Threat Intelligence Bulletin

ATM Jackpotting kit for sale on darknet

www.cyberint.com
ATM Jackpotting Crimeware kit including the “Cutlet Maker” malware

CyberInt recently discovered a darknet website selling a sophisticated software designed to steal money from Automated Teller machines (ATMs), specifically Wincor Nixdorf models\(^1\), by exploiting access to USB ports and absence of proper security policy. The current price is no less than 1,500 USD. This kit is the same ATM malware kit discovered by Kaspersky last week\(^2\), reporting to have found the malware in darknet marketplaces. Apart from the published kit, the website offers an automation method, to enable clients to automatically lunch the malware when connecting to the ATM.

We asses that the darknet website is most likely powered by a Russian native speaking group, as the demonstrating videos has Russian native subtitles, and the ATMs had bank logos with Russian native letters. It fits with Kaspersky’s assessments that the code was written by a Russian native speaker. However, the website is written in fine English, suggesting that their targeted market expands beyond their country’s borders.

This is not the first time Wincor Nixdorf ATMs are being targeted, and sadly, the problem is not unique to their models only, but a part of a much bigger world of ATM targeting. Methods range between physical skimmers\(^3\), reaching tiny proportions in order to fool the user and steal details from the Credit cards, through full malware packages exploiting vulnerabilities in the machine itself\(^4\), to whole

---

\(^1\) [http://www.dieboldnixdorfag.com/internet/site_NL/EN/Products](http://www.dieboldnixdorfag.com/internet/site_NL/EN/Products)


\(^3\) [https://krebsonsecurity.com/tag/wincor-nixdorf/](https://krebsonsecurity.com/tag/wincor-nixdorf/)

\(^4\) [https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf](https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf)
network operations targeting ATMs through bank networks\textsuperscript{5}. ATM hacking services are available not only on the darknet, and are reachable on a simple google search\textsuperscript{6}.

This risk of physical ATM attacks combined with logical ones, is very hard to counter, and falling victim to it has the potential of causing much more damage than money loss: reputational damage, for example, or bank networks being compromised by a hacker through the breach. Therefore, banks should take steps to protect their machines accordingly, and prevent ATM attacks from becoming an easy, worthwhile way for criminals to steal money. For more information on required steps see “Security Countermeasures and Recommendations” section.

**Method Description – Money dispensing process**

The attack method is fully described in the website’s guide section. The guide is very detailed and informative, and available with no registration at all. Registration and payment is required in order to gain access to the whole malware kit.

As mentioned above, the infection is done by injecting a USB drive containing the malware into the ATM. The guide walks the threat actor (the user) through different types of ATMs and where the USB port could be found on each model.

---


\textsuperscript{6} hxxp://phantomhacker.su/atm-hacking/
After uncovering the USB port, the threat actor uses a USB drive and a mouse and keyboard to control the ATM and operate the malware.

![Image of USB drive and keyboard]

The malware kit contains three elements:

1. **CUTLET MAKER:**
   
The main code responsible for emptying the ATM’s cassettes\(^7\). According to Kaspersky, this module’s name also suggests Russian origins, Cutlet (котлета) also means “a bundle of money” in Russian slang. The first country of origin from all Kaspersky’s detected submissions was Ukraine, showing again the “native Russian” connection.

   GUI explanation: Each “CHECK HEAT” and “start cooking!” button corresponds to a specific ATM cash cassette. “CHECK HEAT” dispense one banknote, “start cooking!” will start emptying the cassette 40 banknotes at a time. The “Stop!” button stops an ongoing “start cooking!” process. “Reset” is intended to reset the dispense process.

2. **c0decalc:**

\(^7\) Cassette is where the money in the ATM is kept: [https://en.wikipedia.org/wiki/Automated_teller_machine](https://en.wikipedia.org/wiki/Automated_teller_machine)
A passcode generator for the main code the CUTLET MAKER. The malware GUI will not respond until the code generated from the c0decalc is inserted in the input box (see Figure 4)

Figure 4: The password code is generated only if the client pays for a passcode

The website also offers an online version of the c0decalc generator, which seems to work very much the same:

Figure 5: Web version of the c0decalc passcode generator
3. **Stimulator:**

By using a specific API calls, the stimulator shows the amount residing in each of the ATM cassettes. Each column corresponds to each cassette. Upper row – loaded in cassette currency. Second row – nominal of banknotes loaded in cassette. Fourth row – quantity of banknotes.

![Stimulator](image)

*Figure 6: The Stimulator enables threat actor to check the amount of money in each ATM cassette*

**Method Automation**

The website’s owners recommends Teensy 3.2 as a simple method of automating the whole process. Teensy 3.2 is an Arduino based development board, that could be modified to do many actions, including running the “Cutlet Maker” malware automatically.

![Teensy 3.2 Arduino board](image)

*Figure 7: Teensy 3.2 Arduino board. Could be programmed to automate the hacking procedure*
Outlook and Implications

ATM Malware is a threat the financial industry and Banks in particular have been facing for a long time. This recent discovery shows us that threat actors continue to offer ATM malware in the underground for financial gain.

The potential impact of a successful ATM attack could be devastating not just in term of raw currency lost but also in reputation and trust against the effected organization which could lead to loss of clientele and long term financial gain.

We assess that threat actors will continue to come up with innovative ways to compromise organizations in the financial sector, that include ATM specific malware.

Security Countermeasures Recommendations

- We recommend including code execution prevention and deny policies on every ATM deployed by your organization.
- We recommend implementing to disable or control the type of external hardware that can be connected to the ATM
- We recommend implementing security update policies to keep both the application and the Operating system up to date.
- We recommend defining strict software and hardening policies which will decrease the attack surface of deployed ATMs
### IOCs

<table>
<thead>
<tr>
<th>File Name</th>
<th>SHA1</th>
<th>SHA256</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stimulator</td>
<td>7813becfec5dba77f94131c943137d8642449881</td>
<td>05fae4b6f32da78a8fb425f8c25f7f481f13d6bbbd3048e5b89190822bc470cd</td>
</tr>
<tr>
<td>Cm</td>
<td>66b0d9b10c2898d388bdf2be4a66ac76d5822f4</td>
<td>4a340a0a95f2af5ab7f3bfe6f304154e617d0c47ce31ee8426c70b86e195320c</td>
</tr>
</tbody>
</table>

*Table 1: IOCs*