Can the ATM industry stop Tyupkin in its tracks?

By Suzanne Cluckey

Published: 2014-10-10 · Archived: 2026-04-05 20:38:02 UTC

Article

ATM Marketplace checked in with security experts around the industry to learn how operators can protect themselves from the latest 'jackpotting' scheme, Tyupkin malware.

October 10, 2014 by Suzanne Cluckey — Owner, *Suzanne Cluckey Communications*

This week Kaspersky Lab revealed that, at the request of an as-yet-unnamed European financial institution, the security tech firm had performed a forensic investigation into cybercriminal attacks targeting ATMs around the world.

What Kaspersky experts discovered was unsettling — a new type of malware identified as Backdoor.MSIL.Tyupkin, affects machines from "a major ATM manufacturer running Microsoft Windows 32 bit," Kaspersky reported. Once uploaded, the program allows attackers to remove money by "direct manipulation" (i.e., information entry on the keypad), stealing millions of dollars — otherwise known as jackpotting.

As yet, total losses are unknown — and it appears that the malware is still spreading. According to information published by Kaspersky Lab on Oct. 7:

At the time of the investigation, the malware was active on more than 50 ATMs at banking institutions in Eastern Europe. Based on submissions to VirusTotal, we believe that the malware has spread to several other countries, including the U.S., India and China.

Interpol has alerted the affected member countries and is assisting ongoing investigations, Kaspersky said.

How does it work?

Kaspersky described the attack methodology this week in a news release:

The criminals work in two stages. First, they gain physical access to the ATMs and insert a bootable CD to install the Tyupkin malware. After they reboot the system, the infected ATM is now under their control and the malware runs in an infinite loop waiting for a command. To make the scam harder to spot, the Tyupkin malware only accepts commands at specific times on Sunday and Monday nights. During those hours, the attackers are able to steal money from the infected machine.

Gaining physical access to the interior of an ATM is not the obstacle one might expect, either. According to Scott Harroff, chief information security architect at Diebold, "Depending on circumstances, it can take less than a minute to gain physical access."

Dave O'Reilly, chief technologist at Fraud Technology Research Solutions, said that the practicalities of operating an ATM network — for instance, the need to allow service engineers access to the PC core at times — means that all ATMs might be fitted with the same lock. "Another relevant scenario is the case of a complicit merchant who grants someone access to the ATM on their premises," he said.

The larger question the industry should be asking is whether core access is even needed to carry out a malware attack. "Can attack scenarios be identified that do not need the attacker to have physical access to the PC core?" O'Reilly asked. "The criminals have once again taken the lead and we, as an industry, need to move to prevent not only the current attack methods but future variations that can be envisioned based on what we already know."

Kaspersky provided video from security cameras at infected ATMs showing how attackers gained access to cash. Each session was conducted using a unique, randomly generated digit combination — ensuring that no one outside the gang could profit from the fraud. *(**NOTE**: This means that the Kaspersky video cannot be used to stage an attack.)*

The operator receives instructions by phone from another gang member who knows the algorithm and is able to generate a session key based on the number shown. This ensures that mules collecting the cash do not try to go it alone.

When the key is entered, the ATM displays details of how much money is available in each cash cassette, inviting the operator to choose which cassette to rob. The ATM dispenses 40 banknotes at a time from the chosen cassette.

How widespread is the threat?

The malware identified and named by Kaspersky Lab as Backdoor.MSIL.Tyupkin, has so far been detected on ATMs in Latin America, Europe and Asia, the security provider said. However as previously mentioned, Kaspersky believes that it might also have spread to major ATM markets that include China, India and the U.S. Indeed, Diebold's Harroff confirmed that the Tyupkin malware is in the U.S. market already.

"It’s important to point out that this is not a new form of attack," said NCR director of security marketing Owen Wild. "The malware that is referenced in the report as Tyupkin is the same as PADPIN/ulssm which is a variant of the malware identified in previous ATM attacks that we saw in the U.K. and Russia last year."

Various media reports have asserted that Tyupkin is a variant of Ploutus, malware that was discovered on ATMs in Mexico last year. Shortly afterward, evidence indicated that the code had been rewritten in English and that attacks in the U.S. and Europe might follow. And now, it seems, they have.

According to Vicente Diaz, principal security researcher at Kaspersky, the firm's security team has have observed a major upswing in ATM attacks using skimming devices and malicious software over the past few years.

"Now we are seeing the natural evolution of this threat with cybercriminals moving up the chain and targeting financial institutions directly," he said in the Kaspersky release. "This is done by infecting ATMs themselves or launching direct APT-style attacks against banks. The Tyupkin malware is an example of the attackers taking advantage of weaknesses in the ATM infrastructure."

Interpol digital crime center director Sanjay Virmani concurred. “Offenders are constantly identifying new ways to evolve their methodologies to commit crimes, and it is essential that we keep law enforcement in our member countries involved and informed about current trends and modus operandi."

An ounce of prevention ...

Harroff said that operators should use existing physical security sensors in the ATM to detect unauthorized access to the computer. Additionally, he advised, "Leverage integrated services to provide software updates and information security controls to prevent malware from being added to the ATM."

Kaspersky offered these additional recommendations:

- Review the physical security of all ATMs and consider investing in quality security solutions.
- Replace all locks and master keys on the upper hood of the ATM machines and ditch the defaults provided by the manufacturer.
- Install an alarm and ensure it is in good working order. The cyber-criminals behind Tyupkin only infected ATMs that had no security alarm installed.
- Change the default BIOS password.
- Ensure the machines have up-to-date antivirus protection
- Contact Kaspersky directly for advice on how to verify that your ATMs are not infected.
- To make a full scan of the ATM’s system and delete the backdoor, use the free Kaspersky Virus Removal Tool.

And NCR's Wild recommended steps particularly for operators of NCR ATMs:

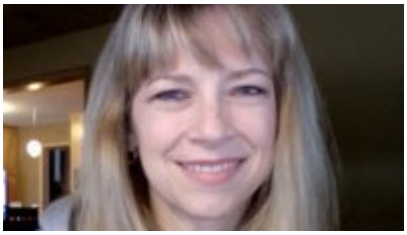
1. Deploy the "stinger" provided by NCR software security team. This program can be distributed over the network and will detect and clean this specific malware if present.
2. Modify the ATM BIOS such that the ATM will only boot from the primary hard disk and nothing else. Then, protect the configuration with the BIOS password. This is the most important change ATM operators must make, and is the most effective method to prevent malware infection on the ATM.
3. Upgrade to Solidcore Suite for APTRA. Solidcore for APTRA will prevent runtime and network attacks, but Solidcore Suite for APTRA also will detect if Solidcore is disabled. In many of these attacks, the malware is disabling all whitelisting and anti-virus protection. Solidcore Suite for APTRA could have alerted that the ATM was unprotected before the cash out took place the following day. However, please note that if the criminal decides to cash out at the same time as malware deployment, and if the criminal disconnects the network cable, then Solidcore Suite for APTRA will only be able to warn of an offline ATM.
4. Consider the physical environment of the ATM deployment. Lobby ATMs should not be deployed in 24/7 unattended environments without compensating physical security controls. A through-the-wall ATM might be more suitable for these locations. Stronger, UL-rated, pick resistant top box locks are available for SelfServ ATMs as a configuration option or upgrade kit.

Ultimately, "each operator must select a solution that best fits their requirements," O'Reilly said. He said that FTR solutions regularly helps FIs to map out a range of appropriate tactics that can be applied fleetwide or at machines

deemed to be most at risk. "These can include appropriate physical access controls, secure BIOS settings, disk encryption, application whitelisting, etc."

The critical point is to move quickly — because a pound of cure could come at a very high cost.

About Suzanne Cluckey



Suzanne’s editorial career has spanned three decades and encompassed all B2B and B2C communications formats. Her award-winning work has appeared in trade and consumer media in the United States and internationally.