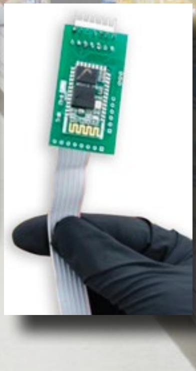
SKIMMERS & SCAMMERS

- ✓Convenience Stores
- ✓Credit Unions
- ✓Travel Centers
- ✓Banks
- ✓Gas Stations
- ✓Restaurants

SKIMMER



SCAMMER

BY SCOTT N. SCHOBER

WIRELESS & CYBERSECURITY EXPERT & CEO

Berkeley
Varitronics Systems
Wireless Detection

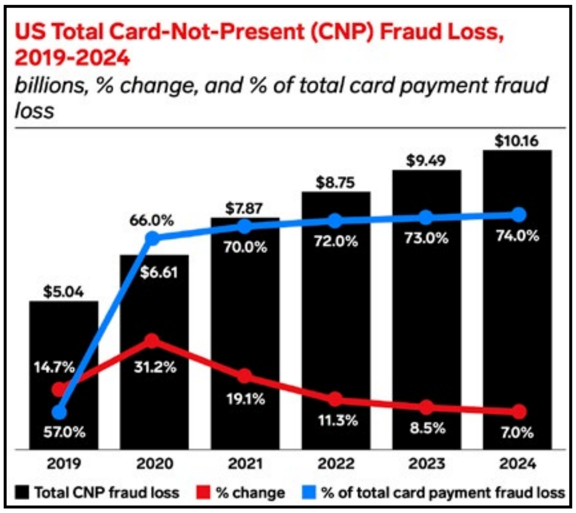
IN THIS REPORT

CONTENTS

BANKS • CONVENIENCE STORES • GAS STATIONS • CREDIT UNIONS • RETAIL CENTERS • RESTAURANTS

THE RISE OF SKIMMERS

Criminals have evolved into hackers, updating their games by targeting not just our money, but all of our data as well. As consumers embrace online shopping and digital transactions more, physical theft is in decline but it's not all good news. CNP (Card Not Present) fraud is on the rise due to emerging scams and technology used to perpetrate credit fraud. Skimmers are essentially homemade magnetic-striped card readers that are installed by criminals and hidden right alongside legitimate card readers. A single swipe is captured by both legitimate card reader and the skimmer which includes name, card number, expiration date and other data associated with their account.



CNP Ffaud Loss data provided by www.insiderintelligence.com

Super-slim inserts slide easily into existing card slots

Most skimmers are comprised of 3 primary components: a magnetic reading head, a plastic or metal façade that covers existing card readers and an insert that includes associated circuitry used to power, read and store the data that the skimmer's magnetic head reads. In addition, most ATM skimmers also include their own keypad overlays or tiny pinhole cameras that record every button press.

Plastic skimmers fit overtop existing slots

All captured data from the magnetic swipe and PIN entry is stored and later retrieved by criminals. It takes only seconds to install many of these overlays found in convenience stores and retail centers so it also takes about the same amount of time to retrieve this data. Some retrievals require a direct connection to the skimmer while others can be achieved wirelessly from distances up to 75 feet away. Besides the initial installation of the skimmer, the data retrieval is the only other time that criminals leave themselves open to witnesses or capture by authorities so they have increasingly designed their homemade skimmer systems to relay all captured data in a rapid fashion.

Takes seconds for criminals to install skimmer overlay

Skimmers are frequently found inside gas station pumps and ATMs but have also been discovered in various vending machines, smart meters and even retail POS (Point of Service) terminals. Installations of these skimmers generally take place in a matter of minutes or even seconds at night or during slow business hours to minimize possible witnesses. Due to the covert nature of skimmers, it is nearly impossible to estimate the number of them currently in operation but according experts, skimming (card not present fraud) costs consumers over $10 billion annually.

There is no national database dedicated solely to skimming statistics, but local and state police regularly tip their hands in the news by revealing sting operations leading to many skimmer seizures and arrests. If you take the time to do the research and the math, you will find that certain regions including Central Florida, Houston and Arizona are all hotbeds of skimmer activity.

Another great resource for education on skimmers (and this report) is KrebsOnSecurity.com. Brian Krebs reports on emerging skimmer technologies, crime busts and even performs his own inspections on suspicious ATMs from time to time.

TOP 6 REASONS
WHY SKIMMERS AREN'T GOING AWAY SOON

1 **Skimmers are essentially invisible.** Most consumers have swiped their cards through hundreds of different payment systems so there's no reason to suspect a skimmer is installed inside a machine that looks legit. Face it, skimmers are hard to locate.

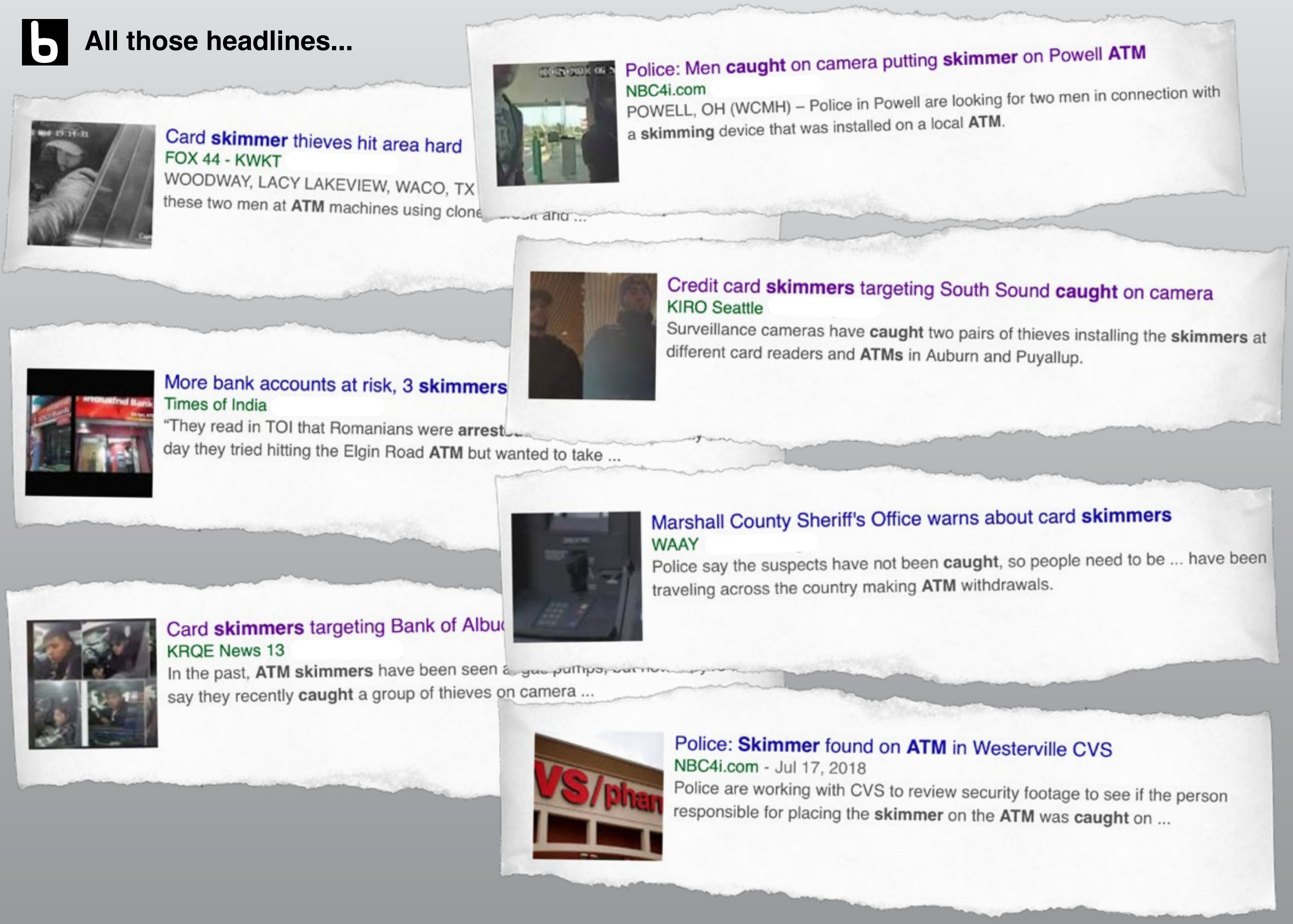
2 **Card reader/writers are cheap and readily available.** The hardware used to make skimmers can be purchased by anyone on Ebay for about $50. This same hardware can also be used to clone stolen cards and create new cards with stolen account data.

3 **Skimmer crime is low risk.** Skimmer installs take only seconds in some cases. The primary exposure that criminals face is data retrieval which is accomplished quickly and increasingly wirelessly.

4 **No one wants to talk about skimmers.** Retailers and banks do not want anyone to know they have skimmers on the premises. This business culture of quiet has kept consumers and the media from being properly educated on the problem of skimming.

5 **U.S. consumers are overly protected.** Since U.S. consumers are already protected by credit fraud, there is little incentive to prevent or take on skimmers directly. Instead, banks typically raise interest rates and fees to combat skimmer fraud which is then passed back onto consumers.

6 **All those headlines...**



Police: Men **caught** on camera putting **skimmer** on Powell **ATM**
NBC4i.com
POWELL, OH (WCMH) – Police in Powell are looking for two men in connection with a **skimming** device that was installed on a local **ATM**.

Card **skimmer** thieves hit area hard
FOX 44 - KWKT
WOODWAY, LACY LAKEVIEW, WACO, TX
these two men at **ATM** machines using clone ...it and ...

Credit card **skimmers** targeting South Sound **caught** on camera
KIRO Seattle
Surveillance cameras have **caught** two pairs of thieves installing the **skimmers** at different card readers and **ATMs** in Auburn and Puyallup.

More bank accounts at risk, 3 **skimmers**
Times of India
"They read in TOI that Romanians were **arrest**...
day they tried hitting the Elgin Road **ATM** but wanted to take ...

Marshall County Sheriff's Office warns about card **skimmers**
WAAY
Police say the suspects have not been **caught**, so people need to be ... have been traveling across the country making **ATM** withdrawals.

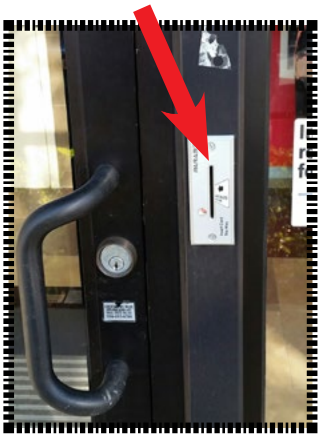
Card **skimmers** targeting Bank of Albu
KRQE News 13
In the past, **ATM skimmers** have been seen a...
say they recently **caught** a group of thieves on camera ...

Police: **Skimmer** found on **ATM** in Westerville CVS
NBC4i.com - Jul 17, 2018
Police are working with CVS to review security footage to see if the person responsible for placing the **skimmer** on the **ATM** was **caught** on ...

WHY HAS FIGHTING SKIMMERS FAILED SO FAR?

Over the years, organizations have attempted to address the problem of illegal skimmers by implementing new technology, educating consumers and proposing new legislation. But all have failed to stem the rising tide of card fraud and skimmers.

HARDWARE INFRASTRUCTURE



skimmer found inside this ATM lobby access control doorway

Security solutions ranging from specialty cameras to secured ATM lobby or vestibule access control hardware have been introduced into the marketplace. Yes, skimmers have even been found inside the lobby access doorway of banks. So before consumers inspecting suspicious ATMs for skimmers can even get close to those enclosed ATMs, their cards are getting skimmed!

There is no shortage of consumer guides offering safety and security tips to consumers. Thousands of whitepapers and blogs have also been published on this subject so I won't join that large list but I will recommend the thorough 'Credit Card Skimming: How to Spot and Avoid Fraudulent Charges' published by TSYS. There are certainly some valuable tips to be obtained here, but like all of these tip lists, suggesting that consumers use cash, pay inside or simply avoid some locations isn't very helpful or realistic. Consumers are a class bred on convenience so suggesting something slightly inconvenient will always fall onto deaf ears.

SERVICE INFRASTRUCTURE

Old POS terminal only accepts mag stripe cards

A lot of fanfare has been made over contactless pay and cards containing chips. Despite the tremendous growth of mobile POS terminals featuring NFC payments, the U.S. is still playing catchup to the rest of the world in many of these areas due to the existing financial infrastructure and expense to update of legacy terminals. Services such as Apple Pay, Android Pay and Samsung Pay have helped pave the way for tokenized transactions. These transactions essentially use a different key or code for every purchase so stealing PINs and even physical cards no longer benefits the crooks. Of course that didn't stop criminals from easily buying stolen consumer identities and loading fake digital cards into Apple Pay. Apple Pay gives banks the choice to require two-factor authentication or call-in authentication for new card authorizations. Most banks allow faster call-in authentications which are much easier to socially engineer and hack.

Very first magnetic stripe credit card from 1969

This year marks the 55th anniversary of the credit card in its current form. First invented by IBM in the 60s, the Air Travel Card was the first to include a embedded magnetic stripe. To this

A TRUE BRUTE FORCE ATTACK!

In early 2019, Hillsboro, Oregon Police discovered a Wells Fargo ATM destroyed by a stolen tractor. The thieves made off with the ATM's cash but lost police in high speed chase due to public safety concerns.

day, the data stored on these magnetic stripes is not encrypted nor protected in any way. EMV chips embedded into cards were supposed to fix security issues like this. Unfortunately, there are just so many older POS magnetic stripe readers still in use that new cards are still issued with old magnetic stripes as a backup. In an effort to speed up lines at the checkout counters, retailers sometimes force consumers to swipe their cards rather than insert them into the more secure chip reader slot.

LEGAL SYSTEM

Legislative proposals against skimming have gained attention but still suffer from a lack of technical understanding. Laws against fraud are foundationally built upon the presence of physically stolen cards or CP (Card Present) charges. Illegal skimming does not require any physical cards except for the initial swipe and skim. All card data that is cloned or sold is treated as CNP or Card Not Present. These crimes are lumped in with other fraud such as a purchase made online without knowledge of consent of the card owner. Fraud laws are written to encompass a variety of crimes that mostly stop at the thief but the damage caused by skimmers goes far beyond one criminal. Typical statutes and convictions usually result in misdemeanors and small fines providing the criminal doesn't rack up a large amount of stolen property. The problem is that it's nearly impossible for law enforcement to connect fraudulent charges made with one card back to that original skimmer.

THERE ARE JUST SO MANY OLDER POS MAGNETIC STRIPE READERS STILL IN USE THAT NEW CARDS ARE STILL ISSUED WITH OLD MAGNETIC STRIPES AS A BACKUP.

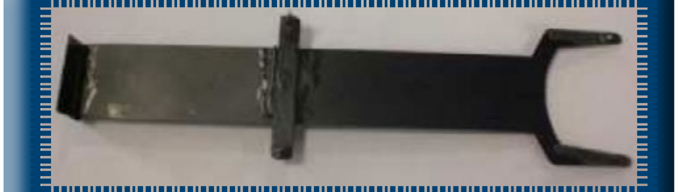
LAW ENFORCEMENT TOOLS

Besides skimmer prevention tips, law enforcement have few options in the way of tools to fight skimmers. Academics have begun researching skimmer detection and prevention methods but no professional tools are commercially available yet. These efforts can take years to raise money for research and prototyping. As far as the private sector, skimmer thieves appear to move too fast for any large scale product deployments that law enforcement can rely on. Government agencies move even slower than that and have approached small security firms to help solve the problem. So where does that leave our police and federal agents?

Banks and gas stations talk about preventative measures but keep their customers in the dark, and the courts can only slap the wrist of criminals after the damage has been done. Academics and security researchers have also weighed in but they offer little more than theoretical solutions. It's no mystery how illegal skimmers have become so pervasive when you consider all of the hobbled attempts to stop them. That only leaves law enforcement leading the fight against skimmers.

Law enforcement toolsets require fast turnaround and highly innovative approaches to combat the rapidly evolving landscape of skimmers and other cybersecurity related threats. Working with authorities over the past 15 years has provided my engineering team with invaluable feedback that could only have come from agents in the field. These same agents demand effective, working solutions.

FORK OVER THE DOUGH!



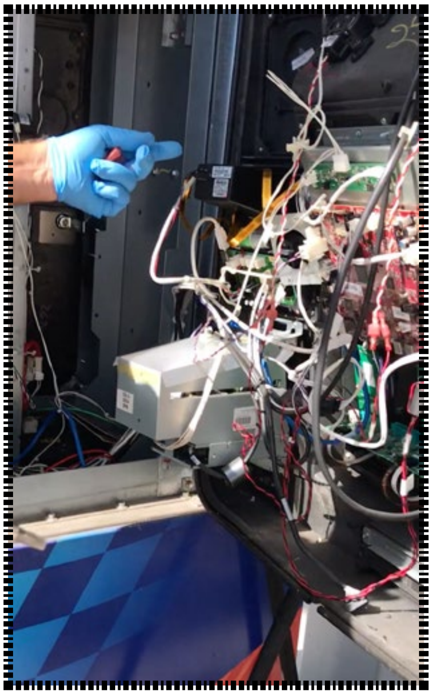
These medievil looking contraptions pry open ATM cash dispensers long enough for criminals to grab the cash and run off. Forking isn't subtle and does not put debit card data at risk, but it is a quick payday for criminals targeting older ATM mechanisms.

The same Internet that has revolutionized our purchases and communications has also fed the dark underbelly of the criminal world. The Dark Web is the digital black market that is home to many criminal enterprises including the trade and sale of credit and debit cards accounts. We have all fallen prey to some kind of fraud but did you know that the going rate for the average stolen card on the Dark Web is only $15? Criminals typically bundle and sell thousands of these cards to other thieves who will then re-sell or use them by simply cloning that data onto a blank card and making purchases. According to experts, the average skimmer nets about $100,000 before it is discovered or stops working. That is a lot of cards, victims and criminals linked by one simple device. You would think that gas stations and banks would require skimmer inspections for all kiosks and kiosk service providers but they are too busy with customers and cost savings to take this kind of action.

BLUE SCREEN OF DEATH!

Jackpotting is malicious software introduced directly into an ATM forcing it to spit out huge volumes of cash. Many ATMs continue to run Windows® XP which has stopped receiving security updates from Microsoft years ago. To crooks understanding how to easily gain access to the OS and USB ports, infecting an ATM with custom malware is as simple as plugging a USB stick into your PC. This kind of attack has long plagued Europe and Asia but hasn't hit the U.S. until only recently.

AVERAGE SKIMMER NETS ABOUT $100,000



Spotting bluetooth skimmer needle in a haystack

Over the years, many gas stations have been approached by consumer advocate groups and news media outlets demanding they check their pumps for skimmers. The ones that comply are forced to shut down their pumps while authorities tediously comb through each one for hidden skimmers. In early 2018, I accompanied FDACS (Florida Dept. of Agriculture & Consumer Services) representatives in St. Petersburg on one of these expeditions and while we didn't discover any skimmers, we spent the better part of day looking for them. All of that time spent searching through a gas station temporarily closed down for business got me thinking. What if we could detect hidden skimmers quickly and effectively?

IT'S A TRAP!

This Card trap physically keeps ATM cards from being removed from their slot using razor-edged spring traps. Frustrated consumers either give up or leave to get help. As soon as they leave the scene, hackers swoop in to spring the ATM card free and take off with it. Simple but effective.

TOP 5 PUMP PROBLEMS

SELF-SERVE CRIMINALS

Bluetooth has evolved a lot since then but the hackers are still attracted to bluetooth's low cost, low power consumption, small size and ubiquity. Criminals have made bluetooth the centerpiece in their wireless skimming enterprises for gas stations in particular. Gas station pumps serve as the perfect conduit for skimmers in the U.S. and abroad for the following reasons:

- **All gas pumps (except in NJ and OR) are self-serve making skimmer installation easier**
- **Only 5 different keys can access 95% of all gas pumps and those 5 keys are all on Ebay**
- **Unlike ATMs, gas pumps do not contain incriminating video cameras or reinforced locks**
- **Visa and Mastercard have extended EMV compliance deadlines for gas stations to 2020**
- **There are 150,000 vulnerable gas stations in the U.S. and 300,000 more internationally**

> “RATHER THAN TAKING APART THE ENTIRE DISPENSER TO GET IN AND LOOK FOR A SKIMMER, THIS ALLOWS THE SERVICE COMPANY OR REGULATORY AGENCY TO DO A QUICK SCAN.”
>
> - BILL CALLAWAY, CROMPCO TANK TESTING

SOLUTIONS AT THE PUMPS

A BLUESLEUTH IS ON THE CASE

Back in 2001, my company developed Mantis, the first professional bluetooth testing device for the emerging bluetooth standard. We sold hundreds of units, but the skimmer landscape has changed a lot since those days. These days, we all carry smartphones capable of bluetooth as low cost wireless modules from China flood the market. And that same ubiquity we find in bluetooth devices has also carried through to criminal use against nearly every single consumer. A new security tool is needed.

Pump inspector's job has become much easier thanks to BlueSleuth-Pro

BlueSleuth-Pro™ focuses on only Bluetooth and BLE (Bluetooth Low Energy) devices, tags, beacons and of course skimmers. The unit includes a direction finding antenna and some software smarts to help identify hidden skimmers within a sea of mostly benign bluetooth devices. There are a handful of iOS and Android apps such as Skimmer Scanner that already detect possible bluetooth skimmers but these apps rely on a consumer phone OS and hardware. They are not dedicated devices with a specialized antenna for hunting down skimmers.

BlueSleuth-Pro™ was first unveiled to its core customer base at the National Conference on Weights and Measures conference in 2018. The NCWM ensures national standards keep pace with evolving technology and includes state and local regulators, regulated industries and federal agencies to ensure the highest level of expertise is combined with practical limitations for the development of fair model standards for adoption by all U.S. states and territories.

We've sold thousands of Bluetooth detection hardware to federal and state agencies looking to secure their networks and facilities against wireless threats, but there is much more work to do.

Bluetooth skimmers are an epidemic amid gas service stations for all of the reasons already covered but credit fraud and theft through ATMs and vending machine kiosk skimmers is an entirely different problem requiring a unique engineering approach.

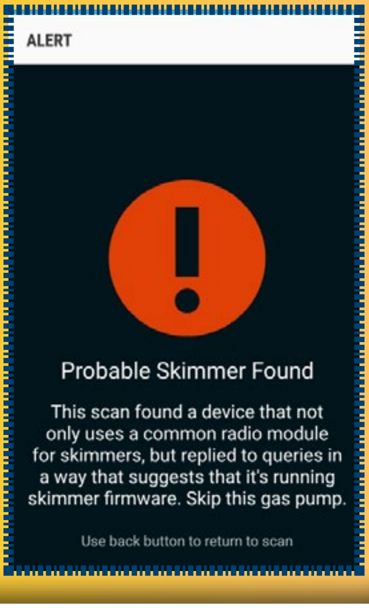
BLUESLEUTH-PRO
RESET VOICE
10:25
70
TAGS
BLE
BT
BEACON
D7:0A:34:F3:72:FB APPLE AIRTAG 20 MINS -43
00:16:AD:8E:71:15 CHIPOLO 45 MINS -69
18:00:DB:0D:A1:17 NR APPLE AIRTAG 20 MINS -78
18:65:90:0E:1B:23 GLX SMART TAG 20 MINS -84
00:16:AD:8E:71:15 TILE TRACKER 35 MINS -86
WHITE LIST
SORT ON
SORT OFF
EDIT WHITE LIST
5 OF 12
BLUETOOTH & BLE LOCATOR

BlueSleuth-Pro™ locates hidden BT/BLE skimmers as well as BLE Tags, Devices & Beacons

THE LIMITATIONS OF SMARTPHONE BLUETOOTH SCANS & APPS

Many law enforcement agents, news reporters and consumer advocates have tried to empower consumers by providing them with skimmer security tips including use of their own smartphones to discover skimmers. Cell phones can only provide a crude warning at best and have no way of indicating direction, distance or which gas pump could possibly contain a skimmer.

Bluetooth device scans and apps do not effectively locate skimmers. Modern smartphone antennas and receivers are not designed to continuously report true signal strength of any bluetooth devices. Your smartphone will occasionally display a suspicious or unknown bluetooth device, but it cannot lock onto or locate it through wireless directional antenna procedures.



ALERT

Probable Skimmer Found

This scan found a device that not only uses a common radio module for skimmers, but replied to queries in a way that suggests that it's running skimmer firmware. Skip this gas pump.

Use back button to return to scan

CRYING ALL THE WAY TO THE BANK OR CREDIT UNION

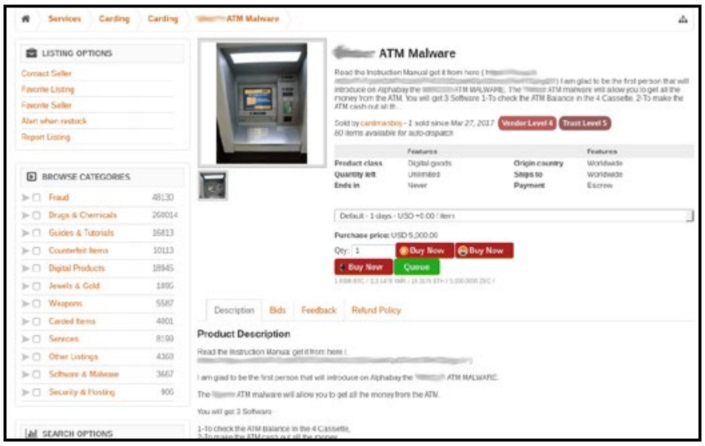
ATM FRAUD AND ITS VICTIMS

Ever since ATMs first appeared in banks, credit unions and convenience stores, they've been the target of criminals. Once, a small fortune of crisp twenty, fifty and hundred dollar bills were the prize for cracking open ATMs. If thieves managed to cleanly drill or pry open the ATM safe, they could walk away with unscathed currency. But these days, ATMs hold something even more valuable than money inside their reinforced steel walls.

Data is the new gold standard for currency. It can be bundled, traded and sold instantly to anyone. Unlike physical currency, data doesn't need to be laundered and can be infinitely duplicated sold and re-sold to every crook in the world. With the Dark Web acting as a black market for window shopping and transactions, criminals and hackers can freely distribute malicious code, modified ATM hardware and how-to guides on a variety of illegal scams including skimmers. A busy ATM can host hundreds of transactions per day. With some 3.5 million ATMs installed globally, you might need a calculator just to figure out how much data is getting stolen every day.

> IDENTITY THEFT FUELS THINGS LIKE RANSOMWARE, IP THEFT AND LOST PRODUCTIVITY WITH DAMAGES TOTALING $10.5 TRILLION BY 2025.

SOURCE: CYBERSECURITY VENTURES' 2017 CYBERCRIME REPORT


Services › Carding › Carding › [redacted] ATM Malware

LISTING OPTIONS

Contact Seller
Favorite Listing
Favorite Seller
Alert when restock
Report Listing

BROWSE CATEGORIES

Fraud	48130
Drugs & Chemicals	260014
Guides & Tutorials	16813
Counterfeit Items	10113
Digital Products	18845
Jewels & Gold	1895
Weapons	5587
Carded Items	4001
Services	8199
Other Listings	4369
Software & Malware	3667
Security & Hosting	906

SEARCH OPTIONS

[redacted] ATM Malware

Read the Instruction Manual get it from here ([redacted]) I am glad to be the first person that will introduce on Alphabay the [redacted] ATM MALWARE. The [redacted] ATM malware will allow you to get all the money from the ATM. You will get 3 Software 1-To check the ATM Balance in the 4 Cassette, 2-To make the ATM cash out all th...

Sold by cardmanboy - 1 sold since Mar 27, 2017 Vendor Level 4 Trust Level 5
80 items available for auto-dispatch

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 5,000.00

Qty: 1

Product Description

Read the Instruction Manual get it from here ([redacted]

I am glad to be the first person that will introduce on Alphabay the [redacted] ATM MALWARE.

The [redacted] ATM malware will allow you to get all the money from the ATM.

You will get 3 Software

1-To check the ATM Balance in the 4 Cassette,
2-To make the ATM cash out all the money

Dark Web pages like this sell ATM malware and how-to manuals to any hacker

However, no calculator can predict just how much damage will be done. This is because metadata like names, account numbers, country codes and expiration dates are stored on the magnetic stripe embedded within every ATM debit and credit card. These pieces of information can be used to burn copies of that card, put towards future fraudulent purchases or sold to hackers looking to piece together full stolen identities also for sale. Identity theft fuels things like ransomware, IP theft and lost productivity with damages totaling $10.5 trillion by 2025 according to Steve Morgan of Cybersecurity Ventures.

Skimmers are the gateway drug to malicious hacking, credit fraud and online theft. They are easy to install and hard to spot, but you already know that by now if you read through this report from the beginning. Countries that have been slow adopt stronger security standards such as EMV technology will endure the brunt of credit fraud as the weakest links. That puts the U.S. as a prime target for the next few years until its banks, gas stations and the laws catch up with other 1st world nations. For now, consider the antiquated magnetic strips

QUICK FACTS:

- **There are more than 3.2 million ATMs worldwide**
- **About every six minutes, a new ATM is installed somewhere in the world**
- **Annually, there were 69 billion worldwide ATM cash withdrawals in 2021**

SCANNING ALL THE WAY TO THE BANK OR CREDIT UNION

SECURING ATMS & RETAIL CARD READERS

All skimmers involve a physical breach and a hidden device that captures card data for future monetization. Skimmer thieves play the long game and are more akin to white collar criminals rather than blue collar thieves who might mug someone for their cash. Both are dispicable crimes but it's important to understand motives and methods so that the best crime fighting tools can be developed. That is where the **Skim Scan**™ and **Skim Swipe**™ come into play.

Skin Scan provides instant peace of mind.
No expensive hardware mods required.
No time consuming inspections required.

Some skimmer detectors try to fight skimmers proactively but this requires expensive and time consuming hardware modifications to every single ATM or POS terminal. Rather than fighting skimmers preemptively, Skim Scan attacks the problem by streamlining law enforcement procedures and personnel already in place. Insert Skim Scan into any ATM or gas pump just as you would any credit or debit card and that's it. A green light means there's no skimmer detected and a red light and audible alarm indicates the presence of a skimmer. This method detects deep insert skimmers hidden inside gas pumps, ATMS and even ATMs that use solenoids to block non-conforming cards.

Now compare this to the old procedure of obtaining permissions, keys, codes and performing lengthy searches inside every ATM to find hidden skimmers. Many kiosks contain a rat's nest of wires so visual inspections on every machine isn't very effective and ties up law enforcement agents.

Skim Swipe™ works the same way except for card swipers generally found in conveneince stores, travel centers and most retail point-of-sale terminals. A single Skim Swipe used daily can virtually end credit and debit card fraud resulting from hidden skimmers and free up workforces for more important tasks.

The future of skimmers is always evolving. Shimmers are a new form of skimmer as they target the supposedly unhackable EMV chips inside modern cards. These shimmers are more sophisticated than run of the mill skimmers, but still rely upon obfuscation and consumer ignorance to steal data. At this time we can only say that we are working harder and faster than the criminals to catch up.

Skin Swipe detects skimmers hidden inside a card reader overlay.

ABOUT THE AUTHOR

INTERSECTION OF CYBERSECURITY & WIRELESS SECURITY

Under the direction of CEO and President, Scott N. Schober, Berkeley Varitronics Systems (BVS) has designed and manufactured thousands of RF analysis and wireless threat detection tools for Fortune 500, military, educational and government organizations to manage secure facilities and their wireless networks. The sharp uptick of cybersecurity attacks in recent years has led BVS to develop content to educate businesses on a variety of cybersecurity topics including ransomware, credit card skimming, drone security and contraband Wi-Fi, Bluetooth and 3G/4G/5G wireless threat detection products. Berkeley Varitronics lives at the intersection of cybersecurity and wireless security.

BVS lives at the intersection of cybersecurity and wireless security

Scott Schober is President & CEO of BVS, a 52 year old private firm

Scott Schober is a wireless and cybersecurity expert appearing regularly on national news networks and shows including Bloomberg, CNN, Good Morning America, Fox News, CBS This Morning, MSNBC, CGTN and hundreds more. Scott is also a presenter and author of Hacked Again, a book inspired from his own battles with hackers and vow to help others learn from his mistakes. Hacked Again is available on Amazon where it currently boasts a 4.3 star rating out of 243 reviews.

Scott wrote *Hacked Again* to tell others his own story, *Cybersecurity is Everybody's Business* to help business owners and *Senior Cyber* to help his parents and grandparents avoid becoming the #1 target of cyber criminals.

JPMorgan
JP MORGAN CYBER ATTACK
BANK DATA AT RISK
INFO FROM 83M CHASE CUSTOMERS EXPOSED
arliament in election overshadowed by Ukraine crisis, Russia
6:33 PT
AMERICA

FOX NEWS LIVE
STATES CONSIDER TRACKING DRIVERS' MILEAGE TO TARGET ROAD TAXES
AMERICA'S newsroom
DETROIT-BASED AUTOMAKER FROM A YEAR AGO
S&P ▲ 0.96

NEW DAY
NEW DETAILS
SCOTT SCHOBER
PRESIDENT & CEO, BERKELEY VARITRONICS SYSTEMS, INC.
LIVE CNN
RIGHT NOW
CHICAGO 42°
DETROIT 37°
HOUSTON 66°
GE CULTURAL INFORMATION AND I HAVE "NO REGRETS"