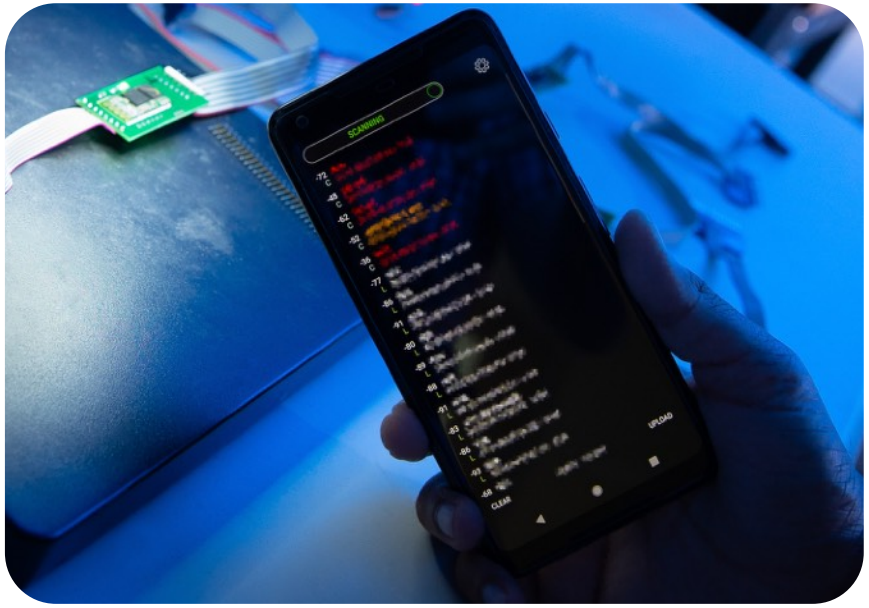


Please Pay Inside

Evaluating Bluetooth-based Detection of Gas Pump Skimmers

Nishant Bhaskar, Maxwell Bland, Kirill Levchenko, Aaron Schulman

UC San Diego

ILLINOIS

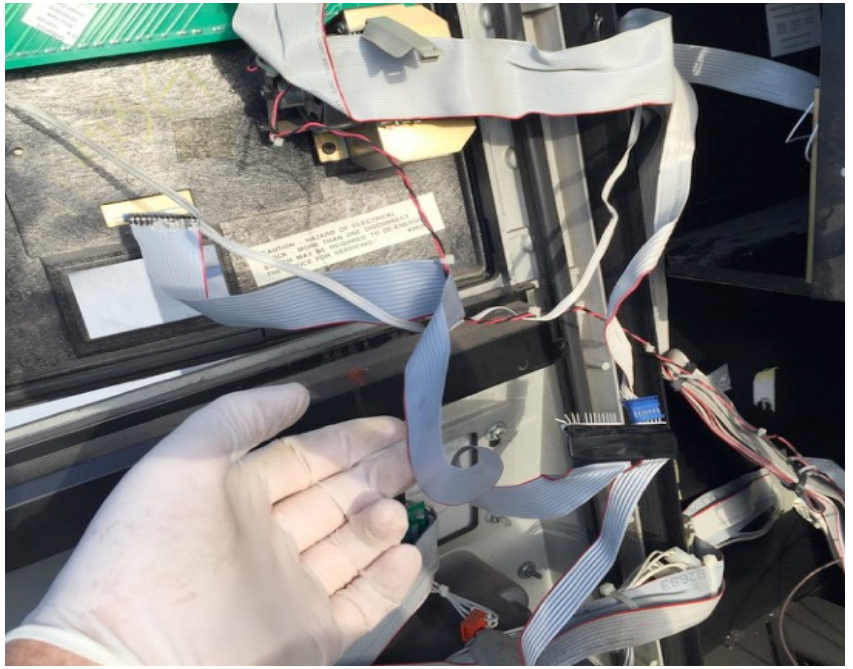
Card skimming at gas stations is a significant problem

Skimmers are found at gas stations across the U.S.

- **972** in Florida and **148** in Arizona in 2018
- **50% increase** from 2017

Skimming is a lucrative business

- **30-100 cards** per skimmer per day, $500 per card
- Estimated fraud in 2018: > **$16 million in one day**



Source: Arizona Weights and Measures

Gas pumps are an ideal target for skimming

Gas pumps have weak security

1. Doors **open easily**
2. Card data is **in the clear** on internal wiring

Gas stations have poor video surveillance

Source: Arizona Weights and Measures

Gas pumps are an ideal target for skimming

Gas pumps have weak security

1. Doors **open easily**
2. Card data is **in the clear** on internal wiring

Gas stations have poor video surveillance

Source: Arizona Weights and Measures

Gas pumps are an ideal target for skimming

Gas pumps have weak security

1. Doors **open easily**
2. Card data is **in the clear** on internal wiring

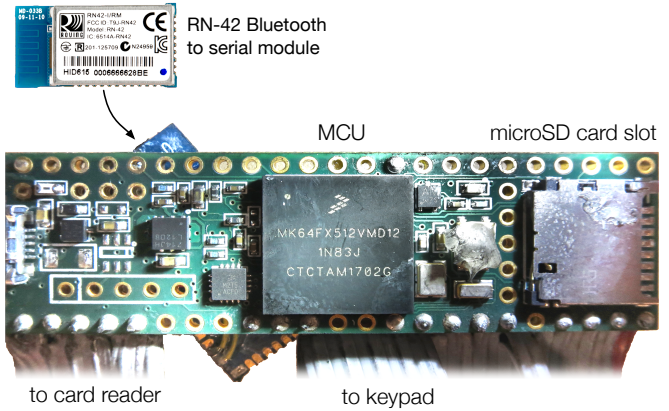
Gas stations have poor video surveillance

Source: Arizona Weights and Measures

Internal gas pump skimming hardware design

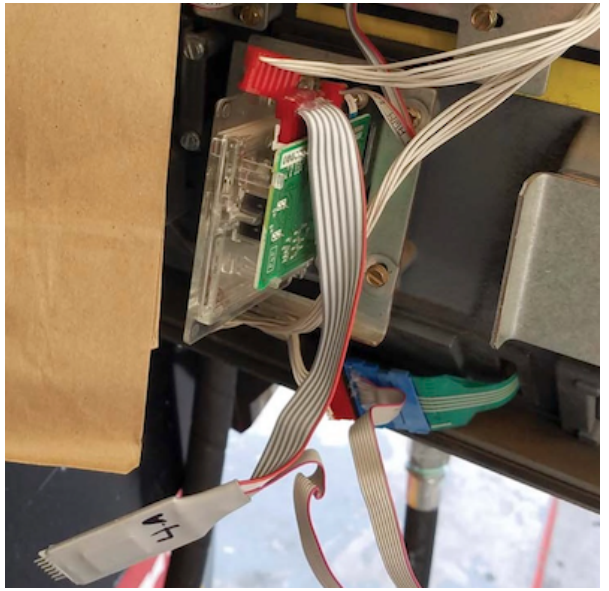
Skimmers are built from off-the-shelf parts

- Microcontroller development board
- **Bluetooth-to-serial module** for data exfiltration



Installers tap skimmers into payment wiring

- Passively reads payment card data
- **Hidden completely inside** pump enclosure

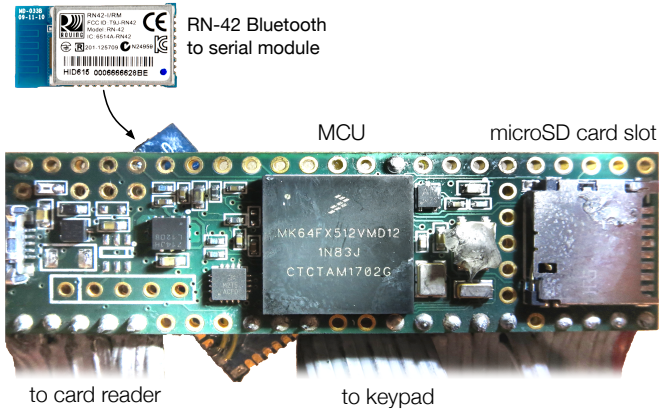


Source: Arizona Weights and Measures

Internal gas pump skimming hardware design

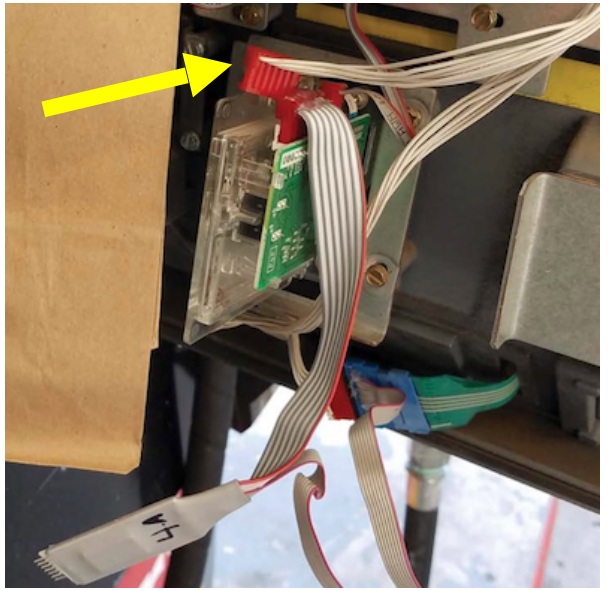
Skimmers are built from off-the-shelf parts

- Microcontroller development board
- **Bluetooth-to-serial module** for data exfiltration



Installers tap skimmers into payment wiring

- Passively reads payment card data
- **Hidden completely inside** pump enclosure

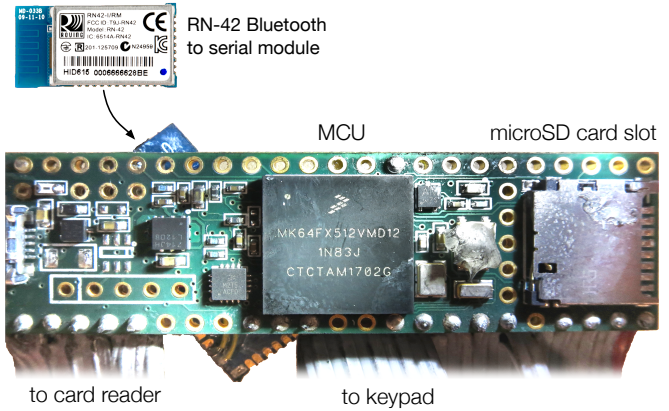


Source: Arizona Weights and Measures

Internal gas pump skimming hardware design

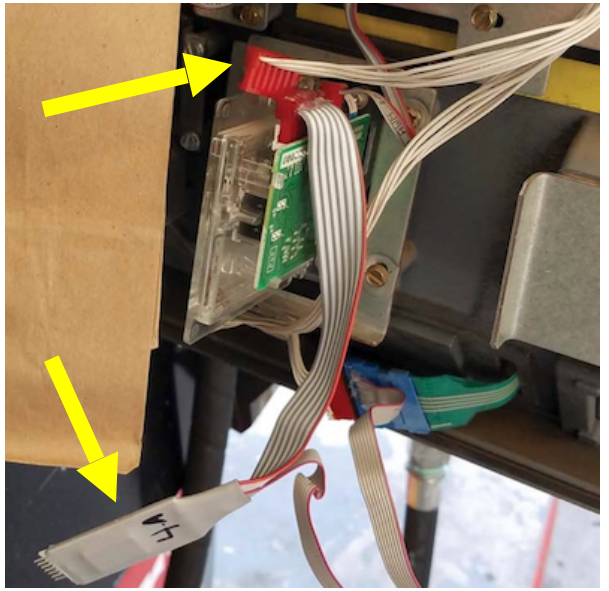
Skimmers are built from off-the-shelf parts

- Microcontroller development board
- **Bluetooth-to-serial module** for data exfiltration



Installers tap skimmers into payment wiring

- Passively reads payment card data
- **Hidden completely inside** pump enclosure



Source: Arizona Weights and Measures

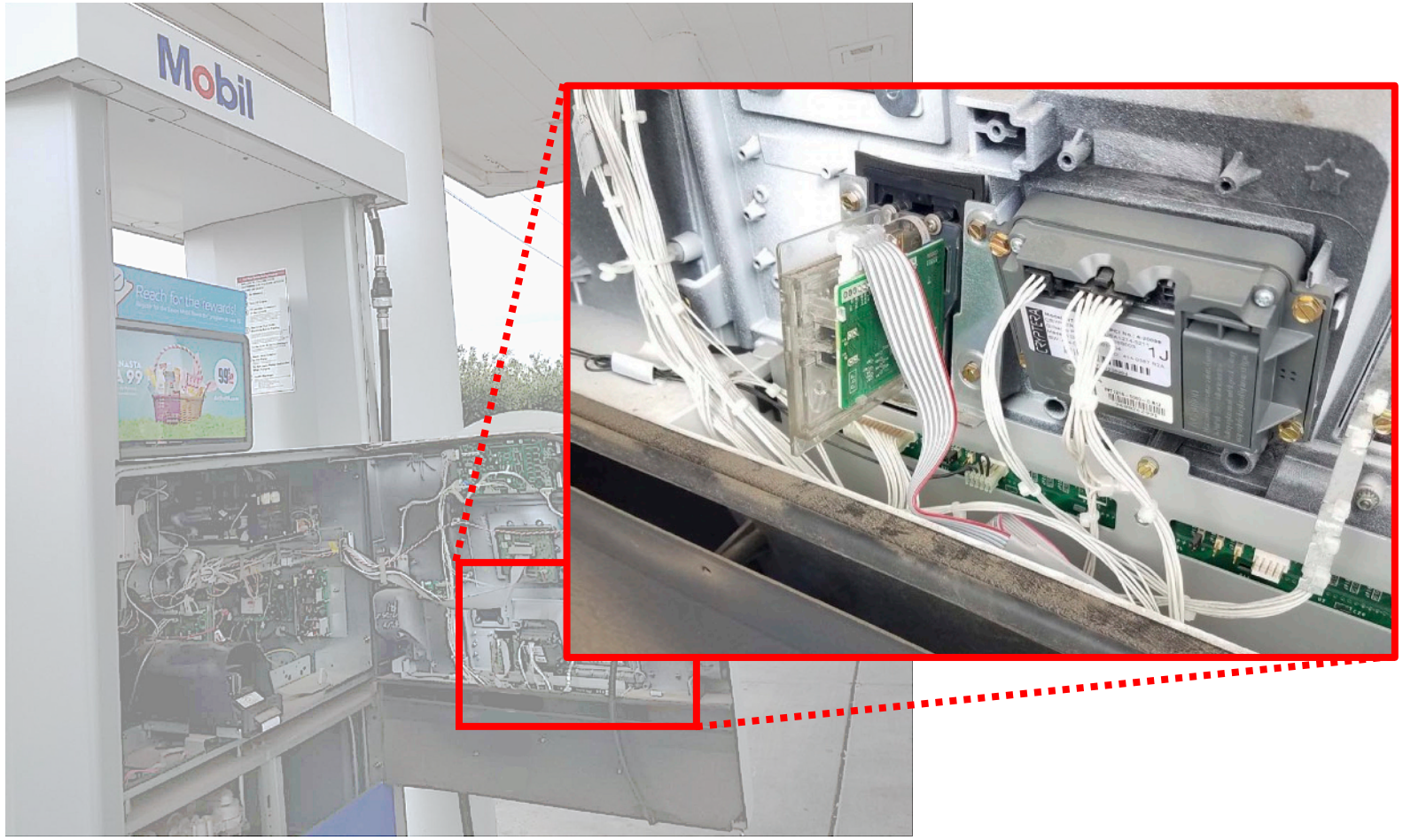
Skimmers installs take less than 30 seconds

Source: Arizona Weights and Measures

Skimmers installs take less than 30 seconds

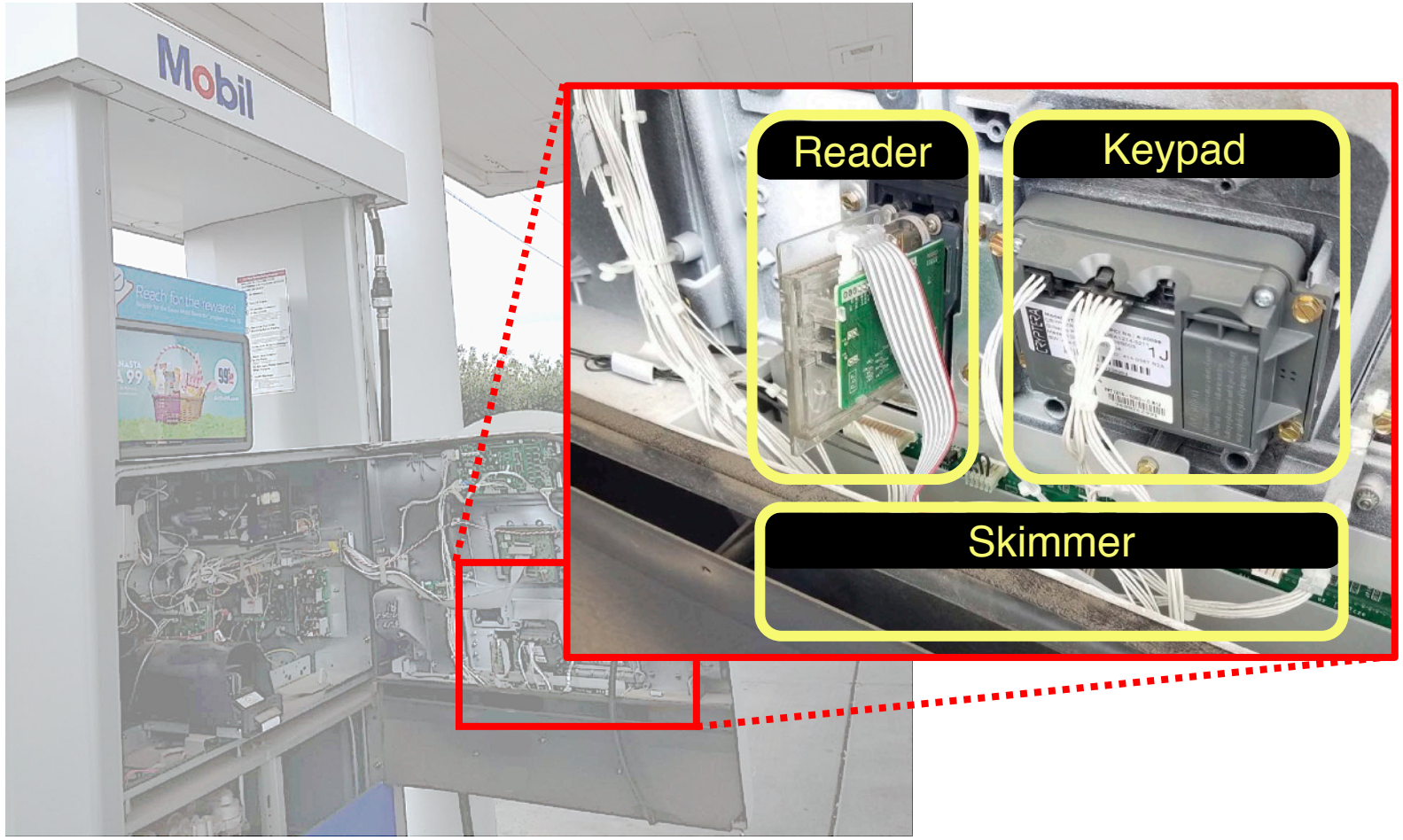
Source: Arizona Weights and Measures

Skimmers installs take less than 30 seconds



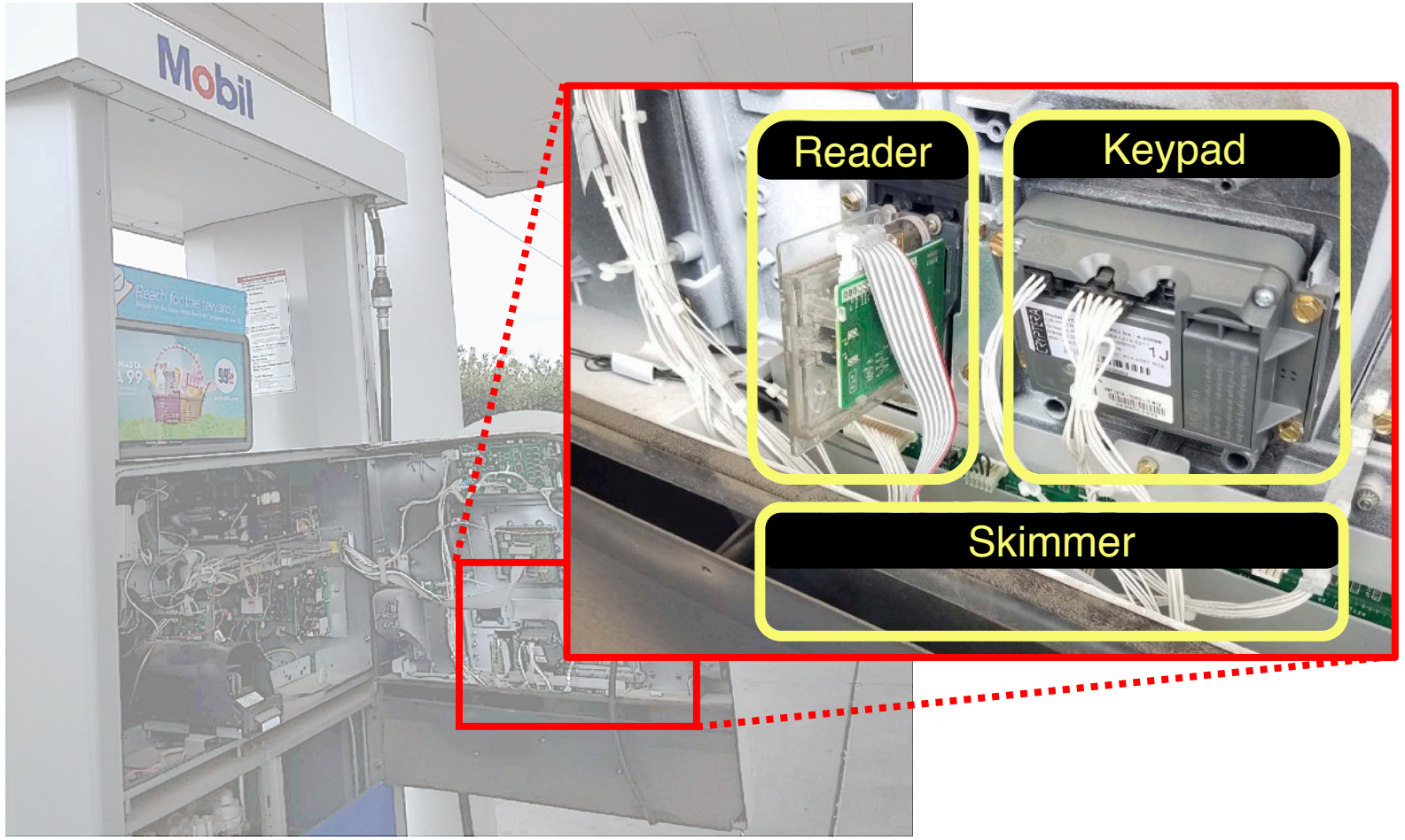
Source: Arizona Weights and Measures

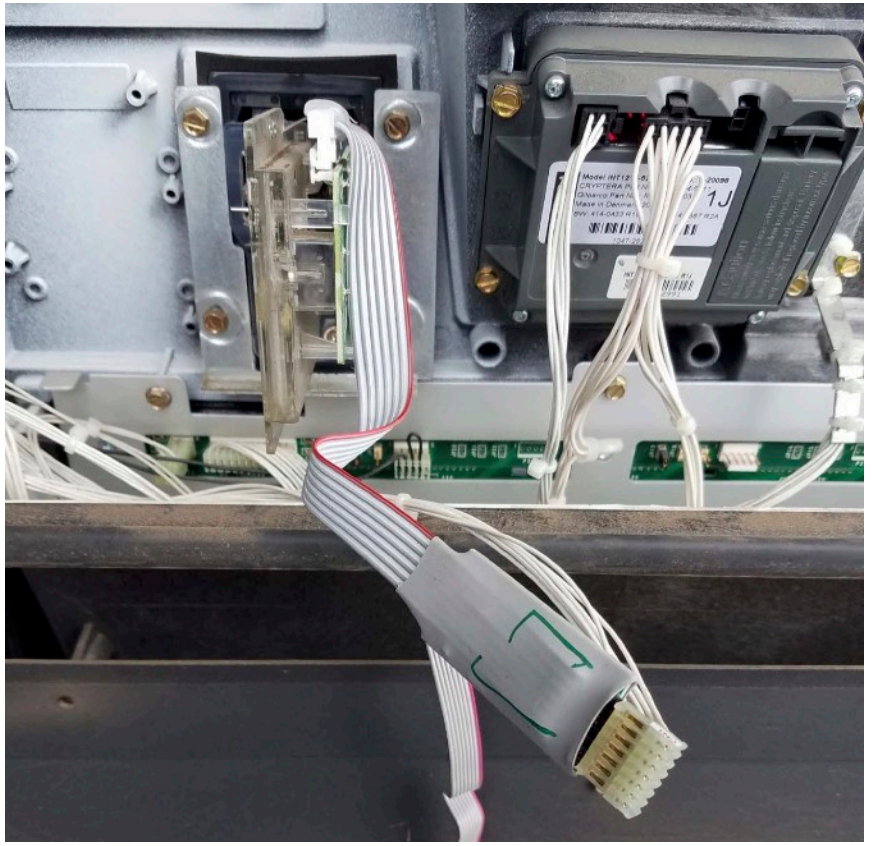
Skimmers installs take less than 30 seconds



Source: Arizona Weights and Measures

Skimmers installs take less than 30 seconds





Source: Arizona Weights and Measures

It is difficult to find skimmers in gas pumps

Finding skimmers is like finding a needle in a haystack

- **7,325** skimmer inspections in AZ (2016-18)
- Skimmers were found in **only 1.5%** inspections

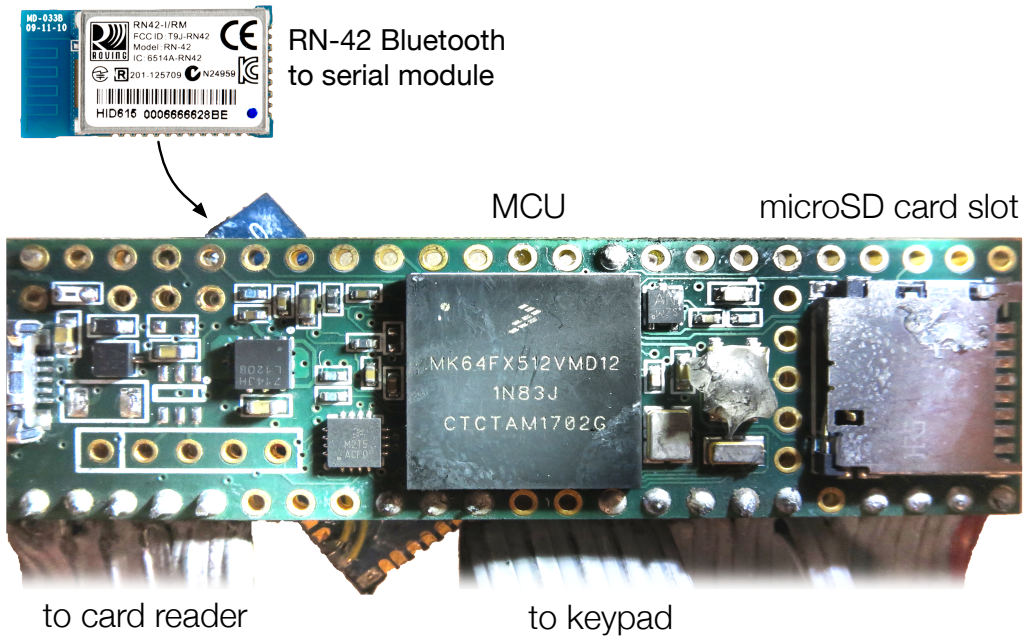
Common detection mechanisms are ineffective

- E.g., Tamper-proof seals (Scaife et al., S&P `19)

Criminals retrieve data from the comfort of their car

Bluetooth enables inconspicuous smartphone-based data retrieval

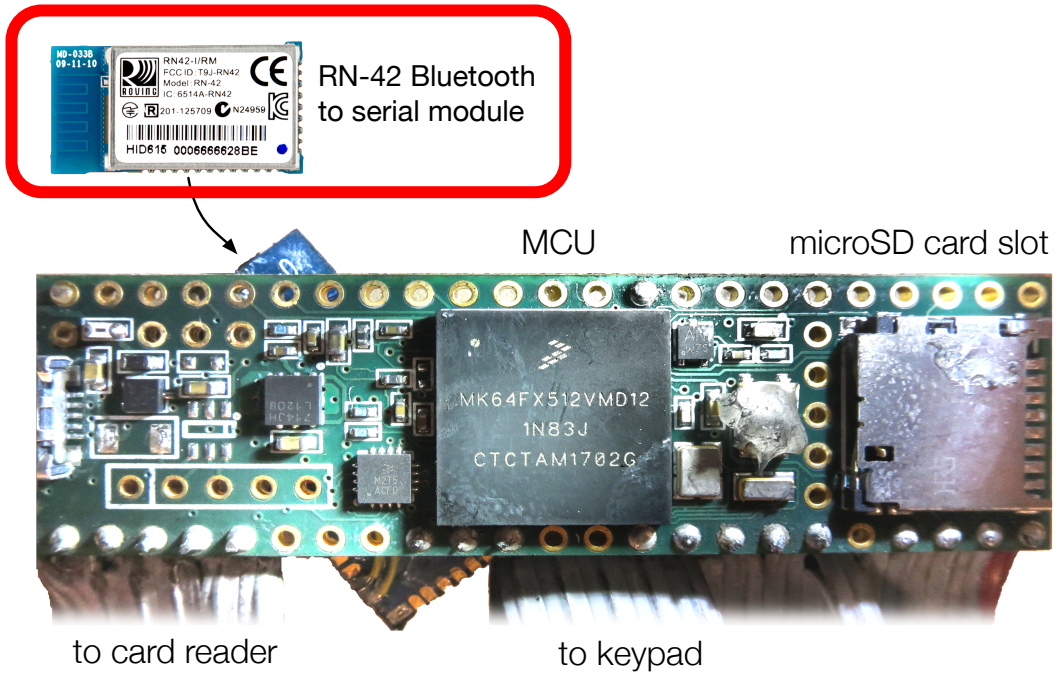
1. Scan for nearby Bluetooth devices
2. Connect to a skimmer
3. Download card data



Criminals retrieve data from the comfort of their car

Bluetooth enables inconspicuous smartphone-based data retrieval

1. Scan for nearby Bluetooth devices
2. Connect to a skimmer
3. Download card data



Criminals can find their skimmers with smartphones, why can't we?

Can smartphones detect skimmers without opening pumps?

We need to do a large-scale study to evaluate how effective it is

Data collection methodology

Developed custom Bluetooth scanning app called Bluetana

44 officials collected Bluetooth scans and inspected pumps

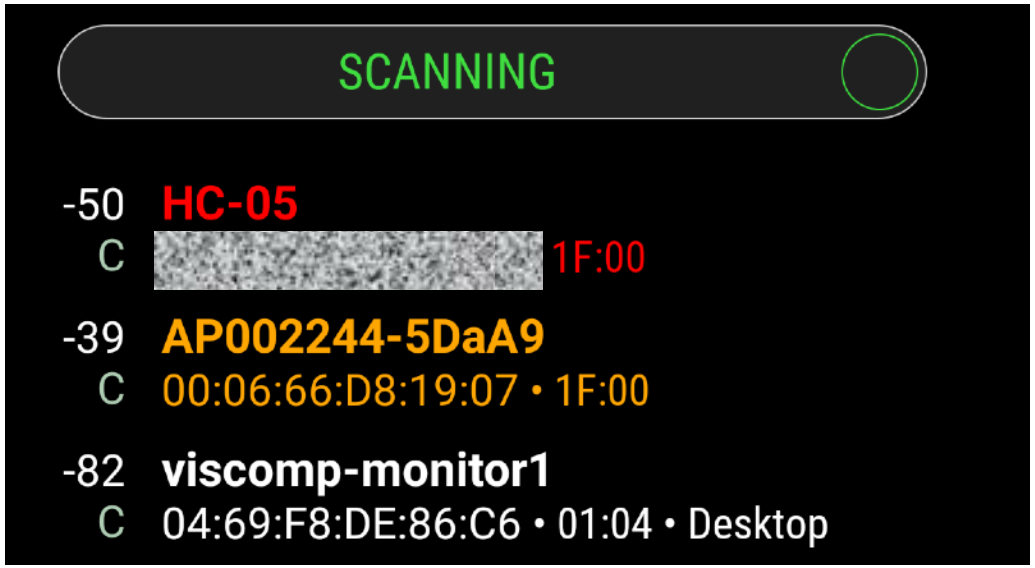
Crowdsourcing Bluetooth scanning for skimmers

Bluetana detection app

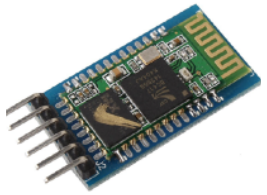
- Runs on inexpensive **($50)** Android phones

Records Bluetooth all scan data

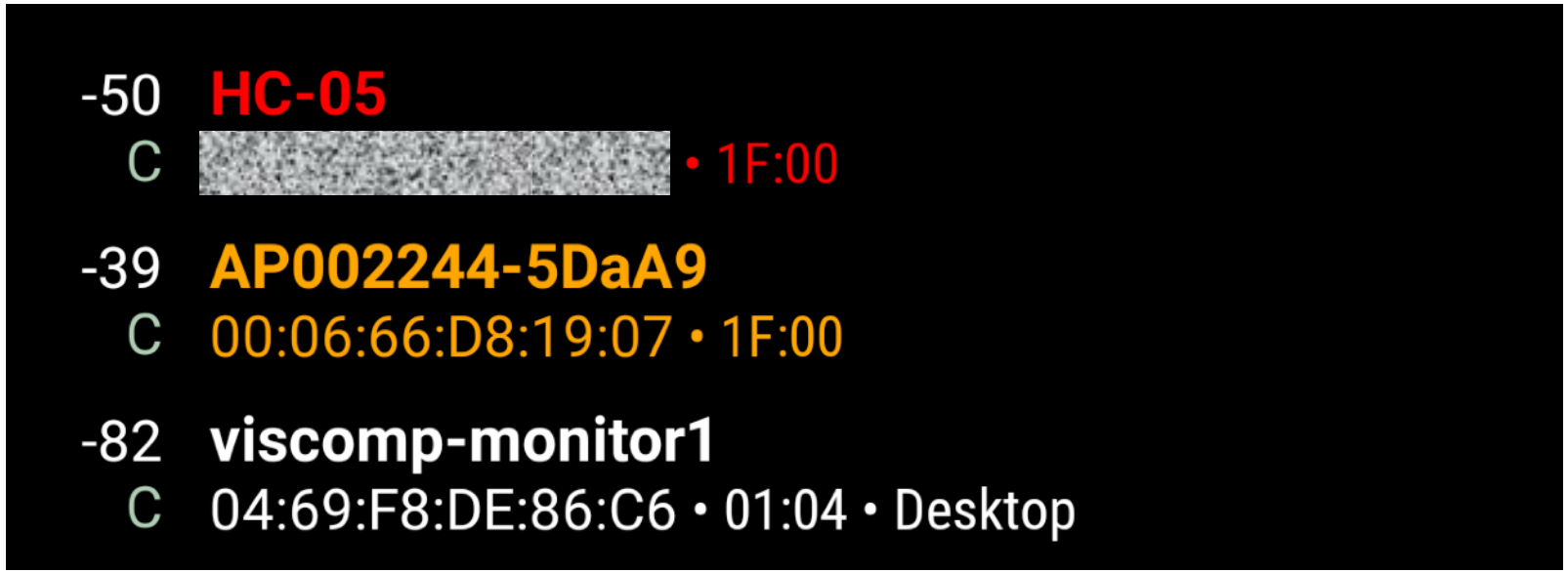
- Device Name, MAC, Class-of-Device, RSSI



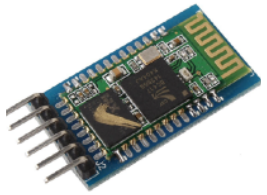
Indicating suspicious devices



Module	Class of Device	MAC Prefix	Device Name
RN 41/42	Uncategorized	00:06:66	“RNBT-xxxx”
HC 05/06	Uncategorized	Various	“HC-05/06”

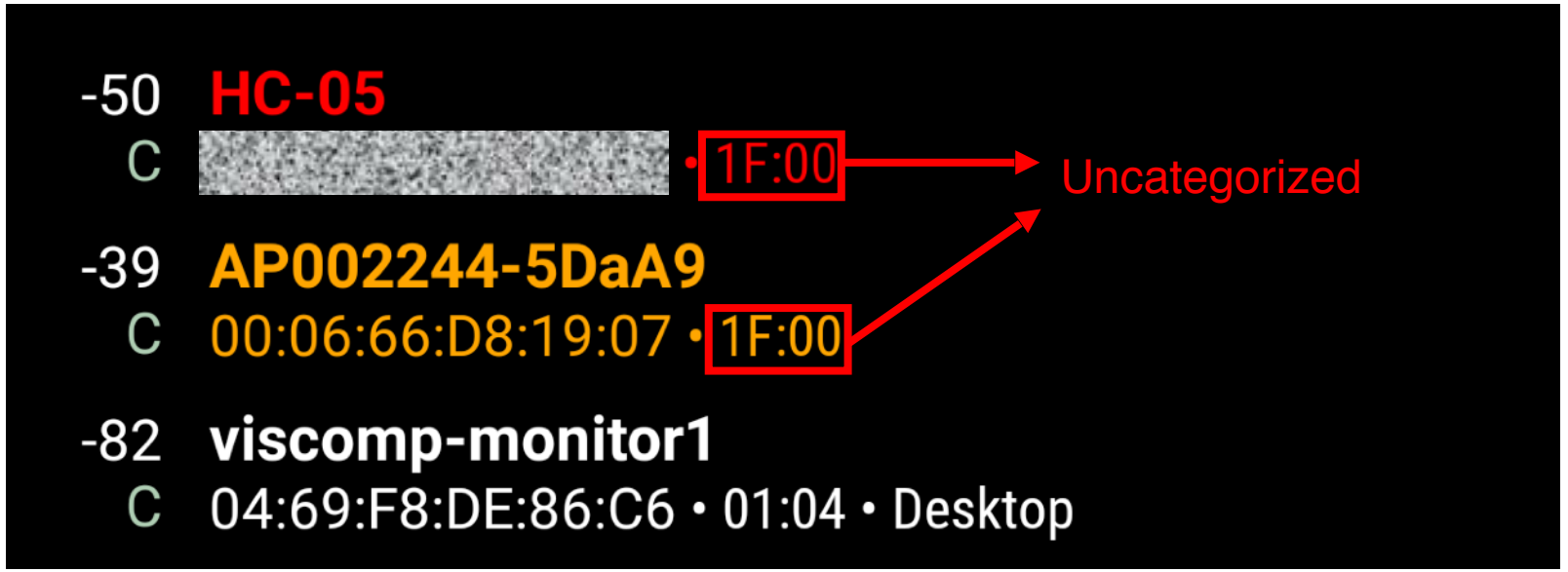


Indicating suspicious devices

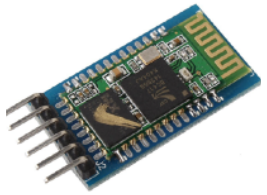


1

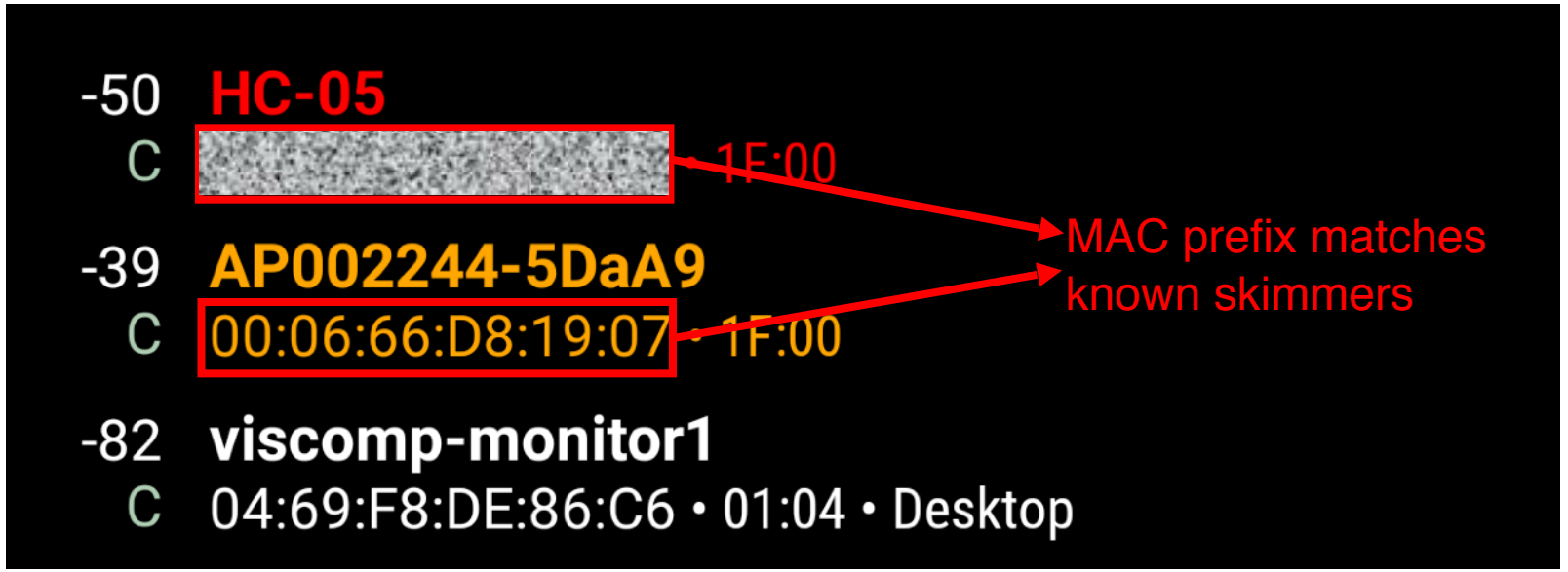
Module	Class of Device	MAC Prefix	Device Name
RN 41/42	Uncategorized	00:06:66	“RNBT-xxxx”
HC 05/06	Uncategorized	Various	“HC-05/06”



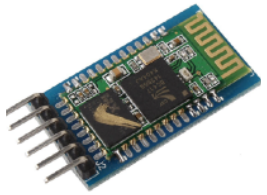
Indicating suspicious devices



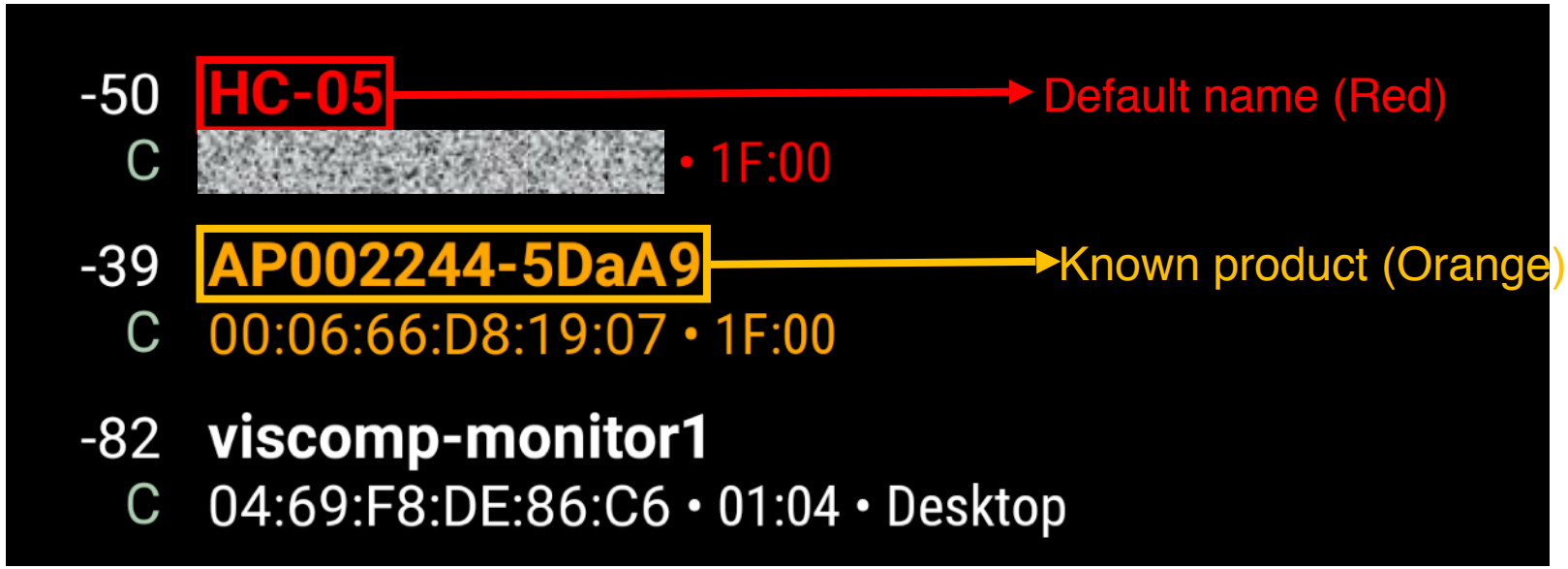
	1	2	
Module	**Class of Device**	**MAC Prefix**	**Device Name**
RN 41/42	Uncategorized	00:06:66	“RNBT-xxxx”
HC 05/06	Uncategorized	Various	“HC-05/06”



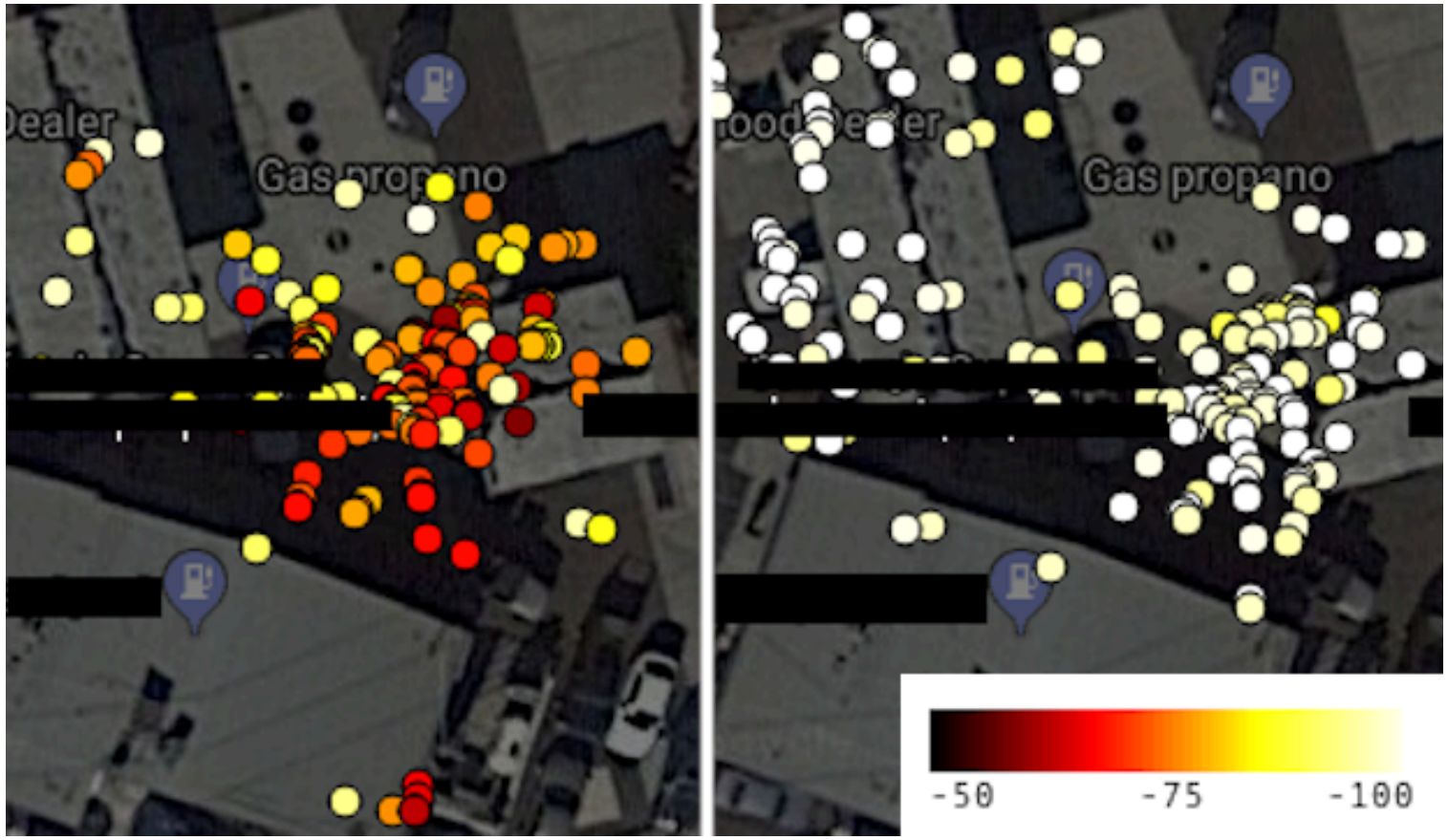
Indicating suspicious devices



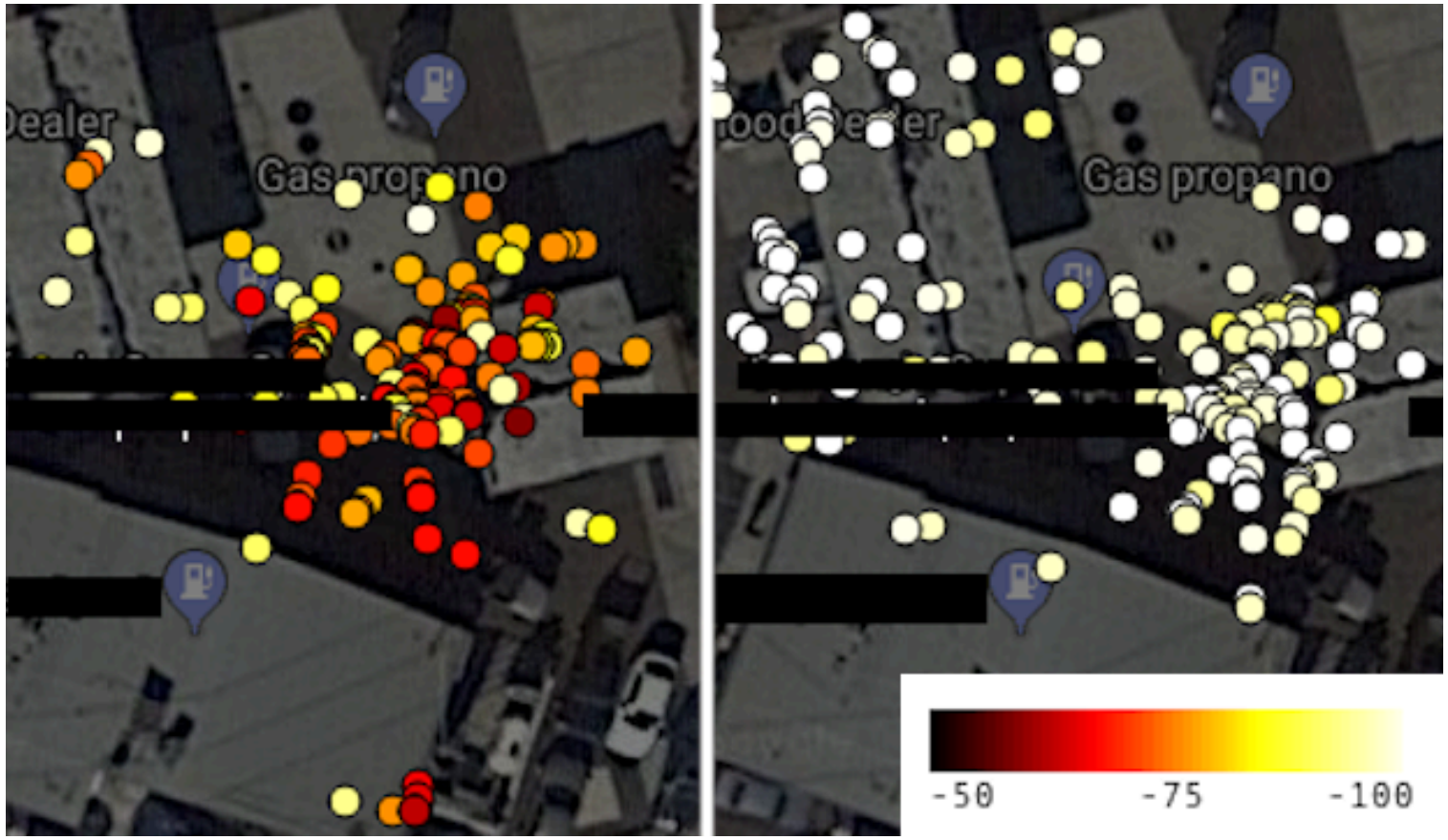
	1	2	3
Module	**Class of Device**	**MAC Prefix**	**Device Name**
RN 41/42	Uncategorized	00:06:66	“RNBT-xxxx”
HC 05/06	Uncategorized	Various	“HC-05/06”



Skimmers have strong signal only near pumps

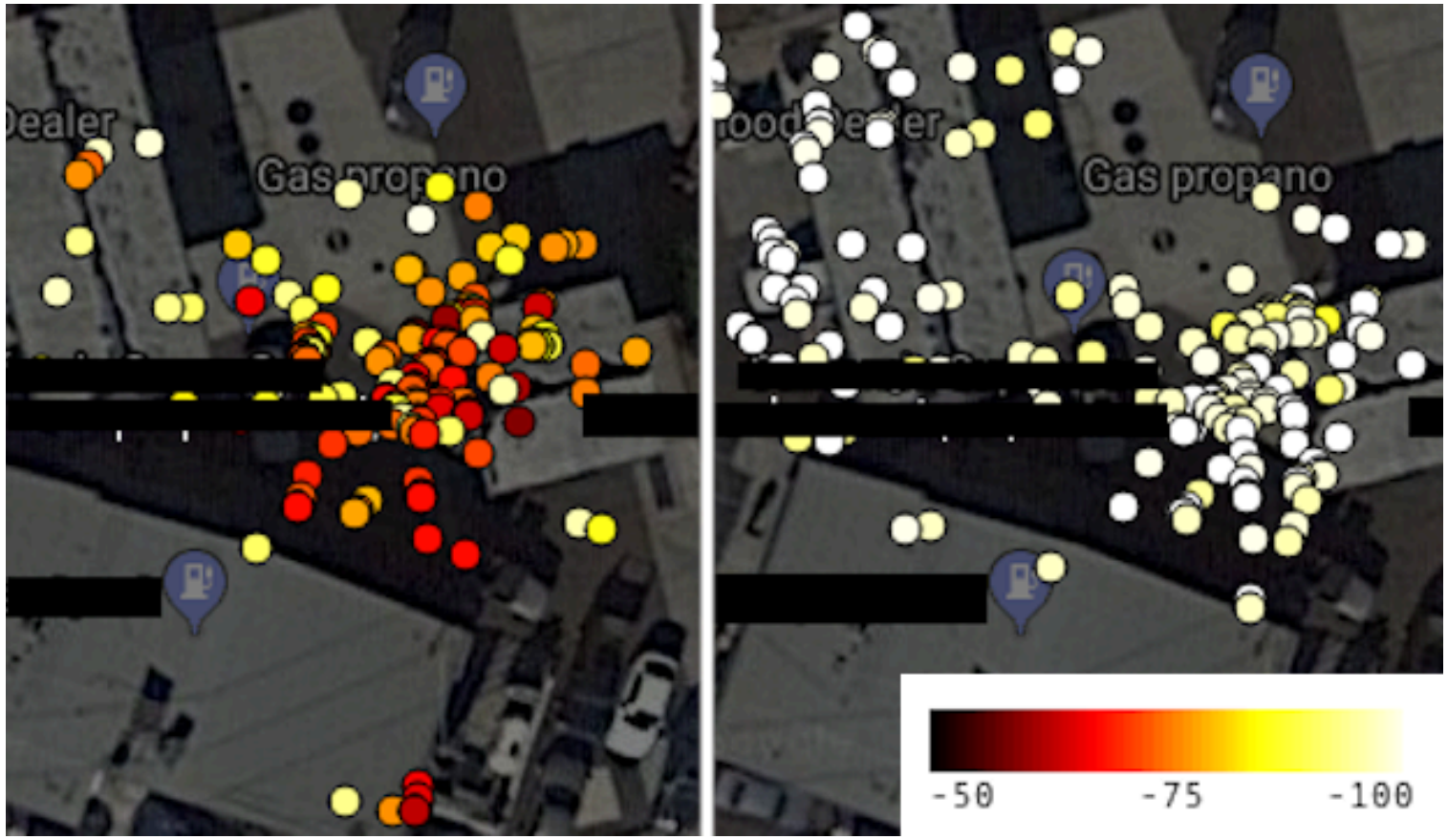


Skimmers have strong signal only near pumps



Likely a skimmer

Skimmers have strong signal only near pumps



Likely a skimmer

Not a skimmer

Overview of results

Scanned 1,185 gas stations in 6 states

64 skimmers detected in the wild by Bluetana and recovered by LE

- Also 23 skimmers received independently from LE

Our analysis

1. What do these skimmers look like in Bluetooth scans?
2. Are they distinguishable from other devices?

Device class

All 87 skimmers advertised an “Uncategorized” device class

Uncategorized is the default for all Bluetooth-to-serial modules

MAC prefixes (manufacturer)

Most skimmers use the "RN" Bluetooth module

- All RN modules have the same MAC prefix

MAC Prefix	#
00:06:66	57
98:D3:31	1
Unknown	28
Total	87

The HC modules have patterns in their MAC prefixes

- Manufacture date as first 4 bytes of MAC prefix

MAC prefixes (manufacturer)

Most skimmers use the "RN" Bluetooth module

- All RN modules have the same MAC prefix

MAC Prefix	#
00:06:66	57
98:D3:31	1
Unknown	28
Total	87

The HC modules have patterns in their MAC prefixes

- Manufacture date as first 4 bytes of MAC prefix

MAC prefixes (manufacturer)

Most skimmers use the "RN" Bluetooth module

- All RN modules have the same MAC prefix

MAC Prefix	#
00:06:66	57
98:D3:31	1
Unknown	28
Total	87

The HC modules have patterns in their MAC prefixes

- Manufacture date as first 4 bytes of MAC prefix

MAC prefixes (manufacturer)

Most skimmers use the "RN" Bluetooth module

- All RN modules have the same MAC prefix

MAC Prefix	#
00:06:66	57
98:D3:31	1
Unknown	28
Total	87

The HC modules have patterns in their MAC prefixes

- Manufacture date as first 4 bytes of MAC prefix

20:13:04:25
20:17:11:20
20:18:01:03
20:18:04:15
20:18:07:16

MAC prefixes (manufacturer)

Most skimmers use the "RN" Bluetooth module

- All RN modules have the same MAC prefix

MAC Prefix	#
00:06:66	57
98:D3:31	1
Unknown	28
Total	87

The HC modules have patterns in their MAC prefixes

- Manufacture date as first 4 bytes of MAC prefix

20:13	04	25
20:17	11	20
20:18	01	03
20:18	04	15
20:18	07	16

MAC prefixes (manufacturer)

Most skimmers use the "RN" Bluetooth module

- All RN modules have the same MAC prefix

MAC Prefix	#
00:06:66	57
98:D3:31	1
Unknown	28
Total	87

The HC modules have patterns in their MAC prefixes

- Manufacture date as first 4 bytes of MAC prefix

YY : YY :	MM :	DD
20:13	04	25
20:17	11	20
20:18	01	03
20:18	04	15
20:18	07	16

Device names

Most skimmers have default names

Sometimes skimmers have disguised names

- Failed attempt to make device look inconspicuous

Often device names are missing

- Device name obtained in subsequent packets

Device Name	#
Default	59
[Law Enforcement]	2
[Mobile Phone]	4
[Indescript Object]	2
[Numerical]	2
Unnamed	18
Total	87

Device names

Most skimmers have default names

Sometimes skimmers have disguised names

- Failed attempt to make device look inconspicuous

Often device names are missing

- Device name obtained in subsequent packets

Device Name	#
Default	59
[Law Enforcement]	2
[Mobile Phone]	4
[Indescript Object]	2
[Numerical]	2
Unnamed	18
Total	87

Device names

Most skimmers have default names

Sometimes skimmers have disguised names

- Failed attempt to make device look inconspicuous

Often device names are missing

- Device name obtained in subsequent packets

Device Name	#
Default	59
[Law Enforcement]	2
[Mobile Phone]	4
[Indescript Object]	2
[Numerical]	2
Unnamed	18
Total	87

Device names

Most skimmers have default names

Sometimes skimmers have disguised names

- Failed attempt to make device look inconspicuous

Often device names are missing

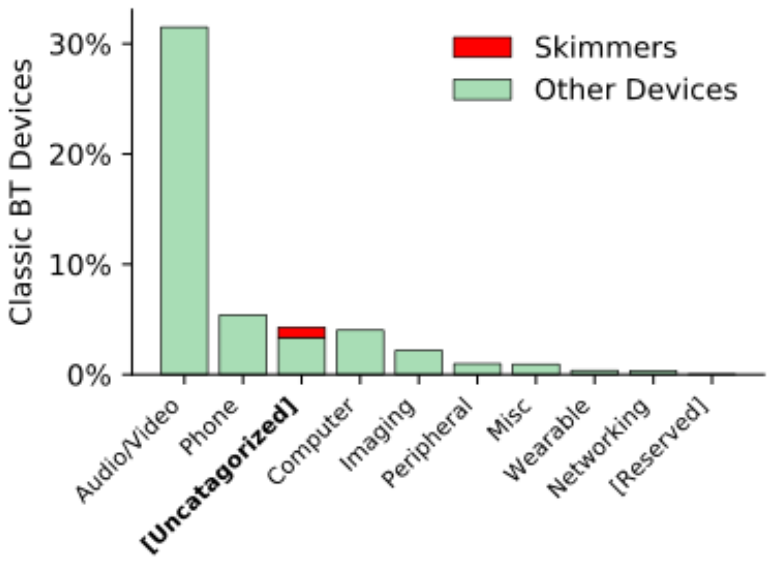
- Device name obtained in subsequent packets

Device Name	#
Default	59
[Law Enforcement]	2
[Mobile Phone]	4
[Indescript Object]	2
[Numerical]	2
Unnamed	18
Total	87

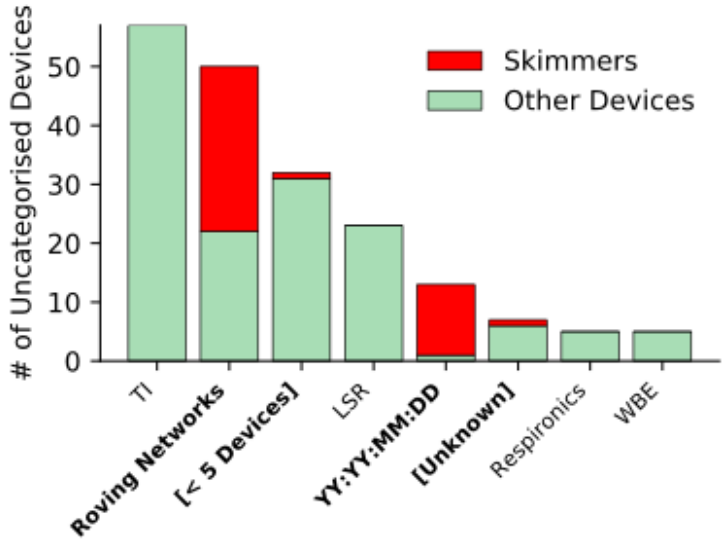
Are skimmers distinguishable from other devices?

Bluetooth devices: 2,562

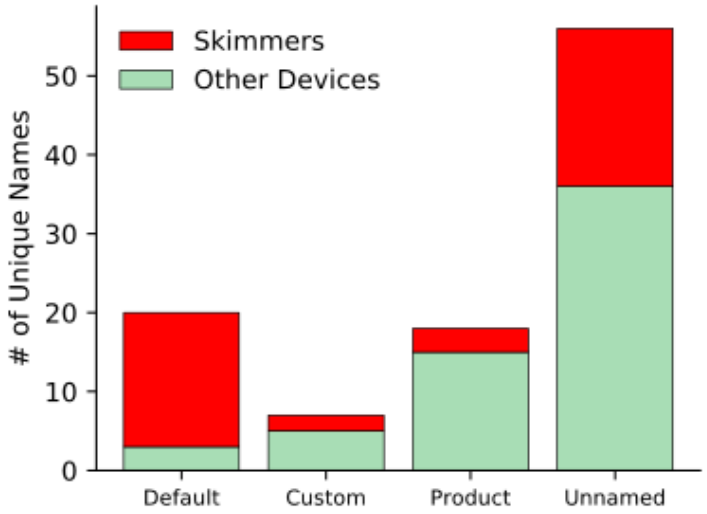
Skimmers: 42



Device class



Manufacturer
(MAC prefix)



Device name

Accuracy of Bluetooth-based detection

Missed skimmers: 36 skimmers detected, **only 6 missed**

Incorrectly detected skimmers: **Only 6%** out of 757 inspections

Countermeasures to Bluetooth-based detection

1. Switching to BLE (or another wireless protocol)

2. Non-discoverable Bluetooth mode

3. Impersonating benign devices

Lessons learned from the field: Criminal operations have close MAC addresses

	(a) Same county	(b) Different counties
Distance in MAC Address space	4	4
Distance between gas stations (miles)	17	448

Close MAC addresses likely originate from the same criminal entity

Lesson from the field: Drive-by inspections work

Highlighting suspicious devices triggered skimmer inspections

ARIZONA DEPARTMENT OF AGRICULTURE
WEIGHTS AND MEASURES SERVICES DIVISION
1688 W. Adams St., Phoenix, AZ 85007
Phone: 602-542-4373 or 1-800-277-6675 (Outside of Phoenix Metro)
Fax: 623-939-8586 State Ombudsman: 602-277-7292
Agency Contact: Damien DeSantiago 602-771-4948
https://agriculture.az.gov

INSPECTION COMMENTS/NOTES
A.R.S.41-1009(A)(7)
Page 2 of 2

DATE: [redacted] BMF: [redacted] INSPECTION: [redacted]

COMMENTS/NOTES

I [redacted] checked all pumps after Blutana was Red. I then searched all dispensers and found 1 skimmer on pump # 2. Skimmer was removed by [redacted] once removed from dispenser Blutana device search stopped being red . I placed the

ARIZONA DEPARTMENT OF WEIGHTS AND MEASURES
1688 W. Adams St. Phoenix, AZ 85007 https://dwm.az.gov
Phone: 602-771-4920 or 1-800-277-6675 (Outside of Phoenix Metro)
Agency contact: Damien DeSantiago (602) 771-4948
State Ombudsman 602-277-7292

INSPECTION COMMENTS /NOTES
A.R.S. §41-1009(A)(7)

BMF # [redacted] INSPECTION # [redacted] TEST DATE [redacted] PAGE 1 OF 1

COMMENTS / NOTES

While using the "Bluetana" scanner two items showed up in red. I opened a fueling device skimmer inspection then announced myself to location staff. The scanner showed the strongest signal to the dispensers closet to [redacted] In dispensers 1/2 and 5/6 I found skimmers installed. For a total

Lesson from the field: Drive-by inspections work

Highlighting suspicious devices triggered skimmer inspections

ARIZONA DEPARTMENT OF AGRICULTURE
WEIGHTS AND MEASURES SERVICES DIVISION
1688 W. Adams St., Phoenix, AZ 85007
Phone: 602-542-4373 or 1-800-277-6675 (Outside of Phoenix Metro)
Fax: 623-939-8586 State Ombudsman: 602-277-7292
Agency Contact: Damien DeSantiago 602-771-4948
https://agriculture.az.gov

INSPECTION COMMENTS/NOTES
A.R.S.41-1009(A)(7)
Page 2 of 2

DATE: [redacted] BMF: [redacted] INSPECTION: [redacted]

COMMENTS/NOTES

I [redacted] checked all pumps after Blutana was Red. I then searched all dispensers and found 1 skimmer on pump # 2. Skimmer was removed by [redacted] once removed from dispenser Blutana device search stopped being red . I placed the

ARIZONA DEPARTMENT OF WEIGHTS AND MEASURES
1688 W. Adams St. Phoenix, AZ 85007 https://dwm.az.gov
Phone: 602-771-4920 or 1-800-277-6675 (Outside of Phoenix Metro)
Agency contact: Damien DeSantiago (602) 771-4948
State Ombudsman 602-277-7292

INSPECTION COMMENTS /NOTES
A.R.S. §41-1009(A)(7)

BMF # [redacted] INSPECTION # [redacted] TEST DATE [redacted] PAGE 1 OF 1

COMMENTS / NOTES

While using the "Bluetana" scanner two items showed up in red. I opened a fueling device skimmer inspection then announced myself to location staff. The scanner showed the strongest signal to the dispensers closet to [redacted] In dispensers 1/2 and 5/6 I found skimmers installed. For a total

33 skimmers recovered only because Bluetana detected them

Conclusions

Skimming devices are detectible in the sea of legitimate Bluetooth devices

Bluetana allows inspectors to find skimmers **faster than manual inspections**

Criminal behaviors **make skimmers easier to find** (and may even indicate their source)

This problem is not going away any time soon **(we found six skimmers in the Bay Area last week)**

Source: Arizona Weights and Measures

Questions