TASK-7

DAY:- 24

DATE:- 20-07-2022

What Are Skimmers?

Skimmers are tiny, malicious card readers hidden within legitimate card readers that harvest data from every person that swipes their cards. After letting the hardware sip data for some time, a thief will stop by the compromised machine to pick up the file containing all the stolen data. With that information, he can create cloned cards or just commit fraud. Perhaps the scariest part is that skimmers often don't prevent the ATM or credit card reader from functioning properly, making them harder to detect.

Getting inside ATMs is difficult, so ATM skimmers sometimes fit over existing card readers. Most of the time, the attackers also place a hidden camera somewhere in the vicinity in order to record personal identification numbers, or PINs, used to access accounts. The camera may be in the card reader, mounted at the top of the ATM, or even in the ceiling. Some criminals go so far as installing fake PIN pads over the actual keyboards to capture the PIN directly, bypassing the need for a camera.

This picture is a real-life skimmer in use on an ATM. You see that weird, bulky yellow bit? That's the skimmer. This one is easy to spot because it has a different colour and material than the rest of the machine, but there are other tell-tale signs. Below the slot where you insert your card are raised arrows on the machine's plastic housing. You can see how the grey arrows are very close to the yellow reader housing, almost overlapping. That is a sign a skimmer was installed over the existing reader, since the real card reader would have some space between the card slot and the arrows.

ATM manufacturers haven't taken this kind of fraud lying down. Newer ATMs boast robust defences against tampering, sometimes including radar systems intended to detect objects inserted or attached to the ATM. However, one researcher at the Black hat security conference was able to use an ATM's onboard radar device to capture PINs as part of an elaborate scam.

Are Skimmers Still a Threat?

While researching an update to this article, we reached out to Kaspersky Labs, and company representatives told us something surprising: skimming attacks were on the decline. "Skimming was and still is a rare thing," said the Kaspersky spokesperson.

The Kaspersky representative cited EU statistics from the European Association for Secure Transactions (EAST) as indicative of a larger trend. The EAST reported a record low in skimmer attacks, dropping from 1,496 incidents (Opens in a new window) in April 2020 to 321 incidents (Opens in a new window) in October of the same year. The effects of COVID-19 might have something to do with that drop, but it's nonetheless dramatic.

That doesn't mean skimming has gone away, of course. As recently as January, 2021, a major skimming scams (Opens in a new window) was unearthed in New Jersey. It involved attacks on over 1,000 bank customers, with criminals attempting to make off with over $1.5 million.

From Skimmers to Shimmers:-

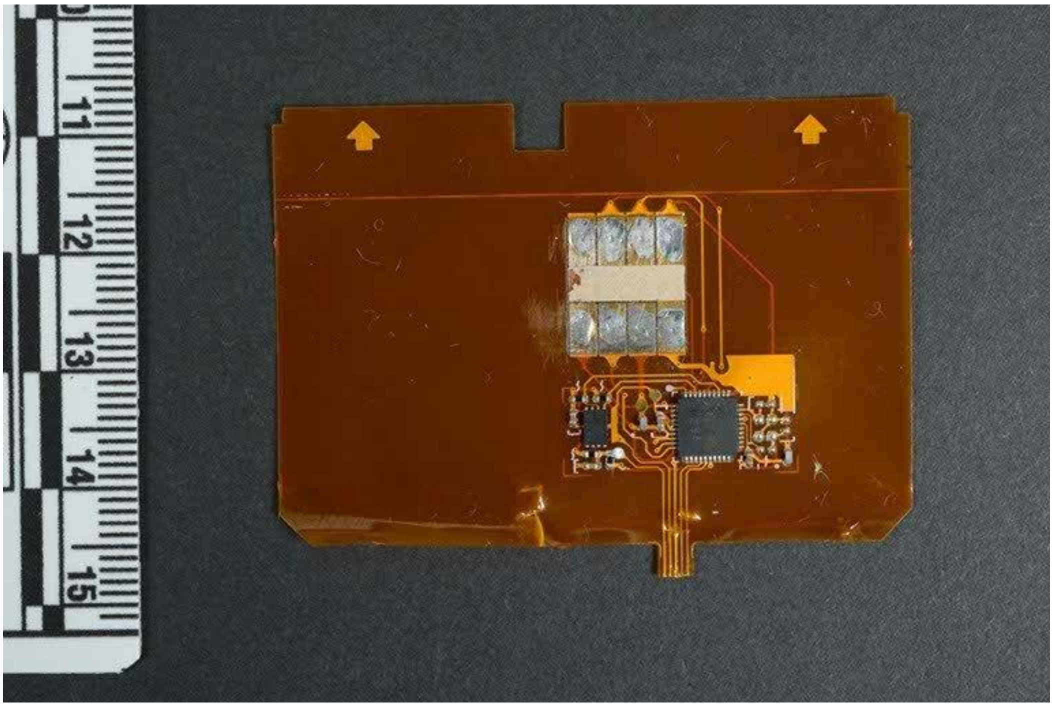
When the US banks *finally* caught up with the rest of the world and started issuing chip cards, it was a major security boon for consumers. These chip cards, or EMV cards, offer more robust security than the painfully simple magstripes of older payment cards. But thieves learn fast, and they've had years to perfect attacks in Europe and Canada that target chip cards.

Instead of skimmers, which sit on top of the magstripe readers, shimmers are *inside* the card readers. These are very, very thin devices and cannot be seen from the outside. When you slide your card in, the shimmer reads the data from the chip on your card, much the same way a skimmer reads the data on your card's magstripe.

There are a few key differences, however. For one, the integrated security that comes with EMV means that attackers can only get the same information they would from a skimmer. On his blog, security researcher brain krebs(Opens in a new window) explains that "Although the data that is typically stored on a card's magnetic stripe is replicated inside the chip on chip-enabled cards, the chip contains additional security components not found on a magnetic stripe." This means that thieves couldn't duplicate the EMV chip, but they could use data from the chip to clone the magstripe or use its information for some other fraud.

The Kaspersky representative we spoke to was unequivocal in their confidence for chip cards. "EMV is still not broken," Kaspersky told PCMag. "The only successful EMV hacks are in lab conditions."

The real problem is that shimmers are hidden inside victim machines. The shimmer pictured below was found in Canada and reported to the RCMP (Opens in a new window) (Internet Archive link). It's little more than an integrated circuit printed on a thin plastic sheet.



HUNTER CAT: ATM CARD SKIMMER DETECTOR:-

The Hunter Cat is the world's first pocket ATM Card Skimmer Detector.
Card Skimmers are devices containing magnetic readers that are covertly added onto / into ATMs, allowing criminals to 'skim' the data off a card's magnetic strip.

Over time, Card Skimmers have become increasingly difficult to detect visually, and are no longer restricted to ATMs, appearing on self-checkouts, petrol pumps, bank doors, etc.

The Hunter Cat is a Skimmer Detector - allowing users to quickly audit a device before inserting their real card.

The device detects the number of magnetic heads that pass over the card, providing instant analysis: OK, Warning, or Dangerous.

Created by:- Salvador in partnership with Electronic cats.

Available at:- https://hunter.electroniccats.com/

Invaluable for multiple industry sectors

INDUSTRIAL:- Internal Hardware / Fleet Auditing.

PEN TESTING:- Provide clients with an additional audit service.

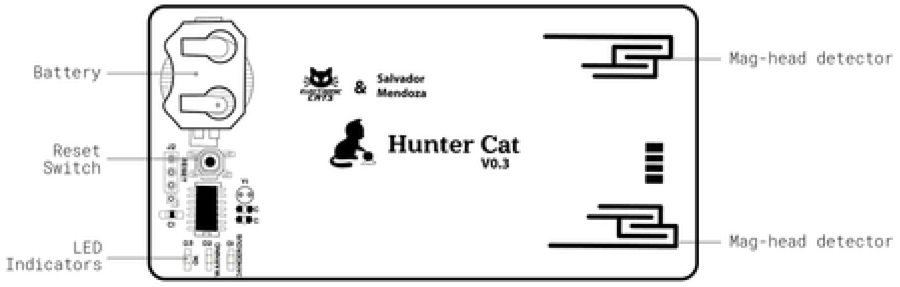
CORPORATE:- Protect your company / employee cards from theft.

PERSONAL:- Protect your bank account - especially when traveling.

HUNTER CAT HANDS ON: HOW TO USE:-

The Hunter Cat consists of two Magnetic Head detectors, three LEDs, a reset switch and a battery. It's the same width and depth as a standard credit card, but slightly longer, allowing for the card to be easily inserted and removed.

It has four exposed pin pads, triggering the ATM mechanism to open the card tray.



Lab401.com / "Hunter Cat" Card Skimmer Detector

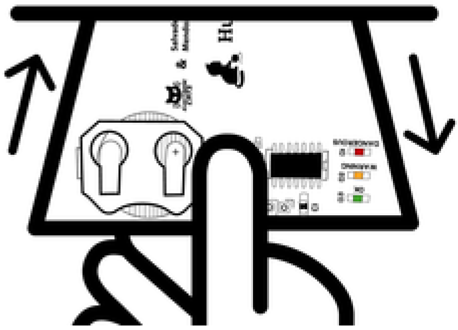
POWERING ON THE DEVICE:-

First Use: To use for the first time, simply place a CR-2303 battery into the battery holder. The LEDS will flash **four times -** the device is ready for use.

Standard Use: Press the reset button. The device LEDs will flash four times, indicating that it is ready for use.

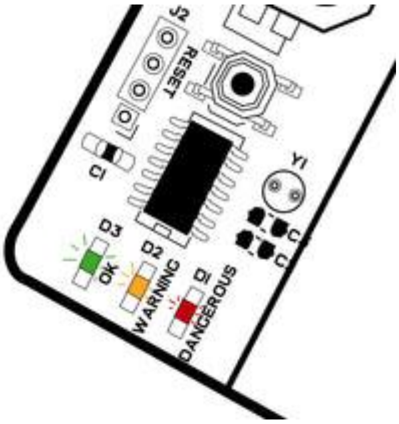
Sleep Mode: After **fifteen seconds of inactivity** - the device will cycle the LEDs two times, and go into sleep mode.

USING THE DEVICE



Insert and remove the device quickly (less than one second) as per standard "add/remove" ATMs.

It is important that the device is inserted and removed in less than one second. to provide accurate results.



The device will process the information, which will take approximate one second and display its audit: OK, Warning, Dangerous.

Based off this result, you can confidently use your bank card, or avoid using the device.