Latin American ATM Thieves Turning to Hacking

By Michael Mimoso

Published: 2017-10-05 · Archived: 2026-04-05 20:42:09 UTC

Thieves in Latin American countries are turning to Eastern European hackers to build ATM malware from scratch, according to a Virus Bulletin talk by researchers at Kaspersky Lab.

MADRID—ATM jackpotting is hardly a novelty act in Latin America where criminals are more than ever connecting with hackers to figure out how to more efficiently steal money from an automated teller than, say, by using a stick of dynamite.

No, it's not uncommon to hear about thefts in Brazil, Mexico, Colombia, Peru and elsewhere that involve explosives and a mangled ATM left in their wake. In fact, Kaspersky Lab researchers Fabio Assolini and Thiago Marques on Thursday at Virus Bulletin showed a couple of surveillance videos during a talk on the subject that show criminals vandalizing machines, destroying them with dynamite and leaving behind sometimes more than just a charred ATM.

But that is changing.

A quick tour through some underground forums, and you're bound to find posts from Latin American criminals soliciting help. Posts written in Portuguese and Spanish on Russian and Eastern European forums are looking for purpose-built ATM malware, and even ATM manuals in order to learn more about the inner workings of these cash boxes.

"Eastern European hackers are leading the way in creating malware for ATMs, with Latin American hackers right behind," Assolini said.

They're investing in, or learning how to write, ATM malware from scratch, the researchers said. Sometimes they're penetrating bank networks to conduct remote attacks, but more often than not, these attacks require physical access to an ATM. That means, Assolini and Marques explained, loading malware from a USB stick, CDs (on older ATMs) or plugging in a USB keyboard in order to access the backend of one of these machines.

Once they're on, criminals can dictate how much money they want to take from the machines, and don't expect them to hang around for a long while.

"They want to jackpot ATMs quickly after infecting the machine or the network," Assolini said, pointing out that the criminals want a hasty exit in order to avoid detection.

In a paper released alongside their talk, Assolini and Marques write about longstanding business relations between Eastern European and Latin American cybercriminals, mostly around cloned credit cards. ATM malware, meanwhile, surfaced starting in 2008 with Skimer, which was able to either steal money or data from cards used at machines. Kaspersky has also published reports on the Tyupkin ATM malware in 2014 and a year later published

another report demonstrating evidence of cooperation between Latin American criminals and the Eastern European groups behind the Zeus and SpyEye banking Trojans.

“The facts demonstrate that Latin American cybercriminals are adopting new techniques as a result of collaboration with their Eastern European counterparts,” they wrote in the Virus Bulletin paper. “We believe this is only the tip of the iceberg, as this kind of exchange tends to increase over the years as crime develops and criminals look for ways to attack businesses and individuals.”

The researchers covered during today’s talk four malware families prevalent among ATM hackers: Ploutus, Prilex , Green Dispenser and Ice5.

Ploutus, Marques said, has been on the scene since 2013 primarily infecting machines in Mexico, and has accounted for more than $64M USD in losses. Ploutus requires physical access via a USB or CD to deploy the malware in order to steal the ATM ID used to activate and identify an ATM before cashing out. A variant of the malware now interacts with a popular ATM platform called Kalignite, which runs on a number of machines made by different vendors including Diebold.

Once an attacker connects to the machine via keyboard, they can use the malware to generate an activation code and access funds stored inside the machine. Marques said the attackers aren’t shy about their work, leaving messages in the code such as “Ploutus: Made in Latin America.”

Ice5 and Prilex are almost exclusive to Brazil and were developed in the country. Ice5 targets ATMs manufactured by NCR, while Prilex was a bit more complex and interacted with libraries from specific vendors, indicating particular knowledge of the ATM and related network.

“Once the malware is running, it has the capability to dispense money from the sockets using a special window this is activated using a special key combination that is provided to the money mules by the criminals,” the researchers wrote, adding that the malware also includes a component that steals strip data from cards that would be collected later.
