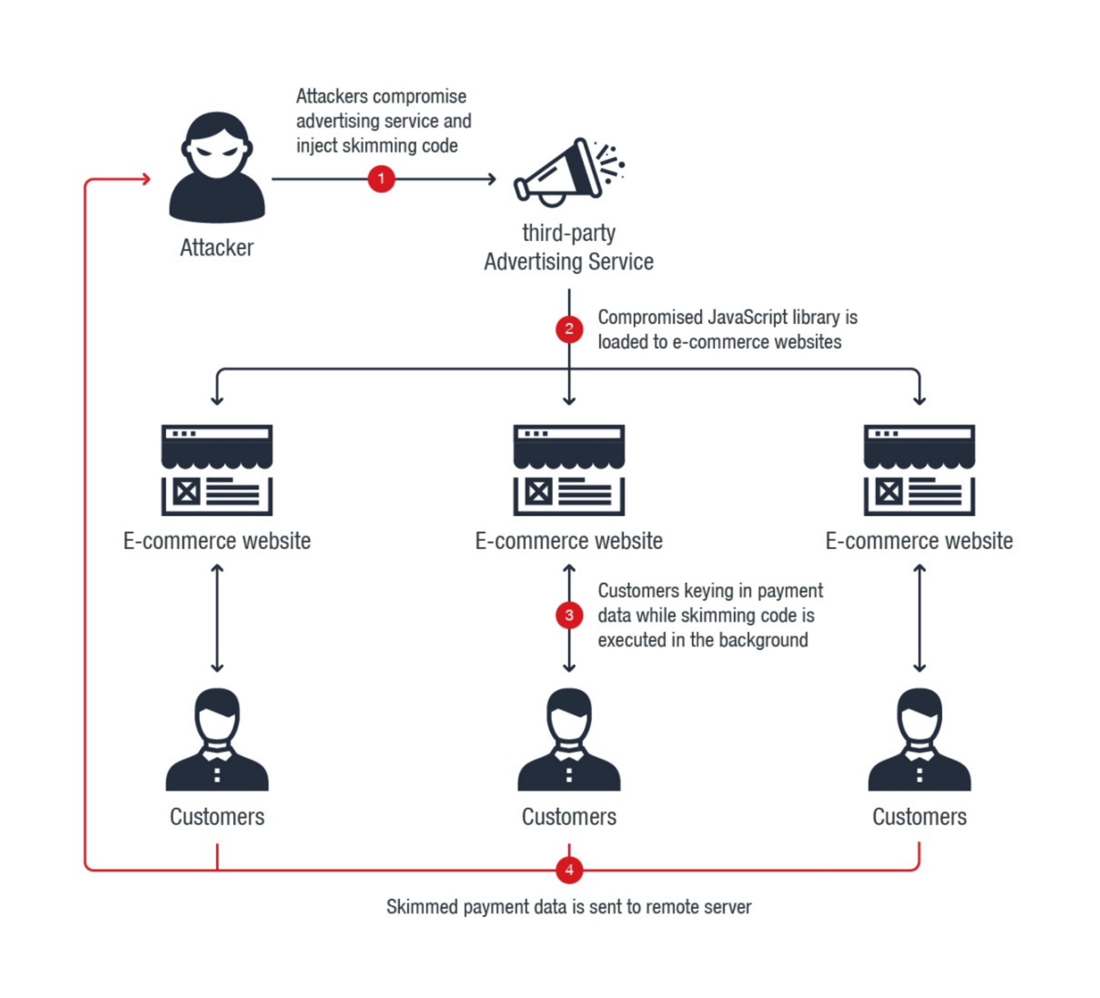
kindred

# Security Newsletter

21 January 2019

Subscribe to this newsletter

# Hackers infect e-commerce sites by compromising their advertising partner


Attackers compromise advertising service and inject skimming code
1
Attacker
third-party Advertising Service
2
Compromised JavaScript library is loaded to e-commerce websites
E-commerce website
E-commerce website
E-commerce website
3
Customers keying in payment data while skimming code is executed in the background
Customers
Customers
Customers
4
Skimmed payment data is sent to remote server

Magecart strikes again, one of the most notorious hacking groups specializes in stealing credit card details from poorly-secured e-commerce websites. According to security researchers from RiskIQ and Trend Micro, cybercriminals of a new subgroup of Magecart, labeled as "Magecart Group 12," recently successfully compromised nearly 277 e-commerce websites by using supply-chain attacks.

Magecart is the same group of digital credit card skimmers which made headlines last year for carrying out attacks against some big businesses including Ticketmaster, British Airways, and Newegg. Typically, the Magecart hackers compromise e-commerce sites and insert malicious JavaScript code into their checkout pages that silently captures payment information of customers making purchasing on the sites and then send it to the attacker's remote server.

The third-party library targeted by Magecart Group 12 is by a French online advertising company, called Adverline, whose service is being used by hundreds of European e-commerce websites to display ads.

Read More on TheHackerNews

Even More on TrendMicro's Blog

Even More

## Bug in Fortnite Authentication Left Accounts Open to Take Over

A weakness in Epic Games' authentication process for the highly popular Fortnite left gamers' accounts exposed to take over risks. An attacker could have stolen login tokens by just tricking the victim into clicking a link.

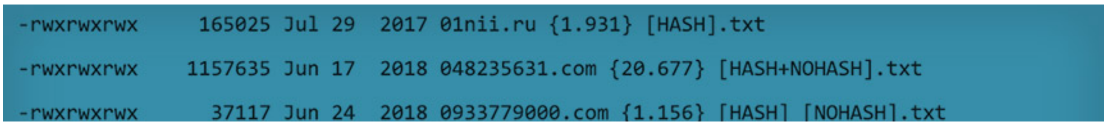
The combination of an unvalidated subdomain and cross-site scripting (XSS) in another allowed security researchers to bypass the protections implemented by the single sign-on (SSO) access control mechanism used for logging into Fortnite.

Epic Games fixed the issues in early December and did not say if they were exploited before that. Fortnite enjoys mad popularity, with at least 78 million monthly players, while statistics point to around 200 million registered users. Its players are often targeted for the V-Bucks - short for Vindertech Bucks or Vinderbucks in their accounts, an in-game currency that can be used to get cosmetic items for your character or to give it a competitive advantage through weaponry.Since real money is involved, criminals often use Fortnite to launder their proceedings by getting V-Bucks with stolen credit cards. The in-game currency is then sold at a discount price. At the moment, 1,000 V-Bucks cost $10.

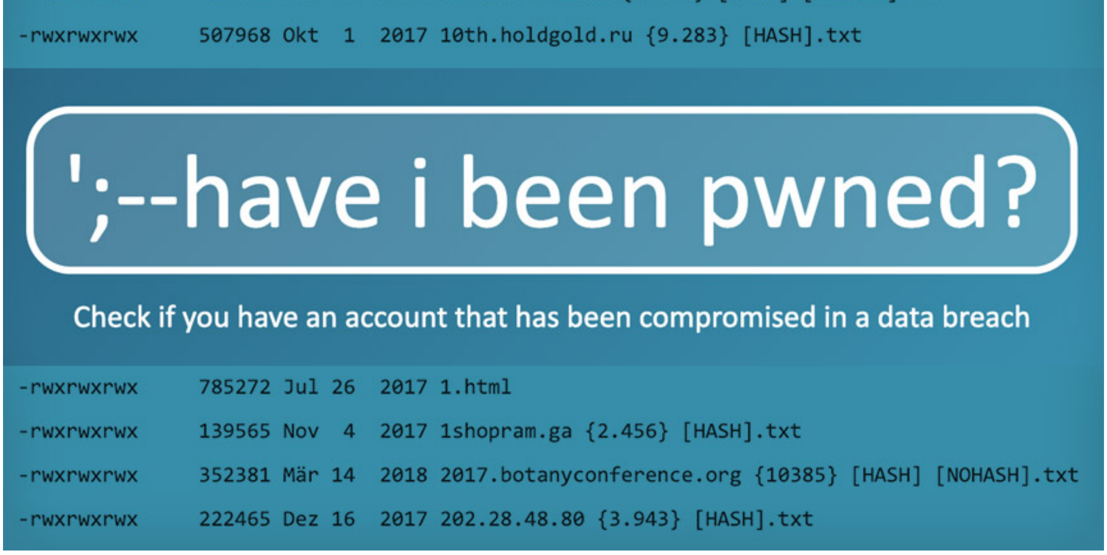
Read More on BleepingComputer

Hacking Fortnite Accounts (CheckPoint Research)

## Data Breach Collection Contains 773 Million Unique Emails



```
-rwxrwxrwx     165025 Jul 29  2017 01nii.ru {1.931} [HASH].txt
-rwxrwxrwx    1157635 Jun 17  2018 048235631.com {20.677} [HASH+NOHASH].txt
-rwxrwxrwx      37117 Jun 24  2018 0933779000.com {1.156} [HASH] [NOHASH].txt
```



```
-rwxrwxrwx     507968 Okt  1  2017 10th.holdgold.ru {9.283} [HASH].txt
```

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

```
-rwxrwxrwx     785272 Jul 26  2017 1.html
-rwxrwxrwx     139565 Nov  4  2017 1shopram.ga {2.456} [HASH].txt
-rwxrwxrwx     352381 Mär 14  2018 2017.botanyconference.org {10385} [HASH] [NOHASH].txt
-rwxrwxrwx     222465 Dez 16  2017 202.28.48.80 {3.943} [HASH].txt
```

On Thursday, Australian information security expert Troy Hunt warned that a collection of email address and passwords combinations that's currently in circulation contains 2.7 billion rows. He says the massive collection of breached data, called "Collection #1," appears to have been compiled from a hodgepodge of sources, and contains 773 million unique email addresses.

The name for the collection comes from the name of the root folder storing all of the data, which is contained in more than 12,000 files and totals 87 GB of data. Hunt says he was alerted to the existence of the collection, which was available via the MEGA file-sharing service - it's been removed - and which has since been shared on at least one hacking forum.

One likely use for all of this data is for credential-stuffing attacks, which is the practice of taking username/password combinations and trying them out on other websites to see where they work. If an individual reuses the same email address and password combination on multiple sites, so can attackers. Last week, for example, many people suspected that streaming service Spotify had suffered a breach, because of lists of "Spotify" usernames and passwords that were being published to text-sharing sites such as Pastebin.

Hunt says the obvious takeaway from the Collection #1 data breach is that everyone should be using a different password for every different site or service they use. That way, if it gets breached - and they get a notification that their username/password combo was pwned - they need only change that one password. "If you're in this breach and not already using a dedicated password manager, the best thing you can do right now is go out and get one"

Read More on BankInfoSecurity

Even More on TroyHunt's Blog

773M Password ‘Megabreach’ is Years Old (KrebsOnSecurity)

## More #News

- Office 365 Secure Score

- CastHack: Hacking Chromecast/Google Homes/SmartTVs
- Phishing toolkit uses custom font and substitution cipher to evade detection
- USB-C Authentication sounds great, so why are people worried?
- Security best practices for Azure solutions
- Don't fall victim to the Chromecast hackers – here's what to do
- PagerDuty Open Sources Its Incident Response Best Practices
- 5.25 Million Unencrypted Passport Numbers Accessed in Starwood Breach
- Banking-Grade Credential Stuffing: The Futility of Partial Password Validation
- A Twitter Bug Left Android Users' Private Tweets Exposed For 4 Years
- Hackers Leak Personal Data from Hundreds of German Politicians On Twitter
- Flaws in a Card Access Control System May Allow Hackers to Bypass Security
- It only takes a Skype Call to Unlock an Android Handset
- Reddit locks out users with poor password hygiene after spotting 'unusual activity'
- Mozilla: Firefox 69 will disable Adobe Flash plugin by default
- Chrome Extension That Steals Credit Cards Numbers Detected On Web Store
- Microsoft and VirusTotal Team Up to Detect Malicious Signed MSI Files
- Flight Booking System Flaw Affected Customers of 141 Airlines Worldwide

# #Patch Time!

- Microsoft Patch Tuesday — January 2019 Security Updates Released
- New Systemd Privilege Escalation Flaws Affect Most Linux Distributions
- SCP implementations impacted by 36-years-old security flaws
- Adobe Patches 'Important' Flaws in Connect, Digital Editions
- Oracle Released Biggest Security Updates – 284 Vulnerabilities are Fixed that Affected Oracle Products

# #Tech and #Tools

- 9 Kubernetes Security Best Practices Everyone Must Follow
- MKCert: Valid HTTPS certificates for localhost
- TLS Fingerprinting with JA3 and JA3S
- SSH Examples, Tips & Tunnels
- Everything you should know about certificates and PKI but are too afraid to ask
- Microsoft Launches Azure DevOps Bounty Program
- Security Training for Engineers
- hassh: Network fingerprinting standard to identify specific Client and Server SSH implementations.
- Bypassing Crowdstrike Falcon detection, from phishing email to reverse shell
- Metasploit Framework 5.0 Released!
- uncaptcha2: defeating the latest version of ReCaptcha with 91% accuracy
- CloudGoat: The ‘Vulnerable-by-Design’ AWS Environment
- Subverting X509Certificate.Equals in .NET
- A tale of private key reuse
- Introduction to WebAuthn API
- MiTM Attack Between Target Windows Machines and a DNS Server

- Effective Security Pipeline
- Social Engineering – Impersonation made easy

This content was created by Kindred Group Security. Please share if you enjoyed!

## Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us