

# **Wawa Breach Affects 30+ Million Payment Cards**

**Cyberint**

## Background

On Dec. 19, 2019, **Wawa**, a US-based chain of convenience stores and gas stations, sent a notice<sup>1</sup> to customers about the discovery of a point-of-sale (POS) compromise; Wawa discovered card-stealing malware installed on in-store payment processing systems and fuel dispensers at potentially all Wawa locations.

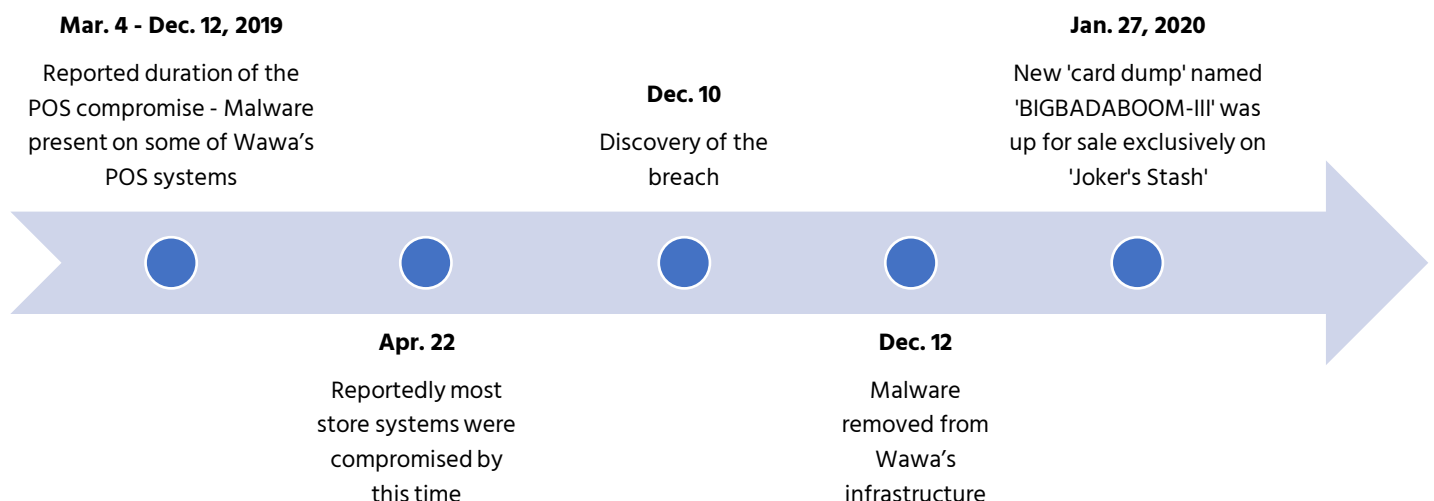


Wawa said the intrusion was discovered on Dec. 10 and contained the breach by Dec. 12. The malware was thought to have been installed more than nine months earlier, around Mar. 4.

The compromised data was card payment details as follows:

- Card holder name
- Account number
- Expiration date
- Additional validation data that could be used to create clone cards for fraudulent use.

On Jan. 27, 2020 the payment card details were put up for sale on Joker's Stash, an underground carding marketplace on the dark web. According to the post, the total amount of exposed data during the malware attack may sum up to more than 30 million debit and credit card records from the people buying in any of Wawa's 850 locations nationwide. The payment card dump was advertised under the name of BIGBADABOOM-III.



<sup>1</sup> <https://www.wawa.com/alerts/data-security>

## Cyberint Research Insights

### Joker's Stash

Joker's Stash is a dark web carding marketplace accessible via the use of blockchain DNS, a decentralized DNS service that requires the installation of a browser plugin to access non-standard top-level domains (TLD).


A decentralized DNS uses peer-to-peer networking to share lookup tables which contain the DNS data. This decentralized approach vs. a standard DNS<sup>2</sup>, allows the use of non-standard TLDs, such as '.bit', '.lib', '.emc', '.coin' and '.bazar', that will prevent censorship or takedown activity such as law enforcement agencies compelling ISPs to a sinkhole or to redirect illegal sites.

### BIGBADABOOM-III

Posted on Jan. 27, 2020, the BIGBADABOOM-III dump claims to include over 30 million track dumps predominantly from US-based victims. The post states that there may be 1 million details from different countries, likely belonging to travelers visiting the compromised retailer.

**Figure 1.** "BIGBADABOOM-III dump" post on Joker's Stash marketplace

2020-01-27  
Brand NEW Huge 30M+ pcs Nationwide "BIGBADABOOM-III" BREACH at JOKER's STASH!



**BIGBADABOOM-III BREACH at JOKER's STASH!**  
the most biggest breach for the last 5 years.

Brand NEW Huge **30M+ pcs** Nationwide Breach  
**30.000.000+** Perfect Pure Fresh TR2+TR1 Dumps  
**40+** US States  
**31.000+** Different Bins  
more than **1M pcs** of EU/ASIA/ARABS/EXOTIC bins (100+ Different Countries)

**BIGBADABOOM-III-EU-part1 (BBB3 BREACH) : EU/ASIA/WORLD TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27  
**BIGBADABOOM-III-US-part1 (BBB3 BREACH) : USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27  
**BIGBADABOOM-III-US-part2 (BBB3 BREACH) : USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27  
**BIGBADABOOM-III-US-part3 (BBB3 BREACH) : USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27

Be READY for the BIG-BADA-BOOM! Exclusively ONLY at JOKER's STASH!

<sup>2</sup> A standard DNS is used to lookup the server's IP address for the domain, typically by sending a request to your ISP's DNS server that in turn forwards the request to the DNS server that is authoritative for the domain in question



## Cyberint's Take

This massive point of sale (POS) malware breach demonstrates how the financially motivated threat actors target both online channels as well as the in-store systems in order to obtain payment data and monetize their haul by reselling it to individual fraudsters.

Typically, POS malware utilizes memory scraping techniques to gather unencrypted card details, in this case 'track 1' and 'track 2' data. This track data is read from the magnetic stripe on a physical card and includes the cardholder name, account number and expiration date amongst other validation data.

Subsequently, with the sale of this card data on a popular 'carding' marketplace, fraudsters are able to write the data back to a 'blank' card, effectively cloning the original and allowing physical fraudulent transactions to be made.

Even though reportedly 30 million credit card details may have been compromised, a significant amount of them could have already expired since the initial compromise in Mar. 2019. Other customers may have proactively deactivated their cards since Wawa's notice last December.

In order to prevent similar attacks and stay ahead of threat actors, companies should aim to leverage best practices for securing the POS endpoints, such as:

- Securing POS identity access,
- Biometrics security measures,
- Up-to-date software and antivirus,
- Alternative physical security mechanism.

As soon as more details on the malware become available, more insights and possibly threat hunting scenarios can be provided as steps for detection, compromise assessment and effective mitigation.

## Contact Information

### **ISRAEL**

Tel:+972-3-7286-777

17 Ha-Mefalsim St 4951447 Petah Tikva

### **UNITED KINGDOM**

Tel:+44-203-514-1515

Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

### **SINGAPORE**

Tel:+65-3163-5760

135 Cecil St. #10-01 MYP PLAZA 069536

### **USA**

Tel:+1-646-568-7813

214 W 29th St, 2nd Floor New York, NY 10001

### **LATAM**

Tel:+507-395-1553

Panama City

---

## **Cyberint.**