vmware® Carbon Black

HOLIDAY SEASON CYBER HEISTS

20 leading CISOs from the retail industry offer their perspective on evolving cyberattacks

JASON MADEY, SECURITY STRATEGIST, VMWARE CARBON BLACK

DECEMBER 2019

Executive Summary

'Tis the season for cyberattacks, particularly when it comes to the retail industry.

According to the VMware Carbon Black Threat Analysis Unit (TAU), retail organizations may see a noticeable spike in attempted cyberattacks during the holiday season.

TAU's analysis across VMware Carbon Black's global endpoint footprint reveals that global retail organizations encountered a 20% increase in attempted cyberattacks during the 2018 holiday shopping season, continuing a trend we've been tracking since 2016.

In conjunction with TAU's dissection of attack data, VMware Carbon Black conducted a survey measuring feedback from 20 leading CISOs from global retailers to determine how cyberattacks are evolving, how these CISOs view the threat landscape and what's being done to stem the tide.

Of note from the survey, 73% of retail organizations said they've seen an increase in cyberattack sophistication over the past year, with 33% of these organizations saying they've experienced an island-hopping attack over the same time period.

And these attacks are potentially harming more than just brand reputation. 40% of surveyed retail organizations said they've lost revenue in 2019 as a result of a cyberattack.

As VMware Carbon Black has noted in previous vertical-specific reports, the dark web continues to compound the attack landscape. Underground providers are offering listings that could affect consumers and retailers including: credit-card skimming guides, counterfeit credit cards, financial-specific malware, and access to specific bank accounts via stolen credentials.

According to our survey, retail CISOs are combating these trends with increased headcount, budgets and, in some cases, the implementation of threat hunting teams. The following report presents the highlights of our latest research and includes specific recommendations for how retailers can enjoy a happy holiday season.

Key Report Findings

Attempted cyberattacks against retail organizations may increase by 20% this holiday shopping season, according to VMware Carbon Black attack data

73% of surveyed retail organizations said they've seen an increase in cyberattack sophistication over the past year

40% of surveyed retail organizations said they've lost revenue as a result of a cyberattack in 2019

Two-thirds (66%) of surveyed retail organizations said they've experienced a ransomware attack over the past year

Kryptik, Emotet and Obfuse were the most prevalent malware families targeting the retail sector over the past year, according to VMware Carbon Black attack data (Of note, Emotet could be found in about 1 out of 5 retail organizations in 2019.)

33% of surveyed retail organizations said they've **encountered an island-hopping attack** in 2019

More than half (53%) of surveyed retail organizations said they **plan on increasing cybersecurity staff in 2020.** 40% said they plan to increase security budget by at least 10% in 2020

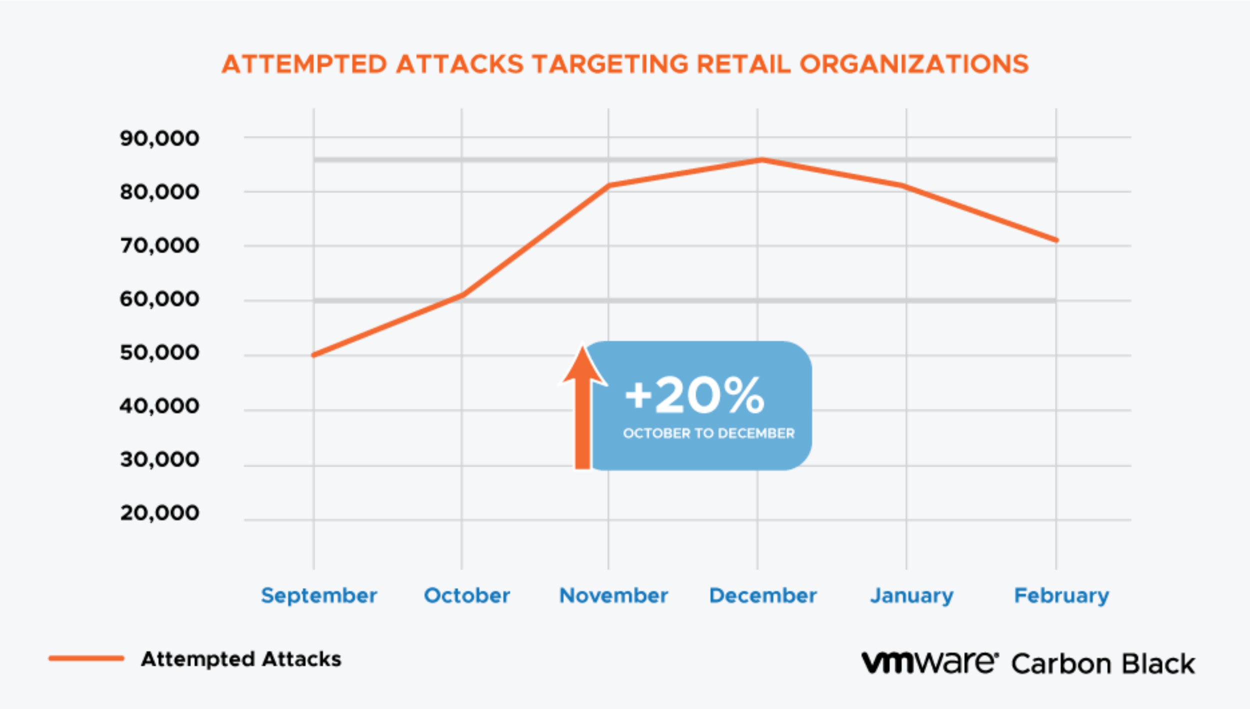
33% of surveyed retail organizations **currently have a threat hunting team**

The dark web currently has listings for retail-related information including: **credit-card skimming guides, counterfeit credit cards, financial-specific malware, and access to specific bank accounts via stolen credentials.**

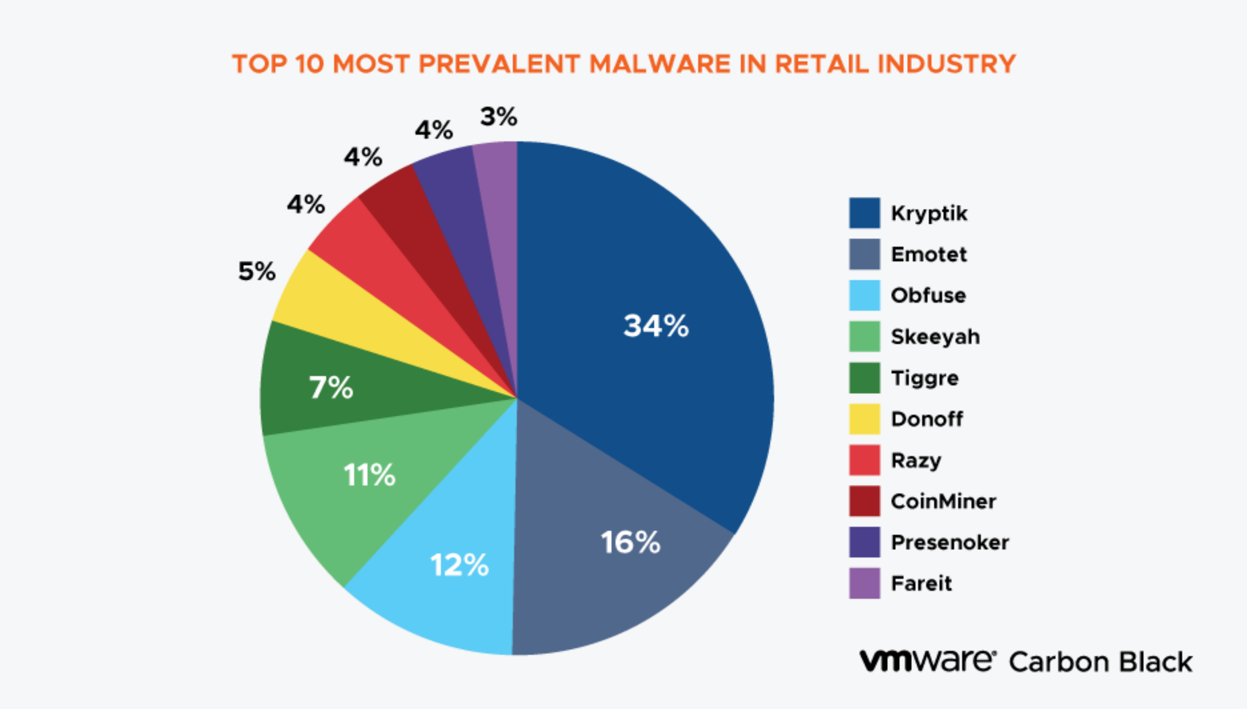
Attack Frequency & Types

According to the VMware Carbon Black Threat Analysis Unit (TAU), retail organizations may see a noticeable spike in potential cyberattacks during the holiday season.

TAU's analysis across VMware Carbon Black's global endpoint footprint reveals that global retail organizations encountered an approximate 20% increase in attempted cyberattacks during the 2018 holiday shopping season, continuing a trend we've been tracking since 2016. In our 2018 report, reflecting the 2017 holiday season, there was a 20.5% increase. "Attempted cyberattack" in the context of this discussion is an actionable alert identified by the threat research team.



Kryptik, Emotet and Obfuse were the most prevalent malware families targeting the retail sector over the past year, according to VMware Carbon Black attack data. (Of note, Emotet could be found in about 1 out of 5 retail organizations in 2019.)



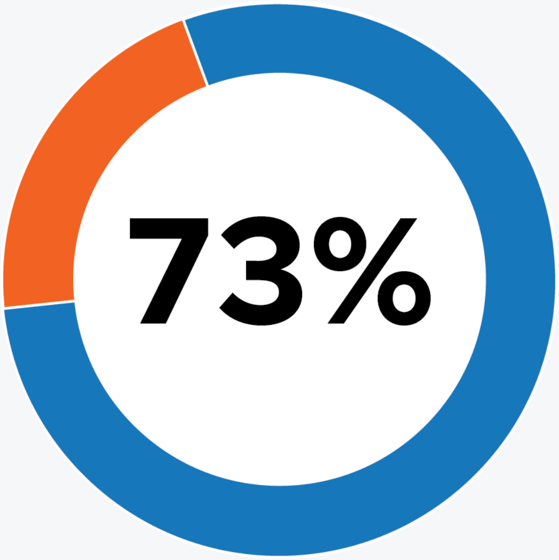
Emotet typically arrives via a malicious email mimicking a legitimate email coming from known contacts. The email contains a malicious file presented as a shipping notification, a past-due invoice or another item requiring urgent action. When the victim opens the file, malicious macros download the Emotet malware.

Once downloaded, Emotet establishes persistence (and typically installs ransomware and banking Trojans). At the same time, it attempts to propagate on local networks through incorporated spreader modules.

Looking for more information on Emotet?
Visit our collaborative threat report with eSentire from earlier this year.

Attack Sophistication

73% of surveyed retail organizations said they've seen an increase in cyberattack sophistication over the past year. This sophistication is taking multiple forms including: destructive attacks (reported by 20% of retail organizations in our survey); island hopping (reported by 33% of retail organizations in our survey) and counter incident response (reported by 25% of retail organizations in our survey).



of retail organizations reported seeing increased attack sophistication this year

vmware Carbon Black

More on Island Hopping

Island hopping is typically propagated via three methods:

- **Network attacks**
- **Watering-hole attacks**
- **Reverse business email compromise (BEC)**

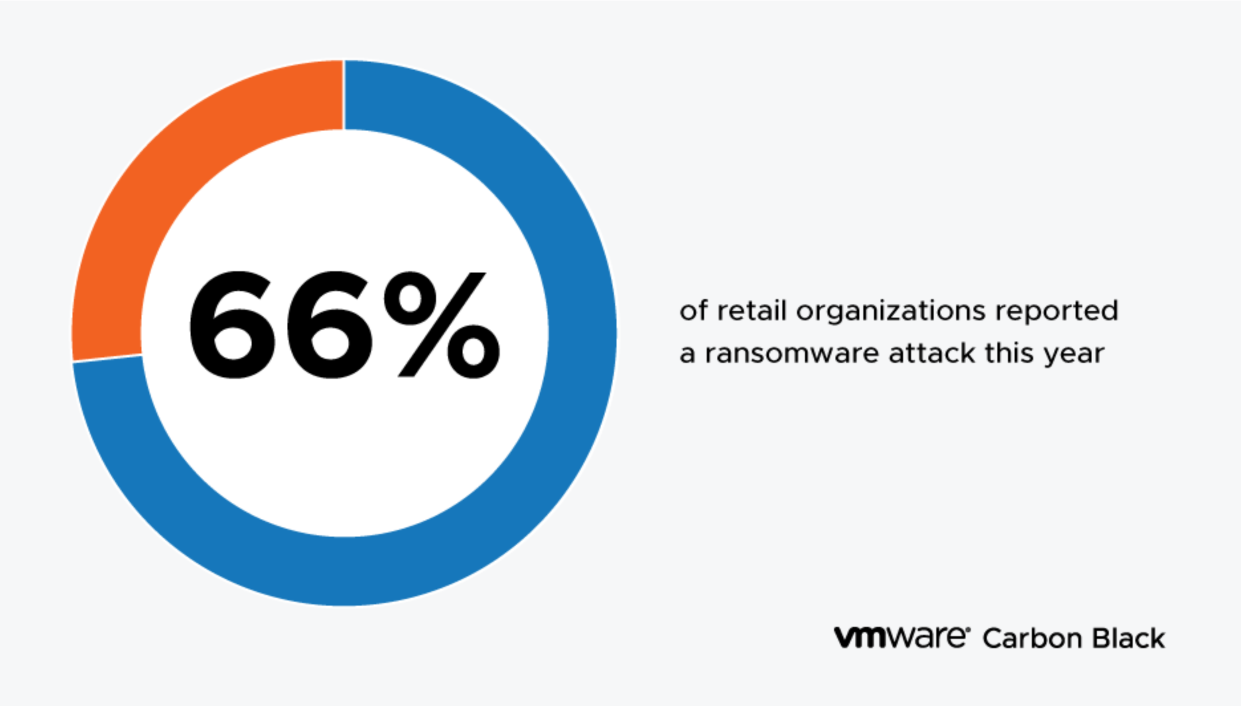
Island hopping attacks come from a wide variety of vantage points, whether it's through partner provisioned Virtual Desktop infrastructure (VDI) access, private network links and VPNs or by leveraging the compromise of partners to establish trust and perform trusted social engineering attacks. In the case of reverse BEC, a cybercriminal commandeers a mail server and then conducts whaling by sending email with fileless malware.

The end result of all of these attacks is the risk of a long-term hostage siege, with the attacker setting up command posts throughout the network. This method allows the cybercriminal to contaminate the hospital network turning the hospital's digital brand into patient zero. Frequent threat hunting is a critical requirement to identify and mitigate these transient and obfuscated points of presence.

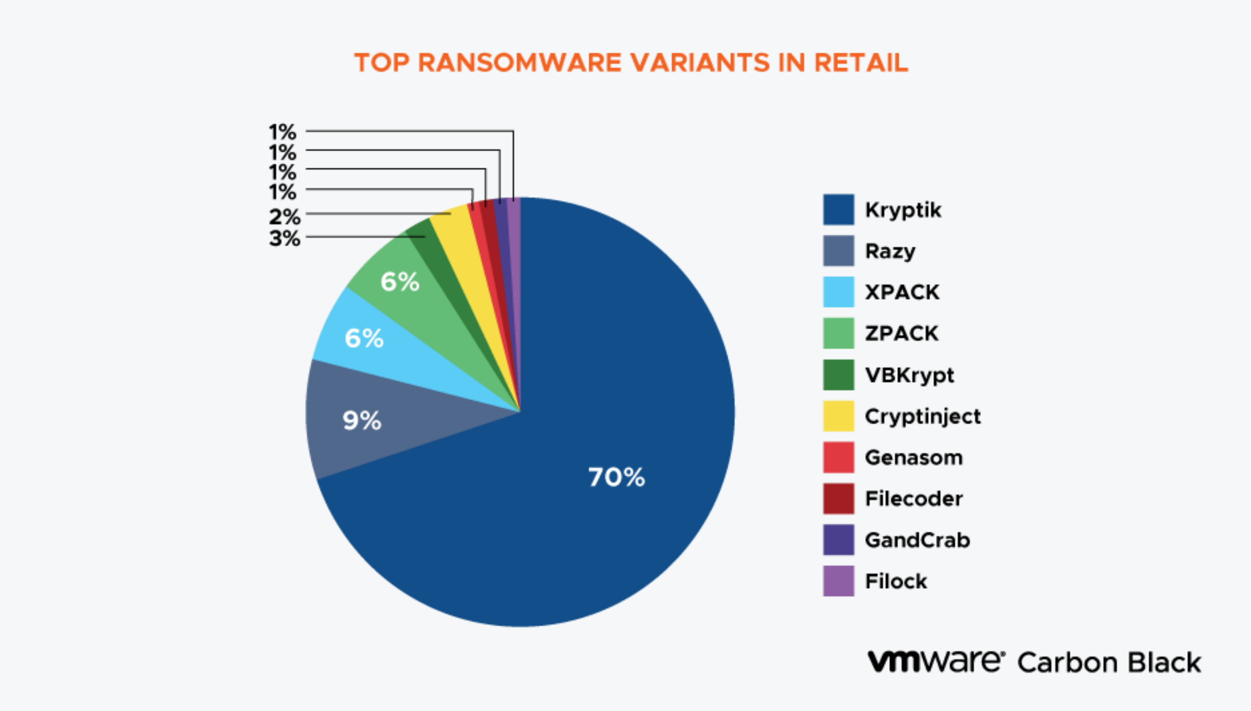
Ransomware

It's impossible to discuss cyberattacks in 2019 without discussing ransomware. Though the threat of ransomware has quieted down (at least publicly) since the days of WannaCry and NotPetya, the threat is still very real and retail is, unfortunately, not immune to the threat.

According to our survey, **two thirds (66%) of retail organizations** said their organization was targeted by a ransomware attack during the past year.



According to VMware Carbon Black's attack data, **Kyptik was the most prevalent ransomware** variant targeting VMware Carbon Black retail customers in 2019



About Kryptik

The Kryptik trojan attempts to target victim machines via nefarious installers. It then attempts to acquire admin rights to make registry modifications, allowing it to execute each time a Windows machine boots.

The Kryptik trojan can be very persistent and, without the appropriate visibility, can be difficult to detect as it attempts to delete its executable file after running.

As noted by a threat profile from the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC): "[The Kryptik trojan] queries the Windows registry for the .ini or .dat file paths. It also queries registry subkeys for the actual host, username, and password related to the specific FTP client application.

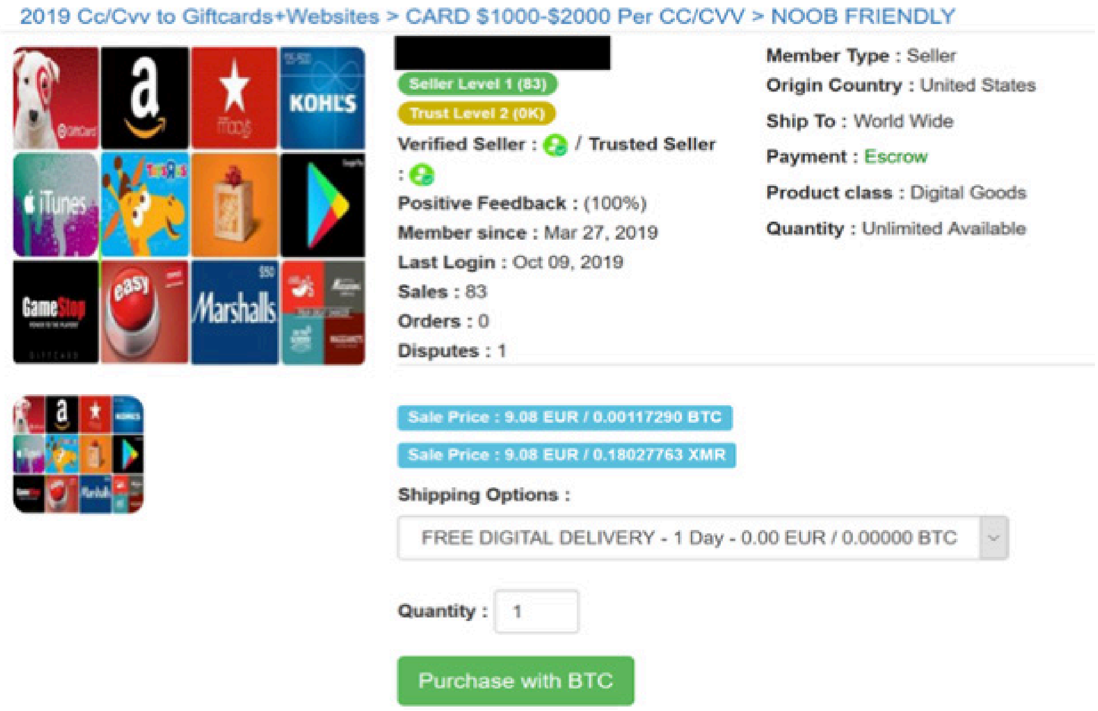
Kryptik searches the registry, querying for both ftpIniName and InstallDir that hold the wcx_ftp.ini file. The trojan can recover many common FTP clients, email clients, file browsers, and file manager programs. Kryptik also can update itself and remotely download new versions."

Kryptik was among the infections found in the notorious attack targeting the Ukrainian power grid in late 2015.

The Dark Web’s Role in Retail Cybercrime

Recent analysis of dark web offerings indicates that the attack surface for retailers can be quite wide. Among some of the listings currently available on the dark web that can affect consumers and retailers include:

1 **Credit Card Fraud and Skimming** - These continue to be of high interest on all dark web markets (other than those that exclusively sell drug-related items). Most listings are focused on selling guides to credit card skimming or instructions for what to do in order to cash out after the criminal has the credit card information. These listings are very low cost (most times less than $5) and may include out-of-date information. There are also listings for in-store carding guides - using counterfeit credit cards in order to obtain merchandise from stores. These listings were $5.50.



2019 Cc/Cvv to Giftcards+Websites > CARD $1000-$2000 Per CC/CVV > NOOB FRIENDLY

[redacted]

Seller Level 1 (83)

Trust Level 2 (0K)

Verified Seller : ✓ / Trusted Seller : ✓

Positive Feedback : (100%)

Member since : Mar 27, 2019

Last Login : Oct 09, 2019

Sales : 83

Orders : 0

Disputes : 1

Member Type : Seller

Origin Country : United States

Ship To : World Wide

Payment : Escrow

Product class : Digital Goods

Quantity : Unlimited Available

Sale Price : 9.08 EUR / 0.00117290 BTC

Sale Price : 9.08 EUR / 0.18027763 XMR

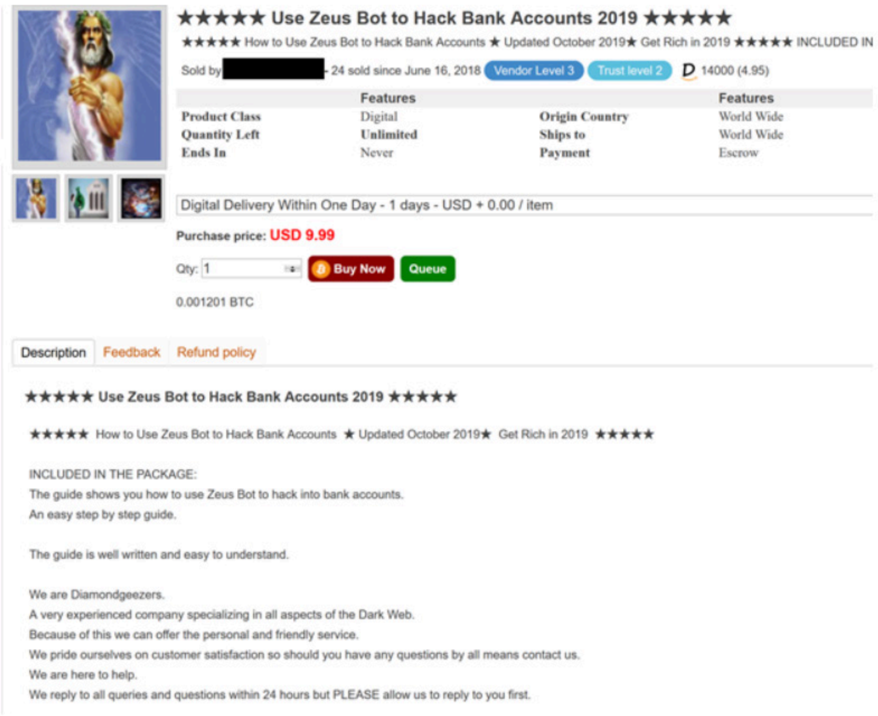
Shipping Options :

FREE DIGITAL DELIVERY - 1 Day - 0.00 EUR / 0.00000 BTC

Quantity : 1

2 **Financial-Specific Malware -** One such malware for sale is Cutlet Maker - a Trojan designed to attack a specific ATM brand and dispense all the ATM’s bills. It’s being offered on the dark web for $500. Additional research on Cutlet Maker indicates that other criminals figured out the way the Trojan worked and posted a key generator that would make it free to use. The offering on the marketplace did not indicate that this was a new or improved version of Cutlet Maker and could just be a way of ripping off other potential criminals, though.

Zeus is also making a resurgence on the dark web and is marketed as a resource for hacking bank information. The Center for Internet Security monthly malware activity report indicated that Zeus has been steadily in the top 10 list of malware active through much of 2019, and often is in the third or fourth position behind whatever malware is trending for the month.



★★★★★ Use Zeus Bot to Hack Bank Accounts 2019 ★★★★★

★★★★★ How to Use Zeus Bot to Hack Bank Accounts ★ Updated October 2019★ Get Rich in 2019 ★★★★★ INCLUDED IN

Sold by [redacted] - 24 sold since June 16, 2018 Vendor Level 3 Trust level 2 D 14000 (4.95)

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Digital Delivery Within One Day - 1 days - USD + 0.00 / item

Purchase price: USD 9.99

Qty: 1

0.001201 BTC

★★★★★ Use Zeus Bot to Hack Bank Accounts 2019 ★★★★★

★★★★★ How to Use Zeus Bot to Hack Bank Accounts ★ Updated October 2019★ Get Rich in 2019 ★★★★★

INCLUDED IN THE PACKAGE:
The guide shows you how to use Zeus Bot to hack into bank accounts.
An easy step by step guide.

The guide is well written and easy to understand.

We are Diamondgeezers.
A very experienced company specializing in all aspects of the Dark Web.
Because of this we can offer the personal and friendly service.
We pride ourselves on customer satisfaction so should you have any questions by all means contact us.
We are here to help.
We reply to all queries and questions within 24 hours but PLEASE allow us to reply to you first.

3

Account Access for Major Banks and Financial Institutions - These listings are offered at $150 to $270 per account. This price point suggests high quality accounts and includes information such as: name, address, DOB, bank name, routing number, checking account number, average monthly balance. One such offering insists that their offerings include accounts that have a “6 figure average balance” and that they are “perfect for bank account takeovers.” Other offerings are intended to be used to launder money and include terms such as “fresh and clean account,” “not hacked,” “allow Zelle to be used to cash out” and “may be used to withdraw from limited PayPal and other accounts.” These listings are often at a higher price point.

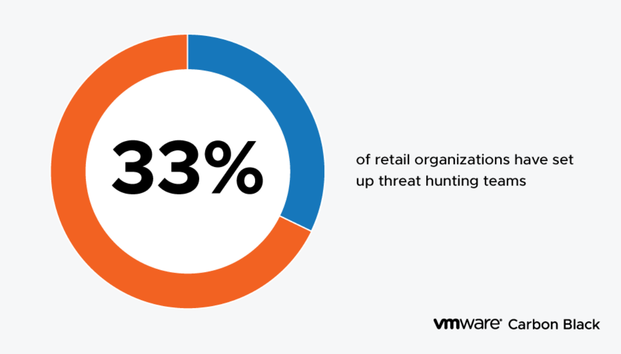
4 **Gift Card Fraud and Related Guides -** These can be found on nearly every dark web marketplace. They range in price from $0.50 to $3. Interestingly, criminals understand that there are efforts to reduce gift card fraud and include notes like "Carding them (gift cards) has gotten a little harder but is still easy if you have the right guide." These comments correlate to recent U.S. arrests for credit card fraud where the suspects used stolen credit card information to purchase gift cards, occasionally using the stolen credit card information encoded directly on other gift cards. The move from selling credit card information to selling "how to" guides suggests that the vendors are attempting to create multiple revenue streams in an already saturated market. Low cost guides are a good way to establish name recognition and maintain relevancy until more lucrative listings (e.g. credit card database dumps) are available.

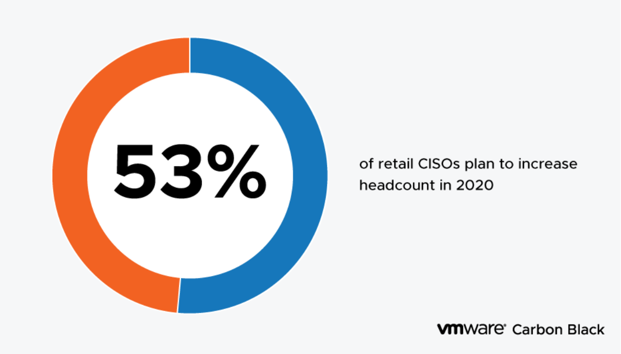
There are also offerings for gift cards at a fraction of the retail value of the card. This includes some airline gift cards in multiple increments from $250-$1,000 face value (the $1,000 value card is selling for $638).

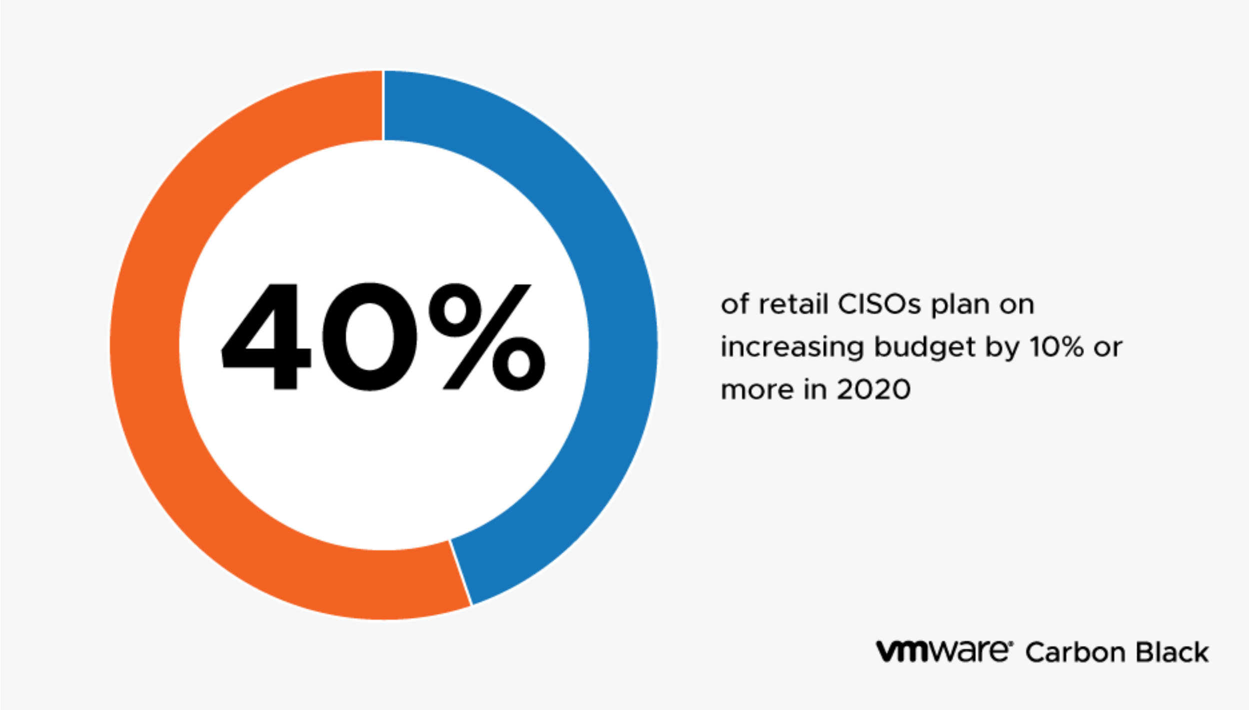
Conclusion & Recommendations

According to our survey, **40% of retail organizations said they've lost revenue** as a result of a cyberattack in 2019, a staggering number that may help CISOs earn more resources in an effort to help defend their organization's data and brand as well as customer data.

The good news from our survey is that more than half (53%) of surveyed retail organizations said they **plan on increasing cybersecurity staff in 2020**. And 40% said they plan to increase security budget by at least 10% in 2020. One-third of surveyed retail organizations **currently have a threat hunting team**, according to our survey.







of retail CISOs plan on increasing budget by 10% or more in 2020

Recommendations

1. **Deploy Threat Hunting Teams:** For retailers, this is increasingly important around the holiday season, when attempted attacks have historically spiked. The first step is making sure your team has visibility into what's happening in the environment. From there, baseline what's "normal" and empower team members to sniff out any anomalies. If the team is spending virtually all of its time responding to alerts, it can be pretty difficult to advance from a reactive position or even know where vulnerabilities exist.

2. **Leverage Data, Facts and Perceived Risk to Lobby for More Security Resources:** As a CISO, translating information security risk into business risk can help business leaders see investment in security as an investment in cost reduction. CISOs should work closely with company leaders to align overall business initiatives with cybersecurity goals. Get these leaders to understand that data is an asset, much like real estate, and that data is a currency that should be protected.

3. **Move Critical Assets to More Secure Compute Configurations Through Iron Boxing:** The first part of this process is to understand the organization's crown jewels and to develop a strategy for their protection. This information may be customer data, financial information, sensitive product or people data, or roadmaps for upcoming product launches. Many retailers have multiple access points to this data, so accounting for that total attack surface (including vendors and partners) will

be critical to long-term success. Application control technology is thought by many retailers to be one of the strongest forms of protection enabling the organization to meet strict regulatory demands and evolve the program to be focused on more than just compliance.

About VMware Carbon Black

VMware Carbon Black is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The VMware Carbon Black Cloud consolidates endpoint protection and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, VMware Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks.

More than 6,000 global customers, including approximately one third of the Fortune 100, trust VMware Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use VMware Carbon Black's technology in more than 500 breach investigations per year.