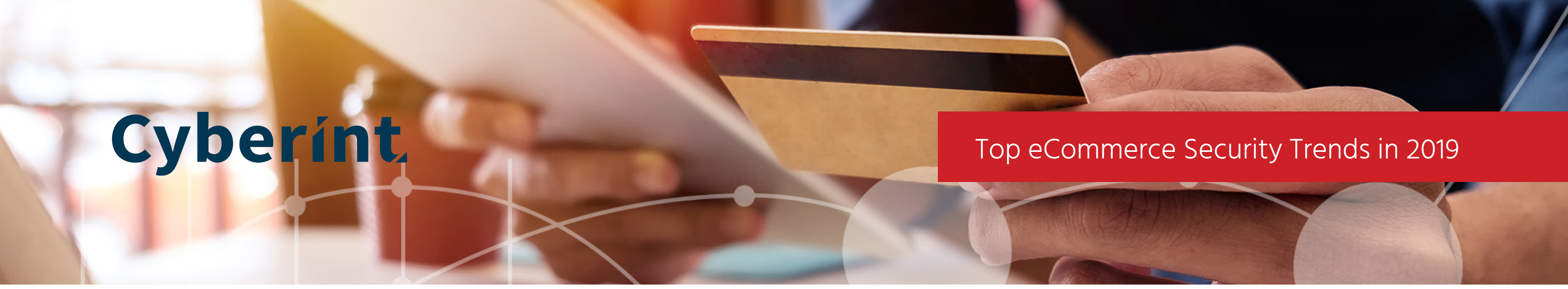
Cyberint

Top eCommerce Security Trends in 2019

Online retailers are lucrative targets for cyber attacks. Research shows that in 2018, retail crime cost retailers $777,877 for every $1 billion in sales. The 2019 Trustwave Global Security Report indicates the largest share of cyber incidents last year involved the retail industry. Threat actors are attacking from all sides, from eCommerce platforms to customer accounts. Moreover, there's been a noticeable shift away from attacks via ATM/gas pumps and Point of Sale systems (PoS), towards attacks against eCommerce applications.



Breaches can result in the theft of intellectual property or financial and customer data, and often cause serious financial losses and damage brand reputation. Retail organizations need to do more to protect themselves, which means protecting their customers, their employees, their business and their brand.

In order to effectively protect critical assets, companies should take a business threat-centric approach. This means that cybersecurity, much like IT, should protect customers along their shopping journey and the associated touchpoints, which are some favorite targets for attacks. Consumer face-to-face spending dropped 2.5% in February, a trend that reinforces the necessity for retailers to enhance the customer experience through multiple channels across digital channels - including 3rd party channels such as social media networks, 3rd party retail marketplaces and more.

Providing customers with more ways to interact with your business, however, also means more opportunities for threat actors to exploit the processes and procedures in place.

■ RISING SOPHISTICATION IN ADVERSARY TTPS

Cybercrime has seen an increase in more sophisticated tactics, techniques, and procedures (TTP) by organized cybercriminal gangs. Moving on from simple 'smash and grab' attacks, cybercriminals are now using tactics similar to ones used by nation-state threat actors.

The 'low and slow' attack is used to gain persistent access to a compromised organization where the data is exfiltrated over a long period of time, which results in an increased time-to-detection of weeks, months, or even years. The following attacks are some of the methods currently favored by cybercriminals.

■ THREATS ON THE RISE

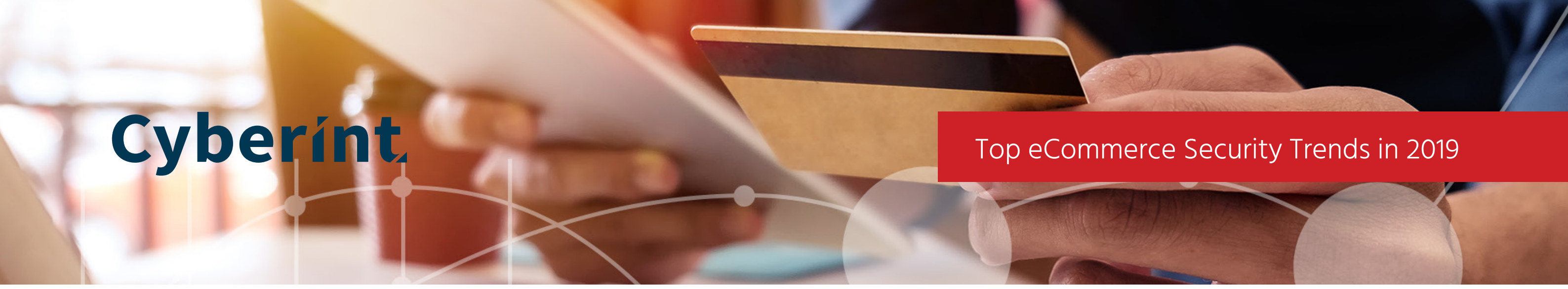
[Data Leakage]

The 'low and slow' method of data exfiltration has proven effective in staying under the radar of detection. This loss of sensitive data is a result of inadequate technical controls. Security administrators must determine what data is sensitive and apply controls to prevent access to that data. It's important to understand the different avenues of accessing the data, such as through a corporate asset to the eCommerce platform.

[Denial of Service]

This type of attack is easily launched by unsophisticated threat actors. In fact, DDoS (Distributed Denial of Service) capabilities can be rented as a service from underground marketplaces. In the past, organized cyber criminals have used DDoS in extortion campaigns – essentially threatening to DDoS a site if money isn't paid to the extortioners.

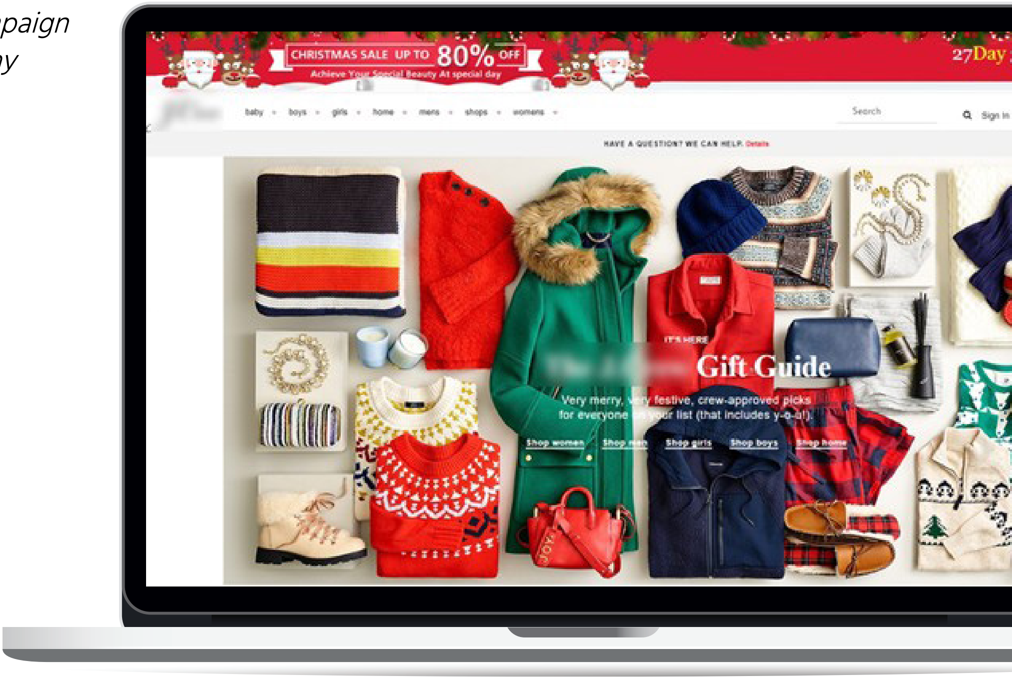
Individuals or groups motivated politically or ideologically will also use this type of attack against an opponent. Earlier this year, the US Department of Justice (DOJ) seized 15 Internet domains used in DDoS attacks launched last December. According to the DOJ, those domains were involved in attacks on government systems, universities, financial institutions, ISPs, and gaming platforms worldwide. One such attack targeted the University of Albany (UAlbany). For more then three weeks, 17 DDoS attacks were made, and according to the head of IT security at UAlbany, the university was specifically targeted.

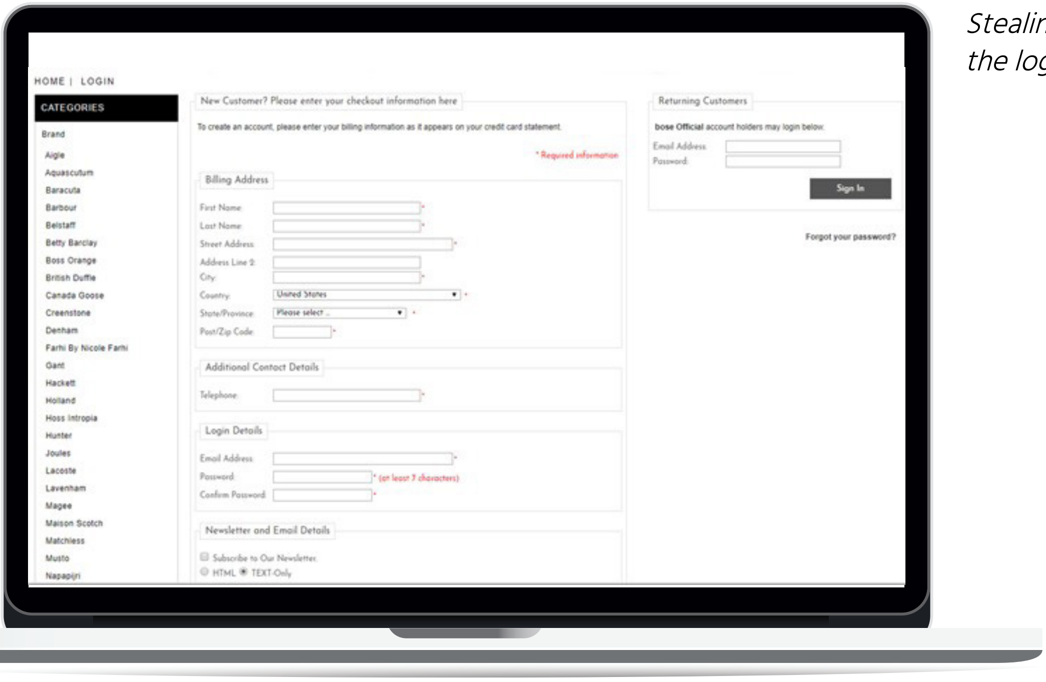


[Social Engineering]

Attackers use psychological manipulation to compel users into making a security mistake or give away sensitive information. Phishing sites, spear phishing, and whale phishing are all forms of social engineering. A spear phishing campaign was recently detected, using methods similar to a Russian threat actor they to refer as TA505, that targeted USA retailers. The phishing email included a document with the logo of the target company to appear legitimate. The document contained a macro that initiated a chain of events to obfuscate the attack in hopes of evading detection.

A phishing site part of a phishing campaign targeting a US retailer over the holiday season 2019


CHRISTMAS SALE UP TO 80% OFF
Achieve Your Special Beauty At special day
27Day
baby
boys
girls
home
mens
shops
womens
Search
Sign In
HAVE A QUESTION? WE CAN HELP. Details
IT'S HERE
Gift Guide
Very merry, very festive, crew-approved picks for everyone on your list (that includes y-o-u!).
Shop women
Shop men
Shop girls
Shop boys
Shop home



HOME | LOGIN

CATEGORIES

Brand

Aigle
Aquascutum
Baracuta
Barbour
Belstaff
Betty Barclay
Boss Orange
British Duffle
Canada Goose
Creenstone
Denham
Farhi By Nicole Farhi
Gant
Hackett
Holland
Hoss Intropia
Hunter
Joules
Lacoste
Lavenham
Magee
Maison Scotch
Matchless
Musto
Napapijri

New Customer? Please enter your checkout information here

To create an account, please enter your billing information as it appears on your credit card statement.

* Required information

Billing Address

First Name: *
Last Name: *
Street Address: *
Address Line 2:
City: *
Country: United States *
State/Province: Please select ... *
Post/Zip Code: *

Additional Contact Details

Telephone: *

Login Details

Email Address: *
Password: * (at least 7 characters)
Confirm Password: *

Newsletter and Email Details

□ Subscribe to Our Newsletter
○ HTML ● TEXT-Only

Returning Customers

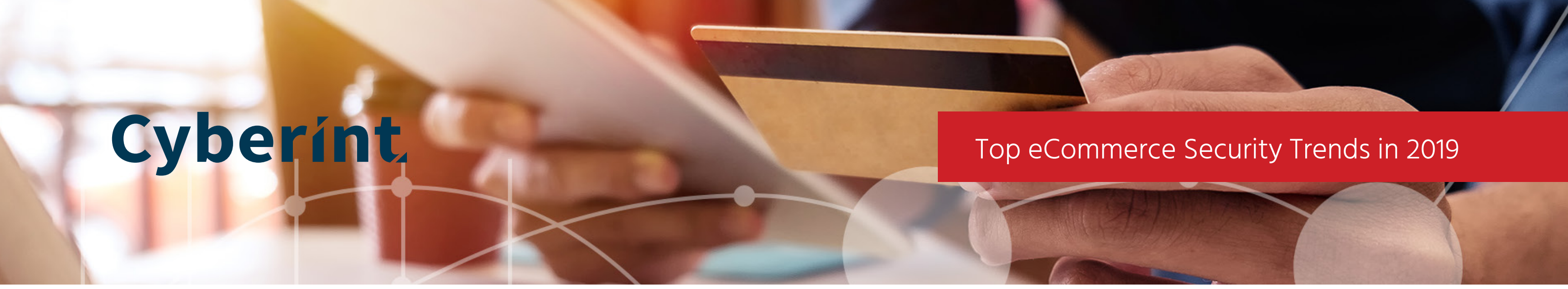
bose Official account holders may login below.

Email Address:
Password:

Sign In

Forgot your password?

Stealing the retailer customers' PII - the login page of the phishing site

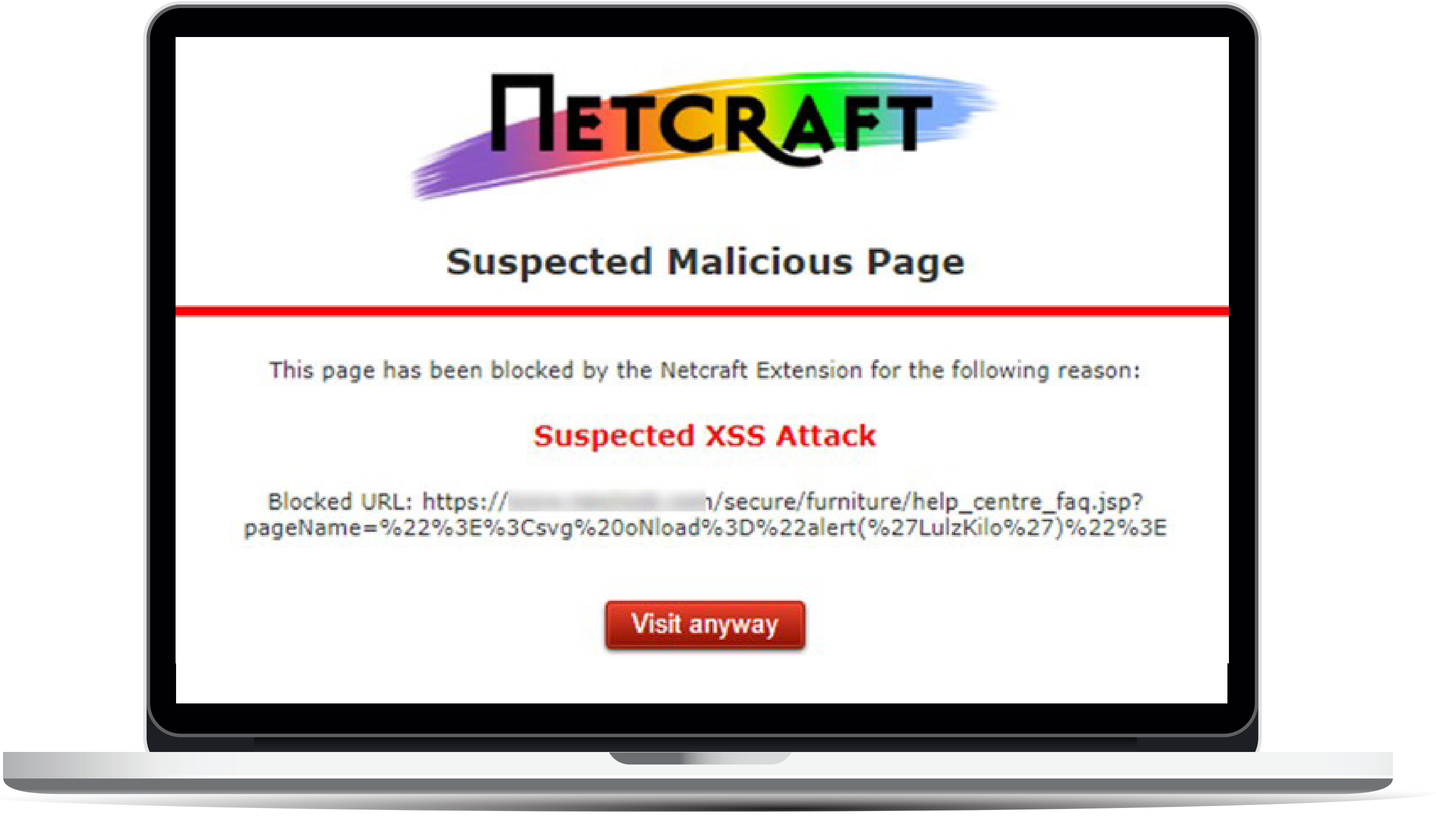


In addition to targeting a brand directly, campaigns against financial organizations can yield credentials that are valid on eCommerce platforms. Once the attackers have credentials from an organization, they can then attempt credential stuffing on another platform.

[Web Application Attack]

Web application attacks are on the rise. As a recent study noted, these types of attacks were the primary source of reported breaches in 2017 and 2018 Q1. These attacks can be motivated by the desire to access customer data or prevent access to the website. Some common web application attacks include cross site scripting (XSS), SQL injection, and cross site request forgery (CSRF).

An attacker executed an XSS attack:



Suspected Malicious Page

This page has been blocked by the Netcraft Extension for the following reason:

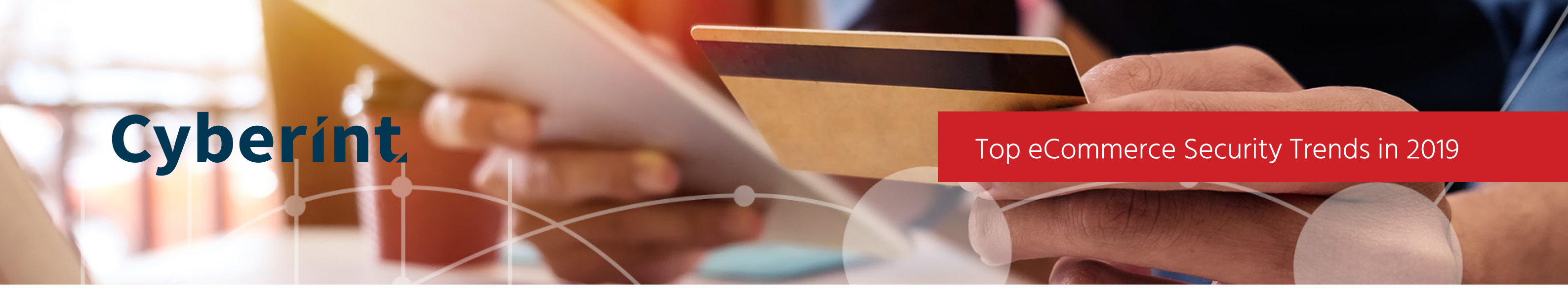
Suspected XSS Attack

Blocked URL: https://[redacted]/secure/furniture/help_centre_faq.jsp?pageName=%22%3E%3Csvg%20oNload%3D%22alert(%27LulzKilo%27)%22%3E

Web applications are critical touchpoints for customer engagement, but often it's also the weakest link for external attacks. To shore up this weakness, it is estimated that the application security market will reach $7 billion by 2023, which means enterprise spending on security scanning tools will more than double the current spending.

[Supply Chain Partners as favorable threat vectors]

According to an Incident Response Threat Report from Carbon Black, half of all cyber attacks occur through a supply chain or third-party. The financial sector (47%), manufacturing (42%), and retail (32%) are most likely to be victims of this attack.



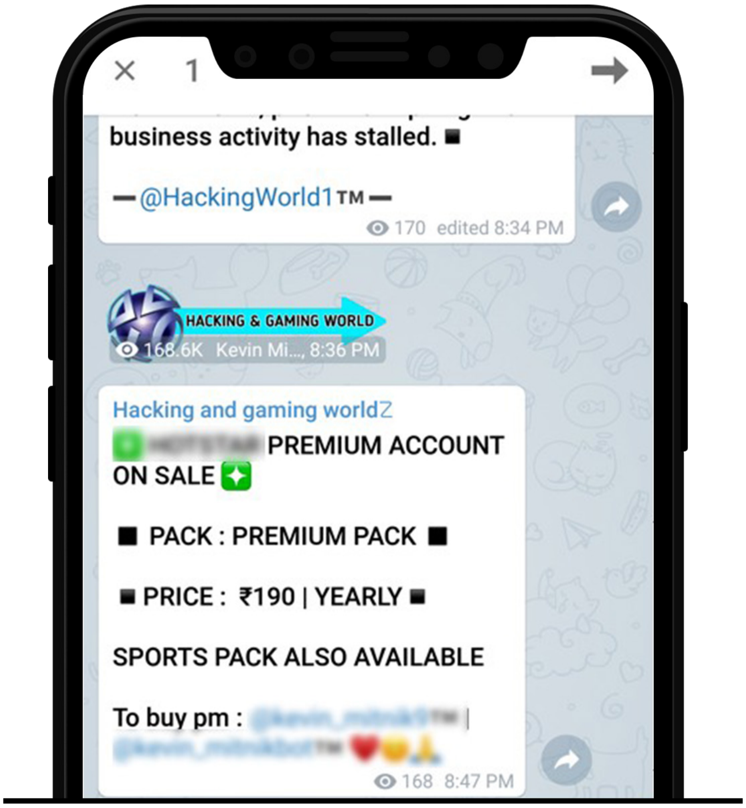
Many organizations have limited information about the security posture of suppliers processing or storing the retailer’s information. The Ponemon Institute says only 35% of companies have an accurate list of all the third-parties with whom they share sensitive information. So even if an enterprise is well protected, attackers are hitting an easier target where they can then pivot to the main target. This has been observed in the Magecart attacks with online advertisers being compromised with payment data stealing scripts that are in-turn trusted and implemented by retail platforms.

Using known server vulnerabilities, cybercriminals such as the well-known Magecart campaign, break into websites and inject card payment skimming code to exfiltrate customer and credit card data. The authentic transaction still occurs so the attack could go on for months before being detected. The Magento eCommerce transaction platform has been determined to be a highly targeted platform. Magento is one of the most popular platforms with an estimated market share of 14-30%. Magento has been found to have specific security weaknesses, particularly in v1.x versions that are likely being exploited, such as exposed administrative consoles.

[Credit Card Fraud]

Theft of credit card data has been a primary target for hackers for many years, and that trend continues today. While EMV chip payment cards have reduced counterfeit fraud, card not present (CNP) fraud is rising. Since 2012, losses from CNP fraud have increased steadily each year. The initial victim in this attack is the consumer whose payment card data has been stolen. The retailer subsequently becomes a victim when chargebacks are issued due to fraudulent transactions. Cybercriminals known as ‘Carders’ exchange tutorials and lists of retail websites that don’t implement additional card verification processes such as American Express SafeKey, Verified by Visa, or MasterCard SecureCode. Marketplaces on the Dark Web resell ‘carded’ merchandise such as gift cards and in-game currency. Others sell services such as fraudulent refunds. For example, an actual employee of a retailer will instruct someone how to submit a fraudulent refund in exchange for a percentage of the refund.

Threat Actor offers accounts for sales on Telegram



business activity has stalled. ■

—@HackingWorld1™—

170 edited 8:34 PM

168.6K Kevin Mi..., 8:36 PM

Hacking and gaming worldZ

[redacted] PREMIUM ACCOUNT ON SALE ✳

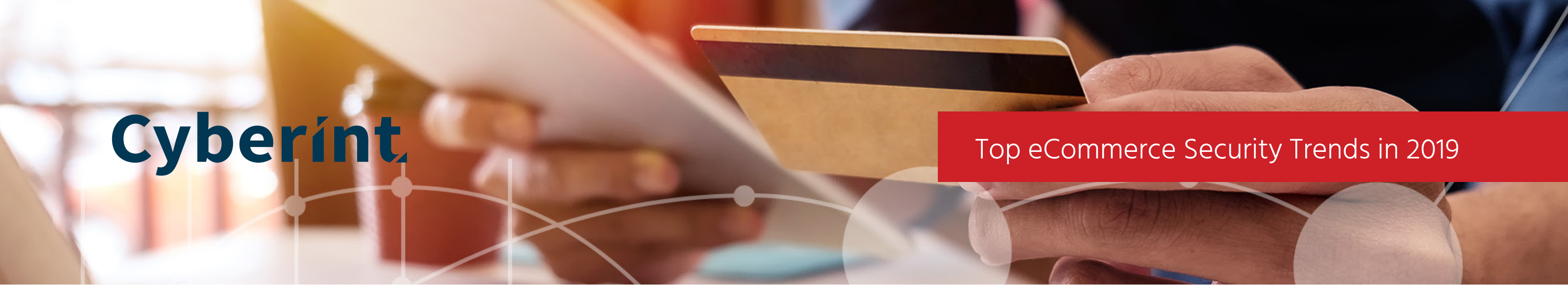
■ PACK : PREMIUM PACK ■

■ PRICE : ₹190 | YEARLY ■

SPORTS PACK ALSO AVAILABLE

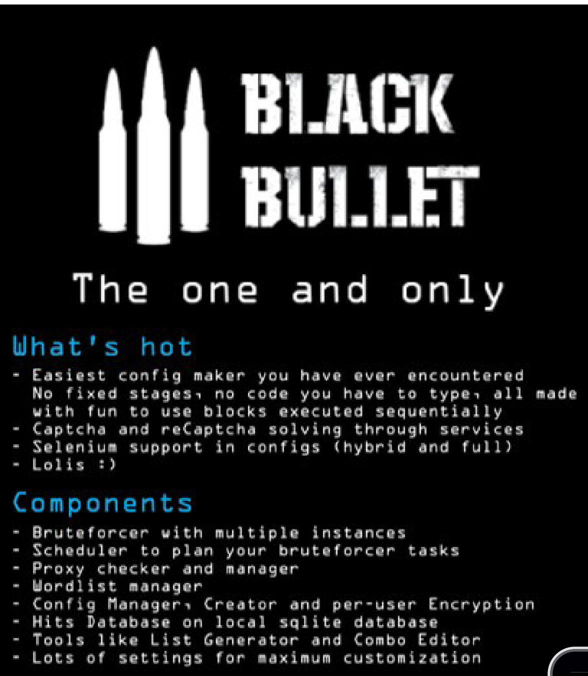
To buy pm : [redacted] | [redacted] ❤😊🙏

168 8:47 PM



[Account Takeover by Credential Stuffing]

People have a tendency to reuse passwords, which makes credential stuffing attacks highly effective. A credential leak from one source can be leveraged by threat actors using widely available off-the-shelf attack tools, which require only entry level hacking skills. After obtaining the list of credentials, it's as easy as clicking 'start' in the attack software to get a list of valid accounts. Account takeover and accounts for sale continue to be strong active threats, particularly to the retail sector. These transactions often occur on the Dark Web, but also on social media sites. According to the 2018 Identity Fraud Study by Javelin Strategy & Research, losses from account takeovers more than tripled over the previous year to $5.1 billion.



BLACK BULLET

The one and only

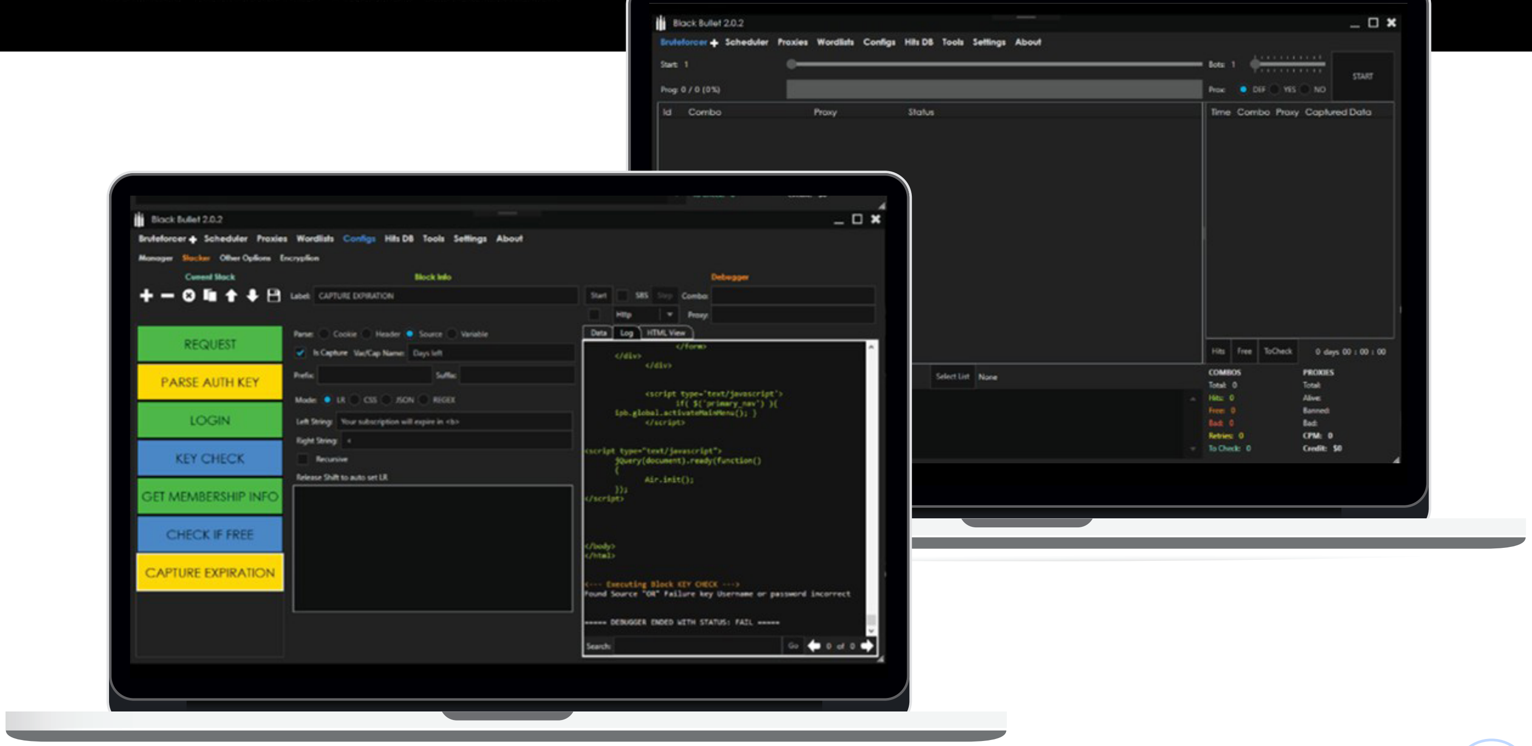
What's hot

- Easiest config maker you have ever encountered
  No fixed stages, no code you have to type, all made
  with fun to use blocks executed sequentially
- Captcha and reCaptcha solving through services
- Selenium support in configs (hybrid and full)
- Lolis :)

Components

- Bruteforcer with multiple instances
- Scheduler to plan your bruteforcer tasks
- Proxy checker and manager
- Wordlist manager
- Config Manager, Creator and per-user Encryption
- Hits Database on local sqlite database
- Tools like List Generator and Combo Editor
- Lots of settings for maximum customization

Brute force tool created by a hacking group



The brute force interface

Start: 1
Prog: 0 / 0 (0%)
Bots: 1
Prox: ● DEF ○ YES ○ NO
0 days 00 : 00 : 00
Select List: None

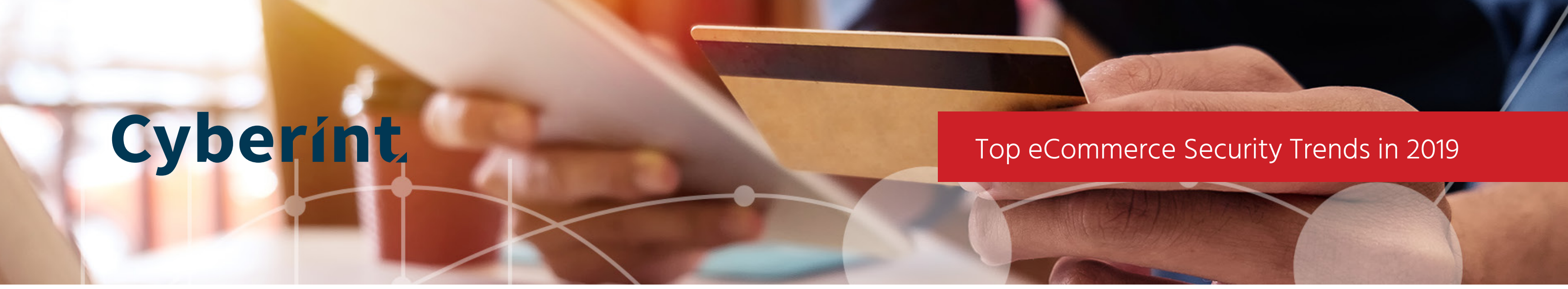
COMBOS
Total: 0
Hits: 0
Free: 0
Bad: 0
Retries: 0
To Check: 0

PROXIES
Total:
Alive:
Banned:
Bad:
CPM: 0
Credit: $0

Label: CAPTURE EXPIRATION
Parse: ○ Cookie ○ Header ● Source ○ Variable
☑ Is Capture Var/Cap Name: Days left
Prefix: Suffix:
Mode: ● LR ○ CSS ○ JSON ○ REGEX
Left String: Your subscription will expire in <b>
Right String: <
□ Recursive
Release Shift to auto set LR

Combo:
Proxy:
Http
0 of 0

```
                    </form>
        </div>
                </div>


                <script type='text/javascript'>
                        if( $('primary_nav') ){
        ipb.global.activateMainMenu(); }
                </script>


<script type="text/javascript">
        jQuery(document).ready(function()
        {
                Air.init();
        });
</script>




</body>
</html>


<--- Executing Block KEY CHECK --->
Found Source "OR" Failure key Username or password incorrect


===== DEBUGGER ENDED WITH STATUS: FAIL =====
```



[Mobile Applications]

The use of retail mobile applications continues to rise. A study conducted by Synchrony shows the average consumer uses 4 retail apps on their phone, which is double from the previous year. Cybercriminals are leveraging this consumer touchpoint by tricking mobile users to install fake or malicious apps. According to a report from RSA, 28% of all fraud attacks in Q2 2018 were attributed to malicious apps. Although it's the consumer being targeted, retailers also suffer loss of sales and damage to brand reputation.

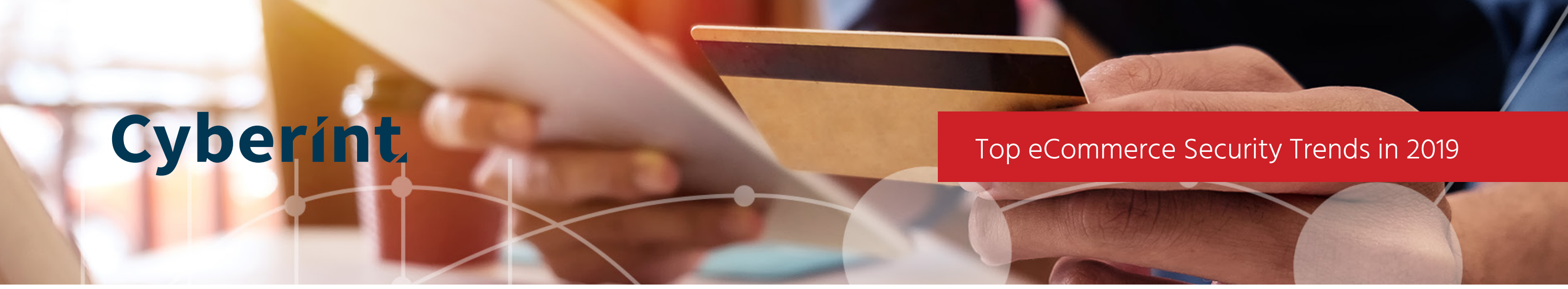
[Compromise of Cryptographic Keys]

As more organizations are encrypting data in transit and data at rest, it's also creating greater opportunities for attack. The uptick in data encryption has increased the likelihood of attackers targeting crypto keys. The more keys an organization needs to manage, the likelihood of key mismanagement increases. Cryptographic keys are used to protect digital assets and communication. It's difficult to know a key has been compromised until it's already been exploited. Keys are more vulnerable when keys are used incorrectly, reused, over-used, stored inappropriately, moved insecurely, or not destroyed after expiration. Well-known vulnerabilities such as POODLE and 3SHAKE result in man-in-the-middle attacks.

[Cloud Infrastructure Attack]

With organizations continuing to move more applications and data to the cloud, it has become a growing target for cybercriminals. One of the biggest trends is the increase in illicit cryptocurrency miners that take advantage of the vast processing infrastructure of cloud environments.

Two notable breaches involved databases storing sensitive information in the cloud with no passwords. A watchlist with more than 2.4 million records, owned by Dow Jones, of risky individuals and corporate entities has been exposed after being left on a cloud server without a password. Another breach involved an AWS hosted database containing the contact information of over 49 million Instagram influencers, celebrities and brand accounts. The database, with no password protection, held the influencer's personal contact information, such as the Instagram account owner's email address and phone number.



FINAL WORD

As online retailers offer customers multiple channels, those additional avenues increase the attack surface and increase the potential of revenue loss from fraud, legal fines from GDPR, account takeover, and brand abuse. However, an even more important element at stake is the economy of trust. A decade ago, digital advertising and social media coined the term "economy of data", and more recently it's been the "economy of experience". Cybersecurity can affect that experience and subsequently impact trust. Today, cybersecurity can build or destroy companies, making the "economy of trust" critical.

In the eCommerce world, trust is going to play an increasing role in the ability to retain customers and enable users to complete the shopping journey quicker and repeatedly. The circle of trust between business and consumer can be easily broken and costly to mend. And the ability of a business to maintain that trust can come down to how seriously they view cybersecurity.

Cyberint
sales@cyberint.com

UNITED KINGDOM
Tel: +44-203-514-1515
14 Grays Inn Rd, Holborn | London | WC1X 8HN | Suite 2068

USA
Tel: +1-646-568-7813
214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

ISRAEL
Tel: +972-3-7286777 | Fax: +972-3-7286777
Ha-Mefalsim 17 St | 4951447 | Kiryat Aryeh Petah-Tikva | Israel

SINGAPORE
Tel: +65-3163-5760
10 Anson Road | #33-04A International Plaza 079903 | Singapore