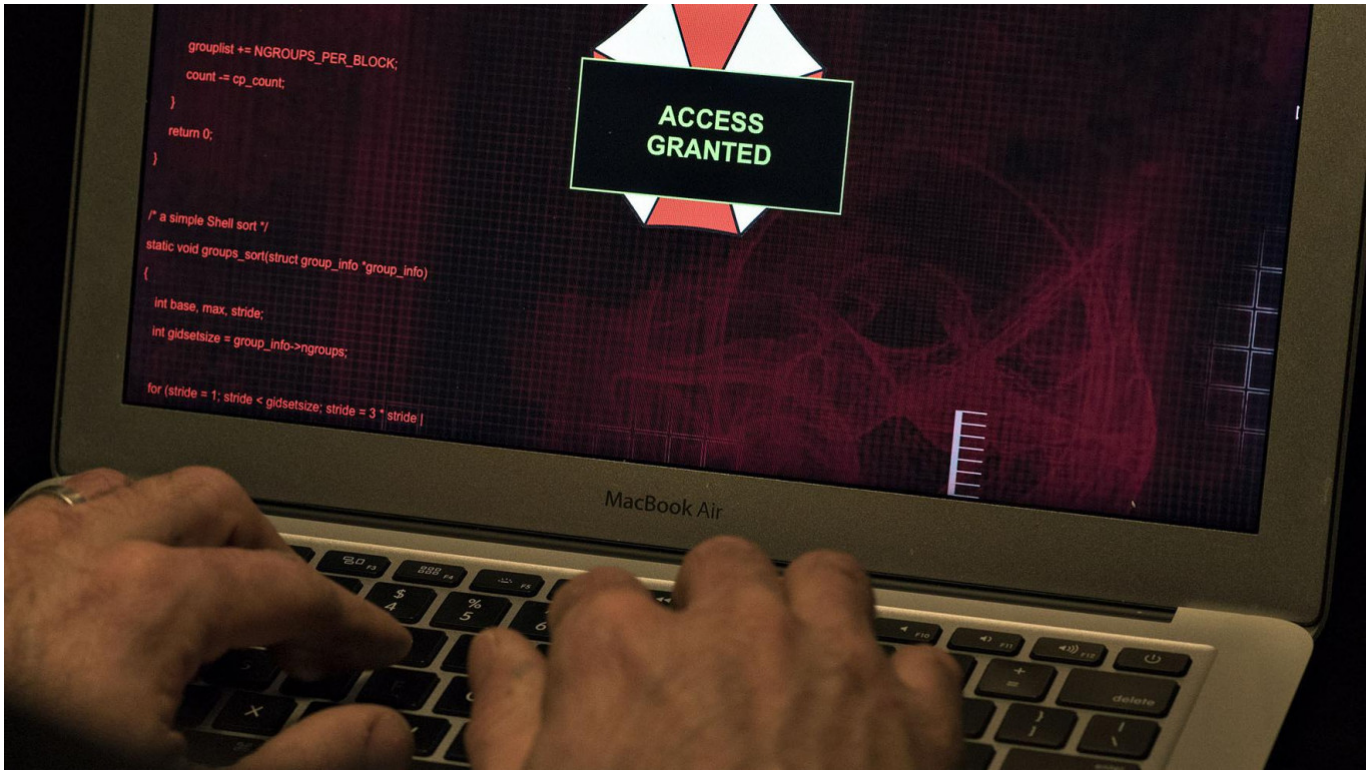
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Cyber Heist Linked to Russians Targets Banks From Moscow to Utah

December 11, 2017



Bloomberg

(Bloomberg) — A previously unknown ring of Russian-language hackers has stolen as much as $10 million from U.S. and Russian banks in the last 18 months, according to a Moscow-based cyber-security firm that runs the largest computer forensics laboratory in eastern Europe.

The MoneyTaker group broke into 20 systems, which includes 15 U.S. lenders, targeting ATMs with "mules" and Russia's interbank money-transfer system, Group-IB said in a report provided to Bloomberg.

The hackers, who also breached a U.K. software and service provider, are now probing institutions in Latin America and may be trying to compromise the Swift international bank messaging service, according to the security firm, whose clients range from Russia's biggest lender Sberbank PJSC to Raiffeisen Bank International AG.

"Criminals have changed tactics and are now focusing on banks rather than their clients, as

was the standard operating procedure in the past," Dmitry Volkov, the head of Group-IB's cyber intelligence department, said by phone.

Russia, considered a hotbed of government-backed information attacks, increasingly finds itself a victim of cybercrime. It took the initial blame for the Badrabbit ransomware virus that spread to more than 200 targets globally, even though some of the biggest disruptions affected Russian businesses.

'Limited Resources'

Since its first successful breach in May 2016, MoneyTaker has stolen from banks in New York, California, Utah and Moscow, primarily targeting smaller institutions with limited cyber defenses, Group-IB found. The average haul from U.S. banks was about $500,000, and it stole over $3 million from three Russian lenders.

"They understand that banks — especially community banks with limited resources — are the easiest marks," Volkov said.

The cell remained undetected by using so-called fileless malware that only exists on a computer's temporary memory and destroys itself when the system reboots, meaning it's not permanently stored and therefore can more easily evade anti-virus programs, according to Group-IB.

Related article: How Russia Became a Hacking Superpower

At one bank, the hackers gained access to the network via the home computer of the lender's system administrator.

While hackers are transnational, many new types of attacks are discovered in Russia because it's at the forefront of cybersecurity, a deputy head of the Russian Central Bank's information security and protection department, Artyom Sychev, said in an interview in November.

In Cross-Hairs

Group-IB said the U.S. banks were targeted by gaining access to their card-processing system and then opening accounts at the compromised institutions. The attackers removed limits on the legitimate bank cards and used mules to withdraw cash from ATMs.

The virus was so stealthy that, in at least one instance, a bank was successfully robbed twice.

While Group-IB didn't uncover evidence of a successful attack on Swift by MoneyTaker, it found that the hackers were searching for documents related to the messaging system, which could indicate pending attacks. Last year, in one of the biggest heists in cybercrime history, hackers used Swift to steal $81 million from Bangladesh.

"The more we dig, the more we'll find," Group-IB's Volkov said. "This report doesn't represent the full picture, and I can say with 100 percent certainty that there are more victims that haven't been identified yet."

Original url:
https://www.themoscowtimes.com/2017/12/11/cyber-heist-linked-to-russians-targets-banks-from-moscow-to-utah-a59885