

VENDETTA BROTHERS, INC.

A WINDOW INTO THE BUSINESS OF THE CYBERCRIMINAL UNDERGROUND

CONTENTS

Introduction	1
Key Findings	2
Vendetta World	3
Going International—Geographical Targeting Patterns	4
Market Diversification—Multiple Sources of Stolen Payment Data	5
Option 1: Outsource the Grunt Work	5
Option 2: If You Want Something Done Right—Do It Yourself	6
Option 2A: CenterPOS	6
Option 3: Straight to the Source—Physical Skimming Operations	7
Customer Dispute Resolution	8
Cybercrime That's Organized	9



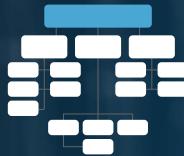
INTRODUCTION

An enterprising duo of cybercriminals we call the “Vendetta Brothers” use various strategies to compromise point-of-sale (POS) systems, steal payment card information and sell it on their underground marketplace “Vendetta World.”

Using the monikers “1nsider” and “p0s3id0n,” we have observed the pair using practices more commonly seen in legitimate business, including outsourcing, partnerships, diversifying their market, and insulating liability. The Vendetta Brothers have so far focused on credit card data belonging to users in the United States and several Nordic countries. We believe they operate from Spain and Eastern Europe.

The Vendetta Brothers frequently partner with other cybercriminals access to POS systems to deliver malware or to provide skimming hardware that captures payment information. They likely use these partnerships to outsource and insulate themselves from many of the more tedious and lower-margin tasks of locating, identifying, and sometimes exploiting target payment systems. This approach provides the duo with both increased profit margins by accessing a more diverse array of payment systems and improved security by using recruited proxy partners to mitigate risk and potentially frustrate investigators. Their operations may indicate improved creativity in the cybercriminal world in response to more frequent exposure.

KEY FINDINGS



A pair of cybercriminals we call the "Vendetta Brothers" use practices more commonly seen in legitimate business to steal payment card data from POS systems.



The group uses outsourcing and partnerships with other criminals to diversify their targeting and insulate themselves from culpability.



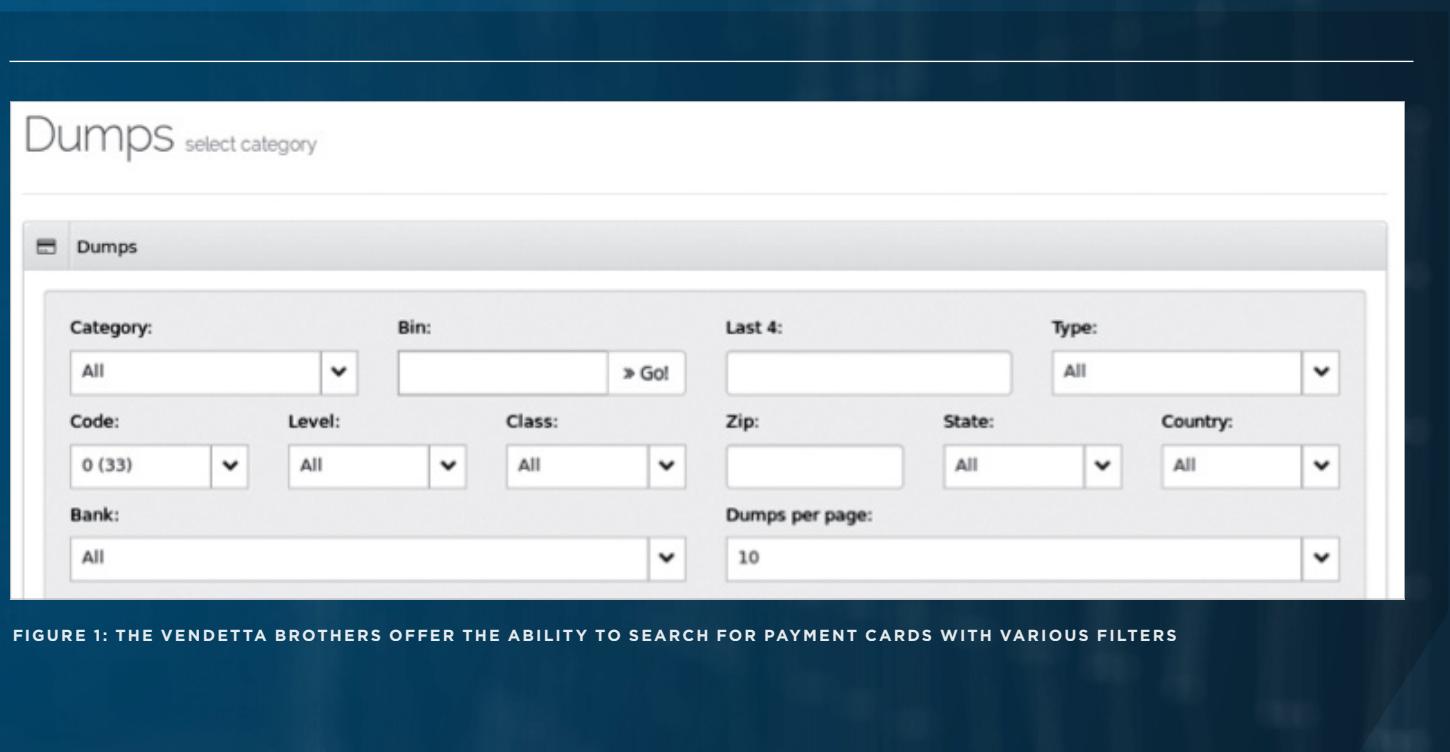
The Vendetta Brothers typically target victims in the U.S. and Nordic countries, using a variety of techniques ranging from phishing to installing physical skimmers.



We may see criminal groups use more advanced techniques in order to scale their operations in the face of more frequent exposure.

VENDETTA WORLD

The Vendetta Brothers dump shop is an e-commerce website that sells stolen payment card information. Cybercriminal customers can search for payment cards from specific banks or geographical regions, as shown in Figure 1. The Vendetta World marketplace contains roughly 9,400 cards for sale, making it a relatively small operation compared to other cybercriminal groups we track.



The screenshot shows a web page titled 'Dumps select category'. At the top, there is a navigation bar with a 'Dumps' tab selected. Below the navigation bar is a search and filter section. The filters include:

- Category:** A dropdown menu set to 'All'.
- Bin:** A text input field with a '» Go!' button.
- Last 4:** A text input field.
- Type:** A dropdown menu set to 'All'.
- Code:** A dropdown menu set to '0 (33)'.
- Level:** A dropdown menu set to 'All'.
- Class:** A dropdown menu set to 'All'.
- Zip:** A text input field.
- State:** A dropdown menu set to 'All'.
- Country:** A dropdown menu set to 'All'.
- Bank:** A dropdown menu set to 'All'.
- Dumps per page:** A dropdown menu set to '10'.

FIGURE 1: THE VENDETTA BROTHERS OFFER THE ABILITY TO SEARCH FOR PAYMENT CARDS WITH VARIOUS FILTERS



GOING INTERNATIONAL

Geographical Targeting Patterns

In early 2016, the Vendetta World shop contained more than 9,400 payment cards with more than 2,000 bank identification numbers from 639 banks in 40 countries, as shown in Figure 2. The top five countries were:

- United States
- Sweden
- Norway
- Finland
- Denmark

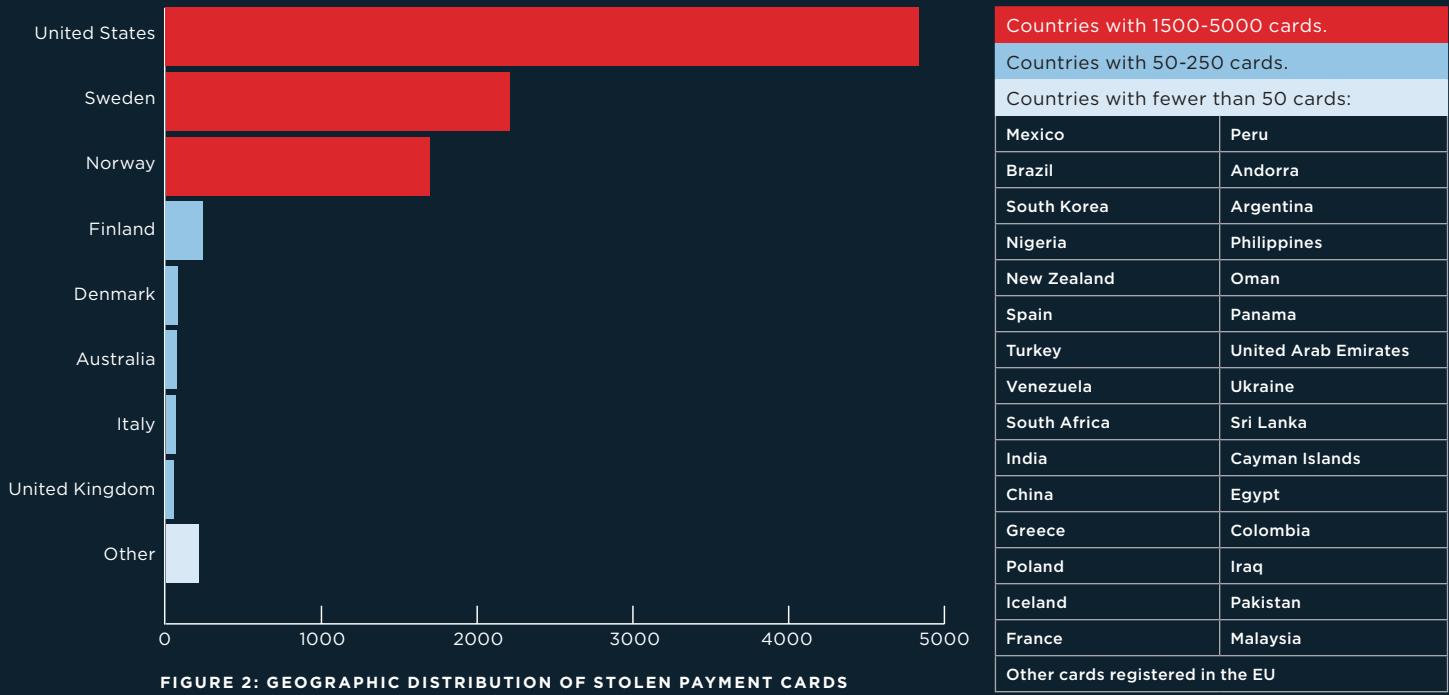


FIGURE 2: GEOGRAPHIC DISTRIBUTION OF STOLEN PAYMENT CARDS

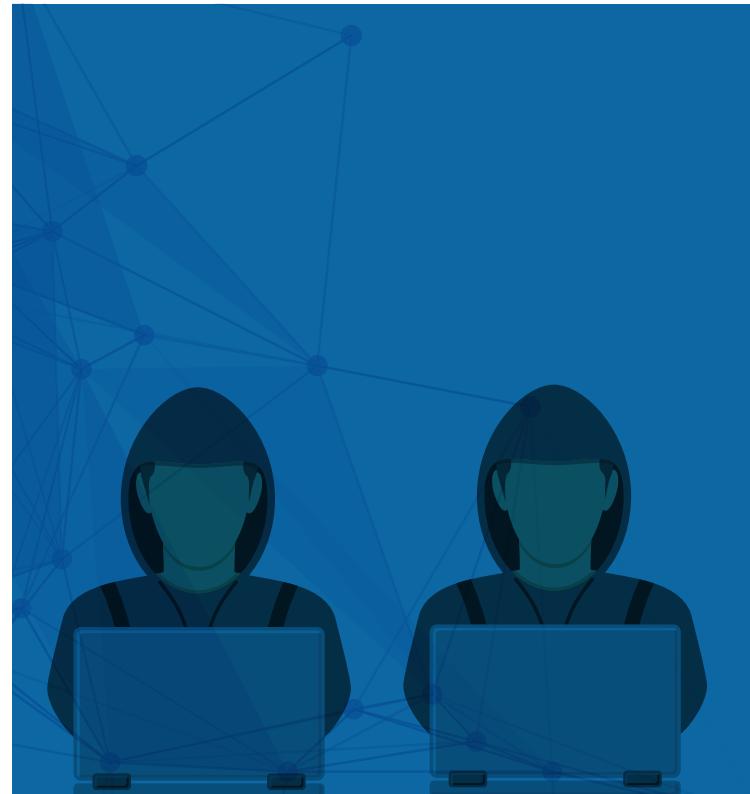
MARKET DIVERSIFICATION

Multiple Sources of Stolen Payment Data

The Vendetta Brothers diversify their sources of payment card data by implementing the following business practices:

- **Option 1—Outsourcing:** Partnering with cybercriminals who already have unilaterally-gained remote access to POS terminals.
- **Option 2—Purchasing Leads:** Spamming services to send phishing emails with Word document attachments that download an executable payload.
- **Option 3—Brick & Mortar:** Deploying physical skimmers with video cameras to capture payment card data as well as the PIN.

The Vendetta Brothers' diversification of stolen data sources may allow them to balance the benefits and risks of their operations, like modern businesses. Each of these mechanisms for stealing payment card information carries with it various tradeoffs, and may be implemented according to how difficult or profitable the Vendetta Brothers believe the operation to be. Rather than relying on a single method, these criminals have diversified their capabilities to respond to discovery, attribution, or remediation.



OPTION 1: OUTSOURCE THE GRUNT WORK

Similar to the way the technology industry outsources various lower-margin aspects of its business, the Vendetta Brothers actively search for partnerships with other cybercriminals on underground forums. They specifically seek out criminals who have already gained access to POS terminals, but who may not have POS malware or the skills required to use it. By using partnerships, the Vendetta Brothers can pass the tedious work of identifying and compromising vulnerable systems on to someone else. Figure 3 shows an advertisement to share profits with anyone able to provide access to a target POS. This tactic helps them focus on deploying the malware and reaping the rewards of stolen payment card information.

👉 PRIVATE POS MALWARE OWNERS - Looking for partners to work on 50% - 50% basis!

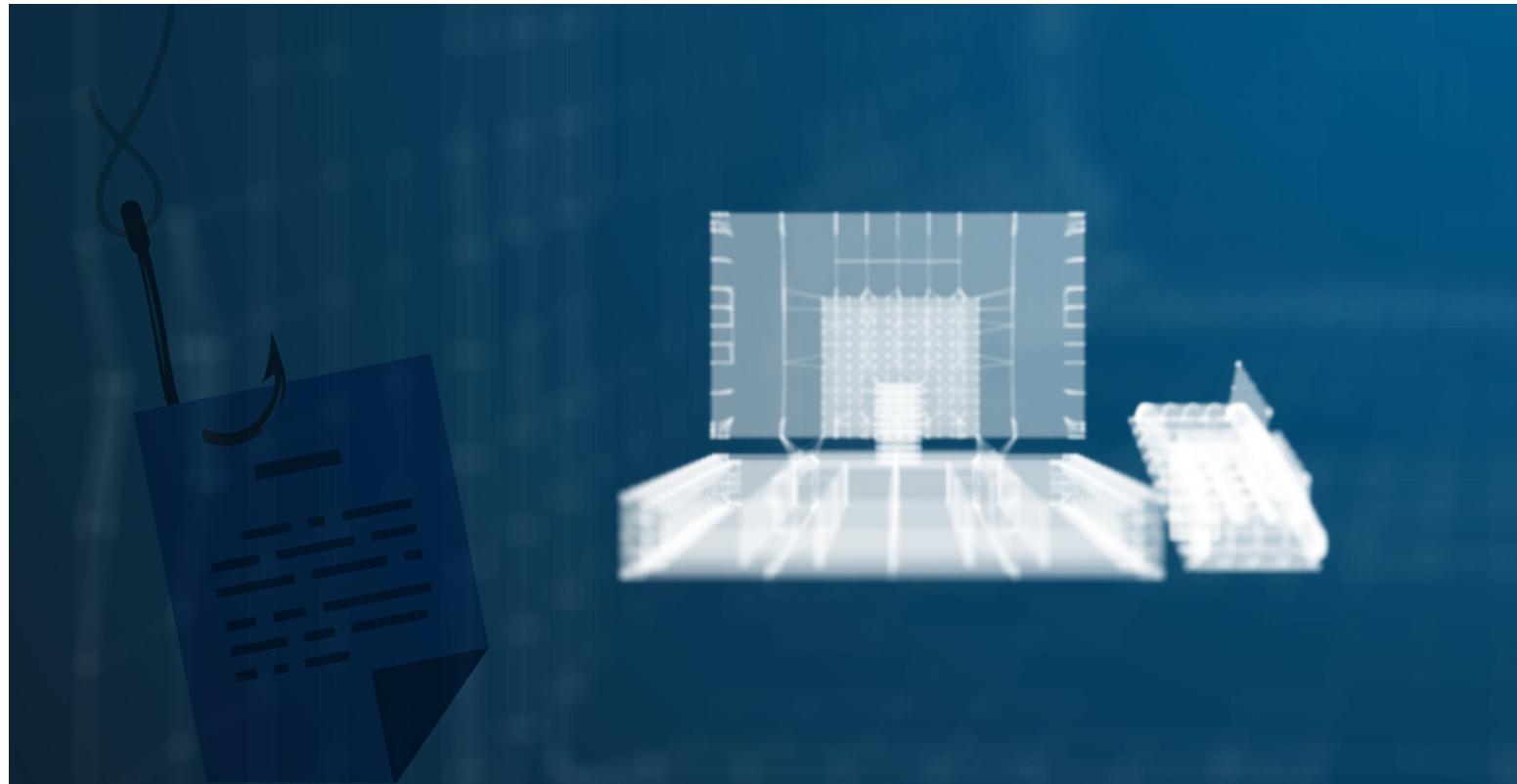
HELLO Dear Fraudsters!

We own PRIVATE P.O.S. MALWARE for dumps grabbing - TRACK 1+2.
We are looking for people that are able to :
*install our malware in shops (cashiers).
*have RDP's / VNC's that we can infect virtually.

So how do we do this? If you have the possibility to infect POS machines in shops we will send you a file that you have to install in POS machine or, if you own a RDP, VNC, PCA, Logmein etc. that is a POS contact us by ICQ or JABBER and we will infect it.

For people that have more than 10 POS'es we are offering panel* (username + password, bulletproof hosting) to see every single track that is coming!
For people that have less than 10 POS'es we are offering logs to see the number of tracks!

FIGURE 3: VENDETTA BROTHERS ADVERTISEMENT FOR PARTNERS



OPTION 2: IF YOU WANT SOMETHING DONE RIGHT, DO IT YOURSELF

The Vendetta Brothers sometimes compromise systems on their own using spam campaigns, possibly leveraging leads provided by their criminal partners. The pair send employment inquiry email messages with attached Word document resumes. Once opened, the Word document uses a malicious macro that downloads and runs “Beta Bot”—an executable available since 2013—from a staging server. Beta Bot then calls out to a set of three command and control (C2) servers to download two more pieces of malware.

The first contains two files, one of which is a version of the legitimate utility PsExec that allows a user to execute commands on a remote computer. The second file is configured to allow Beta Bot to spread laterally to other systems on the POS network. These capabilities allow the Beta Bot malware to spread beyond the initial point of infection, greatly increasing the damage it can cause. The other piece of malware is VendettaPOS, a memory scraper that searches POS system memory for Track 1 and Track 2 payment card data. VendettaPOS shares 98 percent of its code with DEXTER malware samples FireEye has analyzed.

OPTION 2A: CENTERPOS

The VendettaPOS C2 infrastructure shows considerable overlap with that of the “Vendetta World” dump shop. Further investigation revealed a web administration panel for a separate malware family known as “CenterPOS.” CenterPOS is another memory scraper that sends extracted payment card information back to a C2 server. Figure 4 shows a CenterPOS Administration panel.

FIGURE 4: CENTERPOS ADMINISTRATION PANEL



OPTION 3: STRAIGHT TO THE SOURCE— PHYSICAL SKIMMING OPERATIONS

In addition to using malware to steal payment card information from POS system memory, the Vendetta Brothers also use skimmers to capture data. In a skimming operation, criminals typically tamper with a POS device or terminal and install hardware that captures payment card information as the card is swiped or as it interfaces with a chip embedded in the card. The Vendetta Brothers claim they capture the PIN via video recording. Figure 5 shows one of the Vendetta Brothers' advertisements for skimming operations.

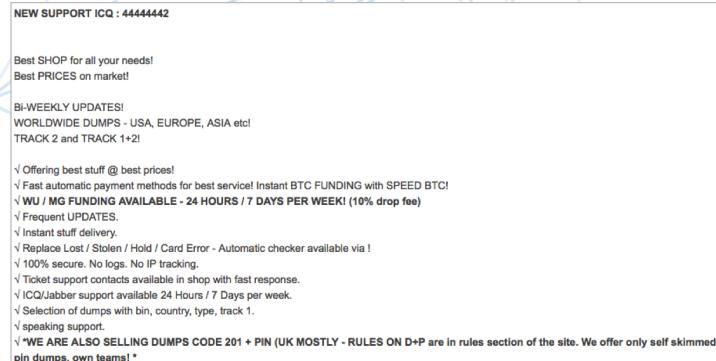


FIGURE 5: ADVERTISEMENT FOR SKIMMING OPERATIONS

CUSTOMER DISPUTE RESOLUTION

As with legitimate and illegitimate businesses alike, product quality is extremely important to success. We observed the Vendetta Brothers respond to a challenge to the viability of their collected payment card data by a putative buyer. Figure 6 (represented without handle information) shows a chat log snippet where one of the Vendetta Brothers' customers threatens to release data to krebsonsecurity.com, a popular security blog curated by Brian Krebs. This example helps reinforce the fact that, even in the cybercriminal underground, humans are still caught up in disputes about product quality.

(2:41:51 PM) **LIBAN:** I will forward all your data everyone will start from the <http://krebsonsecurity.com/>
(2:42:02 PM) **LIBAN:** I swear to god
(2:42:08 PM) **LIBAN:** bye now
(2:42:32 PM) **p0s3id0n:** bye
(2:42:33 PM) **p0s3id0n:** lamer



FIGURE 6: THREATENING TO GO TO BRIAN KREBS FOR DISPUTE RESOLUTION



CYBERCRIME THAT'S ORGANIZED

Observing the Vendetta Brothers' tactics has revealed a business-like approach to their crime operations that allows them to boost profits through expanded targeting, partnerships and diversification. By keeping various aspects of the scheme separate, the pair's operations might only be disrupted to the extent to which the discovered partner was involved.

Outsourcing some aspects of their operation may frustrate a law enforcement investigation. Separating leaders from individuals searching for systems to compromise or purchasing spam email services for malware distribution means law enforcement may be more likely to catch the partner, rather than the Vendetta Brothers. Similar to organized crime in the physical

world, cybercriminals can use partners and intermediaries to carry out certain aspects of their scheme while obfuscating the organizers' role.

Despite the Vendetta Brothers' relatively small operation, they nonetheless emulate proven practices from both business that indicate thoughtful planning on how to maximize profit and minimize risk.



To download this or other
FireEye iSight Intelligence reports,
visit: www.fireeye.com/reports.html

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc.
All other brands, products, or service names are or may be trademarks
or service marks of their respective owners.

