Tyupkin

Insert stick figure graphic here [10]

Tyupkin was a “jackpotting [6]” trojan malware that installed backdoor access into ATM software to steal thousands of dollars; it was active in different iterations from 2014 to 2016. It first appeared in Malaysia in October 2014, with the thieves stealing over 700k USD from 18 ATMs over four days [1]. Within the week, the Malaysian Special Task Force on Organized Crime (STAFOC) was mobilized and attempted to track down the thieves. The Bukit Aman cyber-crime deputy director Mohd Kamarudin Md Din, described the thefts as a “21st century bank heist [1].” As there is no information available regarding their capture, it’s safe to assume these threat actors escaped prosecution. Reactions were immediate. Adli Wahid wrote an article for the Regional Internet Registry Administering IP Addresses for the Asia Pacific reiterating the importance of physical security measures in cyber security discussions: “Your typical malware-of-the-day relies a lot of [sic] exploiting client side vulnerabilities (that is, drive-by-downloads) or authentication weaknesses in Internet facing services. … A threat actor who can access IT assets such as laptops or servers can potentially commit theft or breach security, which in turn can affect the confidentiality, availability and integrity of information systems [2].”

When the Malaysian incidents occurred, one of the financial institutions affected requested a forensic investigation and analysis from Kaspersky Labs. Kaspersky conducted their investigation in coordination with Interpol, dubbing it Backdoor.MSIL.Tyupkin. Though the current targets were in Malaysia, more than 50 ATMs around the world were found to be infected [5].

This version of Tyupkin required a great deal of human intervention to yield any results [3]. An accomplice would open the hood of a target ATM and install a bootable CD. After a reboot, the infected machine was accessed via the keypad. The passcode was a unique digit combination key based on random numbers, freshly generated every session. The number on the screen was fed over the phone to another accomplice who applied the Tyupkin algorithm and returned the appropriate passcode to the on-site individual. Once the system is accessed, the screen displays the amounts in each cash cassette and a choice prompt. Finally, the thief collected banknotes dispensed 40 notes at a time. The average ATM holds approximately $10,000 in four cassettes when full [9], allowing the team to net at least 2k from a single machine.

The unique feature of Tyupkin was the code restricting this backdoor to certain days-Sundays and Mondays- at certain hours-nighttime. The attacks were orchestrated against ATMs from the well-known manufacturer NCR, running Microsoft Windows 32-bit [3]. In 2019, Cisco’s Talos Intelligence wrote a retrospective on ATM malware [7]. Tyupkin took advantage of a vulnerability in the generic Windows extension for the Financial Services API (CEN/XFS) [7], interacting with the ATM through its standard library MSXFS.dll library. A more extensive technical description of the files accessed and the code inserted can be found on Kaspersky’s SecureList resource [8]. Later versions of Tyupkin evolved to add anti-debug and anti-emulation methods as well as disabling McAfee Solidcore in the infected machine. It would also disable the local area network, “likely …to delay or disrupt remote investigations. [8].

Following the Malaysian attacks, more sophisticated thieves orchestrated a series of attacks across Europe from December 2014 to October 2015. The attacks netted a little over 200k USD. The attackers controlled an updated version of Tyupkin switching from a cd to a more-concealable USB port and loading a magnetic card with an attack code to initiate the fraudulent code. Surprisingly, the new-and-improved Tyupkin still scheduled the attacks for Sunday and

Monday nights. Owen Wild, global marketing director for financial services security solutions at NCR, the targeted manufacturer, described that “when those [Tyupkin] attacks were successful, they were extraordinarily successful in capturing large amounts of cash across a large number of cash machines. [9]”

While the European thieves stole less than a fourth of what was stolen in Malaysia, the breadth of the attacks prompted international cooperation between the Romanian National Police, the Directorate for Investigating Organized Crimes and Terrorism (DIICOT), Europol, and Eurojust. The thieves, Romanian and Moldovan nationals, were captured January 2016. While the threat of Tyupkin was officially neutralized, a post on The Hacker News that same year claimed that a contemporary malware, GreenDispenser, employs similar tactics and code. This is borne out by the Talos assessment [7].

WORKS CITED:

[1] T. Jayamanogaran, "Bukit Aman sends out anti-vice crack team on ATM hackers’ trail | Malay Mail", *Malaymail.com*, 2014.
[Online]. Available: https://www.malaymail.com/news/malaysia/2014/10/03/bukit-aman-sends-out-anti-vice-crack-team-on-atm-hackers-trail/756941. [Accessed: 27- Sep- 2021].
[2] A. Wahid, "Physical security is part of cybersecurity | APNIC Blog", *APNIC Blog*, 2014.
[Online]. Available: https://blog.apnic.net/2014/11/11/physical-security-is-part-of-cyber-security/. [Accessed: 27- Sep- 2021].
[3] "Kaspersky Lab and INTERPOL alert: Infected ATMs give away millions of dollars without credit cards around the globe", *www.kaspersky.com*, 2014.
[Online]. Available: https://www.kaspersky.com/about/press-releases/2014_kaspersky-lab-and-interpol-alert-infected-atms-give-away-millions-of-dollars-without-credit-cards-around-the-globe. [Accessed: 27- Sep- 2021].
[4] M. Kumar, "Hacker arrested for ATM Skimming escaped from Prison", *The Hacker News*, 2016.
[Online]. Available: https://thehackernews.com/2016/03/hacker-escaped-prison.html. [Accessed: 27- Sep- 2021].
[5] "Authorities Arrest Eight in Tyupkin ATM Malware Takedown", *Threatpost.com*, 2016.
[Online]. Available: https://threatpost.com/authorities-arrest-eight-in-tyupkin-atm-malware-takedown/115841/. [Accessed: 27- Sep- 2021].
[6] "International Criminal Group Behind ATM Malware Attacks Dismantled", *Europol*, 2016.
[Online]. Available: https://www.europol.europa.eu/newsroom/news/international-criminal-group-behind-atm-malware-attacks-dismantled. [Accessed: 27- Sep- 2021].
[7] "10 years of virtual dynamite: A high-level retrospective of ATM malware", *Blog.talosintelligence.com*, 2019.
[Online]. Available: https://blog.talosintelligence.com/2019/05/10-years-of-virtual-dynamite.html. [Accessed: 27- Sep- 2021].
[8] "Tyupkin: manipulating ATM machines with malware", *Securelist.com*, 2014.
[Online]. Available: https://securelist.com/tyupkin-manipulating-atm-machines-with-malware/66988/. [Accessed: 27- Sep- 2021].
[9] T. Brewster, "$5,000 Malware Allows Anyone To Empty ATMs -- But It Isn't Worth The Trouble", *Forbes*, 2016.
[Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/01/07/atm-hacking-arrests-tyupkin/?sh=1e37061310ae. [Accessed: 27- Sep- 2021].

[10] "Tyupkin Malware Infects ATMs Worldwide", *Threatpost.com*, 2014. [Online]. Available: https://threatpost.com/tyupkin-malware-infects-atms-in-eastern-europe/108734/. [Accessed: 27- Sep- 2021].

FURTHER INFORMATION:
"Infected ATMs give away millions of dollars without credit cards" https://www.youtube.com/watch?v=QZvdPM_h2o8
Tyupkin ATM Malware: Take The Money Now Or Never!
https://www.lastline.com/labsblog/tyupkin-atm-malware/