

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-0827

**CREDIT CARD 'SNIFFERS' POSE
PERSISTENT THREAT TO GROWING
E-COMMERCE INDUSTRY**

Recorded Future analyzed current data from the Recorded Future® Platform, information security reporting, and other open source intelligence (OSINT) sources to identify sniffers that facilitate threat actor campaigns. This report expands upon findings addressed in the report [“Automation and Commoditization in the Underground Economy,”](#) following reports on [database breaches](#), [checkers and brute forcers](#), and [loaders and crypters](#). This report will be of most interest to network defenders, security researchers, and executives charged with security risk management and mitigation.

Executive Summary

As global business is migrating toward conducting more transactions online, threat actors have become more invested in identifying and exploiting vulnerabilities in website payment processing systems and interfaces, particularly ones that permit threat actors to inject malicious JavaScript (JS) and exfiltrate customer data and payment card details.

As this and [previous](#) Recorded Future reporting highlights, the injection of malicious JS code into websites is not reserved to Magecart — an umbrella term for threat actor groups employing this technique — but is also being marketed by multiple threat actors on the dark web who develop customized payment sniffers that are updated regularly, contain multiple capabilities, and are available for purchase or rent. These readily available sniffer variants permit cybercriminals to steal and harvest sensitive information from compromised payment processing websites. As long as these attacks keep paying dividends, threat actors like the three profiled in this report are likely to continue to develop and sell customized sniffers that are capable of defeating updated security measures and alerts.

Key Judgments

- Dark web threat actors are using high-tier dark web sources to advertise and sell customized JS sniffers that are designed and regularly updated to harvest credentials once injected into a website's payment processes.
- Customized sniffer variants contain multiple capabilities and functionalities, including easy-to-use interfaces, as well as the ability to organize compromised data into digestible formats, delete recurring payment card data, extract personally identifiable information (PII), and defeat antivirus settings.

- Due to the public successes around Magecart attacks, threat actors are likely to continue to take an interest in sniffers and will use dark web sources to advertise and purchase customized sniffer variants.

Background

In today's cyber threat landscape, threat actors deploy three common tactics, techniques, and procedures (TTPs) when stealing payment card numbers and other personally identifiable information (PII): skimmers and shimmers, point-of-sale (PoS) malware, and sniffers. We define these techniques, which are not interchangeable, as follows:

- **Skimmers and Shimmers:** Hardware devices that are inserted or laid over ATMs, gas pumps, and other physical payment terminals. These devices are designed to extract [track 1 and 2](#) payment card data and sometimes PIN codes.
- **Point-of-Sale Malware:** Malicious code or software that targets payment terminals and is designed to capture track 1 or 2 payment data, which in some cases can be used to conduct [card-not-present](#) (CNP) transactions. Technically, PoS malware can engage in sniffing, but this is usually network and not payment sniffing. Recorded Future has identified at least 92 PoS malware variants.
- **Sniffers:** Malicious code, usually JavaScript (JS), that is injected onto a website's payment system and is designed to steal payment card information, including card verification values (CVVs), the three- or four-digit number on the back of credit cards, as well as other PII. Methods of code injection include XSS attacks, formjacking, third-party code, and library reuse.

As more sales occur online and through mobile transactions, threat actors are focusing on identifying vulnerabilities within e-commerce platforms and checkout pages on websites. Especially now during the COVID-19 pandemic — e-commerce sales [increased](#) by a reported 49 percent in April 2020 — threat actors are financially motivated to capitalize on these shifts. These vulnerabilities and trends are not only being exploited by individual threat actors but also by advanced persistent threats

(APT) such as the North Korean APT Lazarus Group, [identified](#) in July 2020 targeting major online U.S. and European retailer websites.

When a threat actor uses a sniffer, they inject malicious JS that automatically captures the data from the customers who visit the infected website, allowing for the automated collection of the payment card and PII of numerous customers. The sniffer forwards the compromised data to the threat actor's C2 for further processing and exploitation. Once a threat actor has successfully stolen CNP data from the checkout pages of e-commerce websites, this CNP data can then be used to purchase goods and services, or will be sold on credit card shops. Threat actors frequently use the compromised CNP data to buy highly liquid items or services, themselves using card-not-present transactions.

As addressed in this report, "Magecart," the umbrella term used to describe threat actor groups who harvest compromised payment credentials from websites via malicious JS injection, is not the only group of threat actors using malicious JS. Recorded Future has identified and investigated dark web threat actors advertising customized sniffer variants across dark web sources that contain unique attributes and are regularly updated by operators to defeat newly implemented security measures.

Customized Sniffer Variants and the Threat Actors Behind Them

Sochi

"Sochi" is the primary moniker used by at least two different Russian-speaking persons active on at least three forums: Exploit, Verified, and Club2CRD. Sochi is the creator of the JS sniffer "Inter" and the trojan Android Red. In March 2019, Recorded Future investigated Sochi's dark web activities and found the following intelligence:

- Additional monikers used by Sochi include: "xx5" (Verified) and "SSN" (Club2CRD).
- Criminal activities and services offered include malware development, bulletproof hosting, e-commerce website compromise, cashout, purchasing compromised

banking credentials and access to websites, and resale of compromised credentials from other threat actors, including "BuyCC" and "LookigtoBuy."

- Sochi has also offered to buy out potential accesses to online shops with any type of payment solutions: payment form on the website, iframe, or redirect. The threat actor offers up to 85 percent of the compromised payment cards from the provided access or \$20,000 USD in exchange of 1,000 credit cards.

Regarding Sochi's sniffer variant Inter, we found that the threat actor began advertising it in December 2018 and described it as a universal sniffer designed to steal CNP payment data from payment platforms, specifically Magento, OpenCart, and OsCommerce as well as websites that use iframes or third-party payment processors. Some instances of Inter were found searching for different strings such as "GetCCInfo:fuction" in the source code of a website.

Currently, Sochi is selling licenses for Inter for around \$1,000, and purchases include the sniffer's payload, user manual, 24/7 customer service, free admin panel, and upgrades. Inter has the following technical capabilities and features:

- Captured data is transformed into a GIF image format before being transferred to the control panel, which permits exfiltration via a GET request.
- The sniffer does not interfere or drop SSL connection.
- Inter is updated regularly so as to remain undetectable to antivirus software.

Billar

"Billar" is a Russian-speaking threat actor who has been active on the criminal underground since 2013 and also operates under the moniker "mr.SNIFFA." Billar is the creator and sole designer of a JS credit card sniffer known as "mr.SNIFFA," which they began advertising first on Exploit Forum on December 3, 2019.

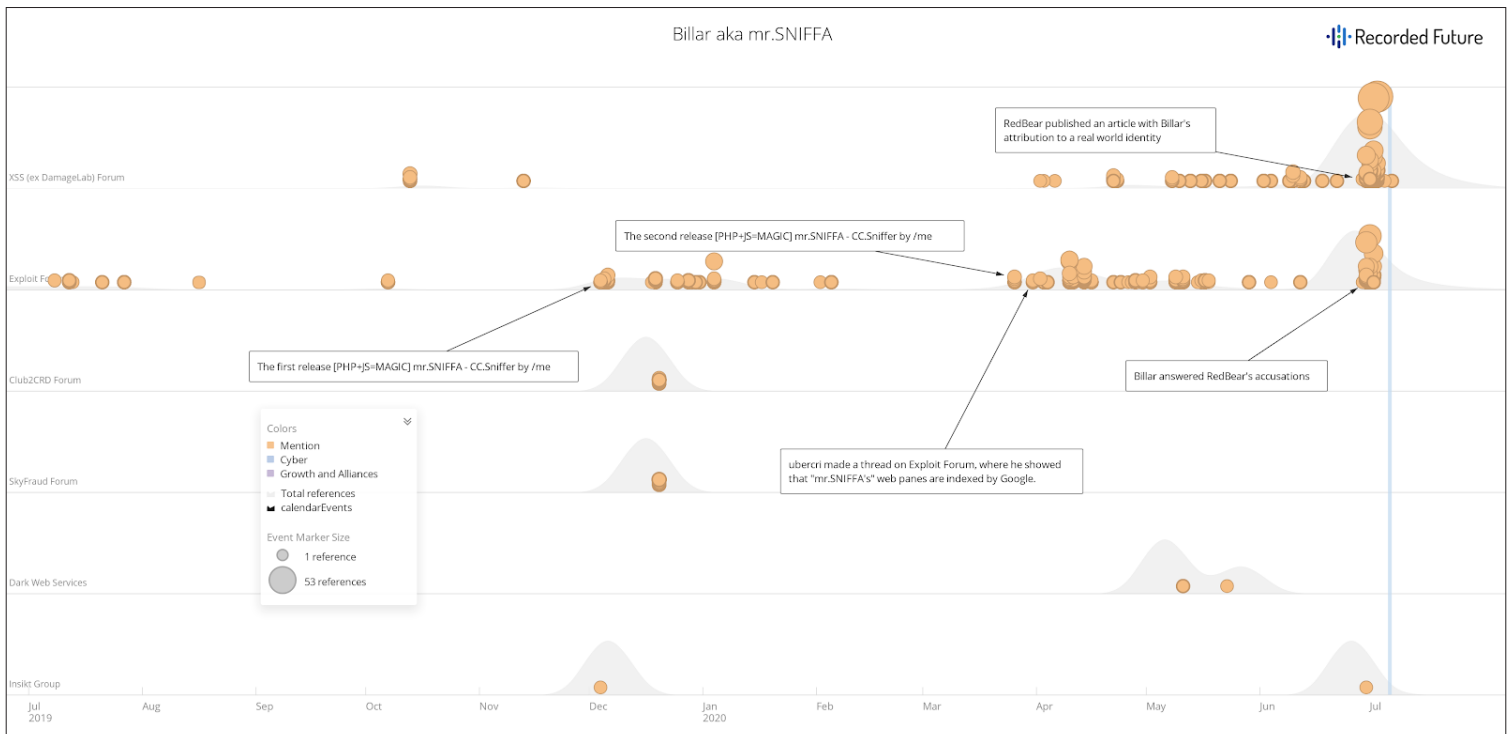


Figure 1: Notable Billar activities from December 2019 to July 2020. (Source: Recorded Future)

On March 30, 2020, "Ubercri," a well-known hacker and a member of multiple underground communities, shared with Exploit Forum members that some of mr.SNIFFA's admin panels can be found via a Google search, making it easy to identify businesses and websites compromised by Billar's sniffer variant.

On June 29, 2020, "RedBear," an experienced malware coder, penetration tester, and reverse engineer, published on XSS Forum research that potentially identified the operator of Billar. According to RedBear, Billar is operated by "Mikhail Mikhailovich Shkrobanets." Recorded Future analysts reviewed RedBear's research and analyzed the steps used to identify Shkrobanets, assessing that RedBear's research is complete and likely accurate, even though some of the steps RedBear took to identify Billar were not legal or ethical.

Currently, Billar is advertising mr.SNIFFA on Exploit Forum for about \$3,000. The package includes the following features:

- A unique way of receiving, implementing, and executing malware code
- Cross-browser obfuscated data transfer

- MaxMind GeoIP integration
- An admin panel that possesses enhanced security to defeat brute-force and DDoS attacks
- 24/7 support and flexibility for any customers' needs

Poter

"poter" is a member of several top-tier Russian-speaking underground forums, including Exploit, Verified, Korovka, as well as the low-tier forum Monopoly, first registered as far back as 2014 on some forums. poter is proficient in various types of financial fraud techniques, including e-commerce, payment card fraud, and money laundering, and is also proficient in malware coding and is a developer of various phishing and scam websites, emails, admin panels, and data grabbers that are applicable for Android, Apple, PayPal, Visa, SunTrust, Flash Player, and other organizations.

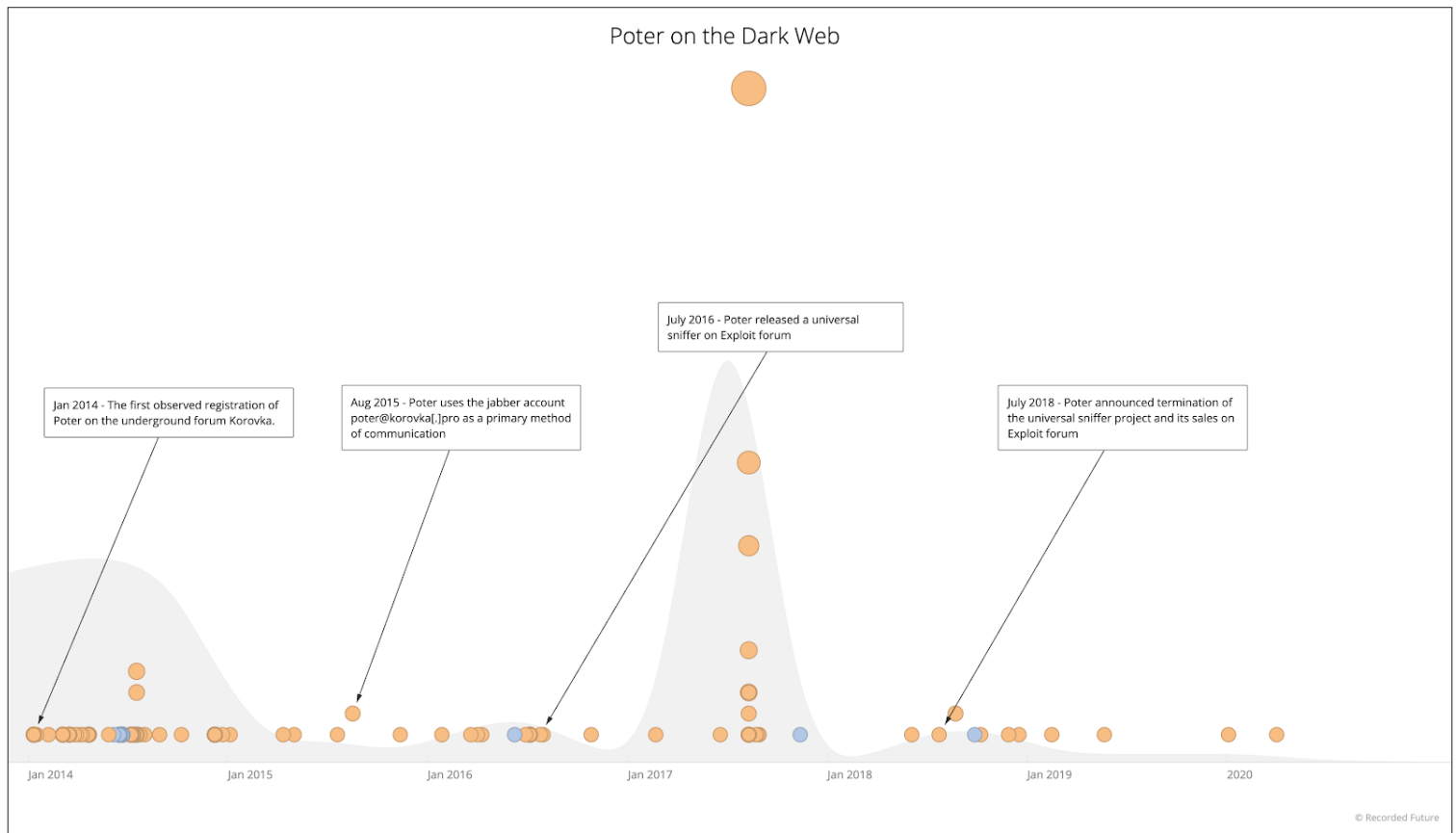


Figure 2: poter's activities on the dark web. (Source: Recorded Future)

The threat actor is a well-known developer of the “Universal Sniffer,” capable of stealing payment card data and victim passwords. This sniffer variant first appeared on Exploit Forum on July 17, 2016 and was removed by the same threat actor on January 10, 2019. It is not clear why poter stopped advertising their Universal Sniffer, and other threat actors may continue to use it privately.

According to poter, the Universal Sniffer had the following basic technical features that were regularly upgraded by the threat actor:

- Written in JS
- Checked all compromised Bank Identification Numbers (BIN)
- Organized stolen payment cards in a single format
- Deleted repeating payment cards
- Grabbed login, password, and shipping/billing addresses from compromised payment cards
- Filtered out compromised payment cards by state

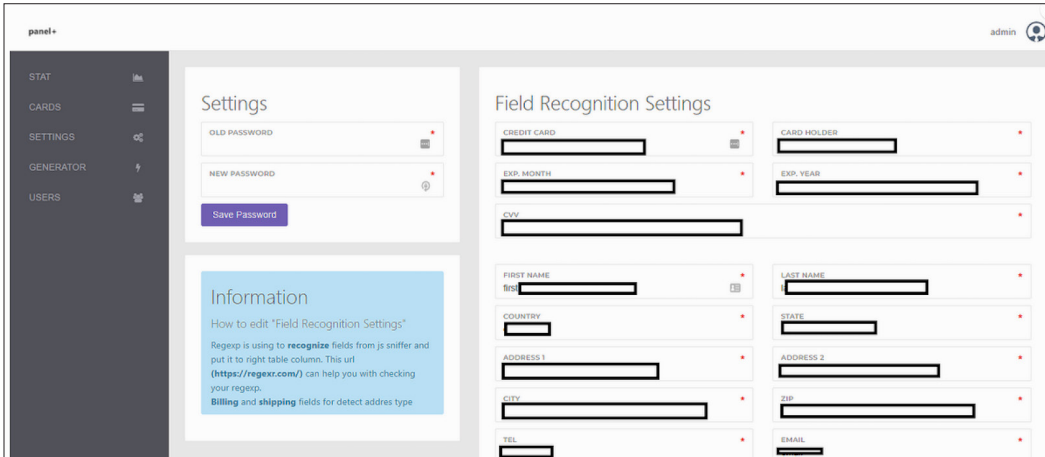
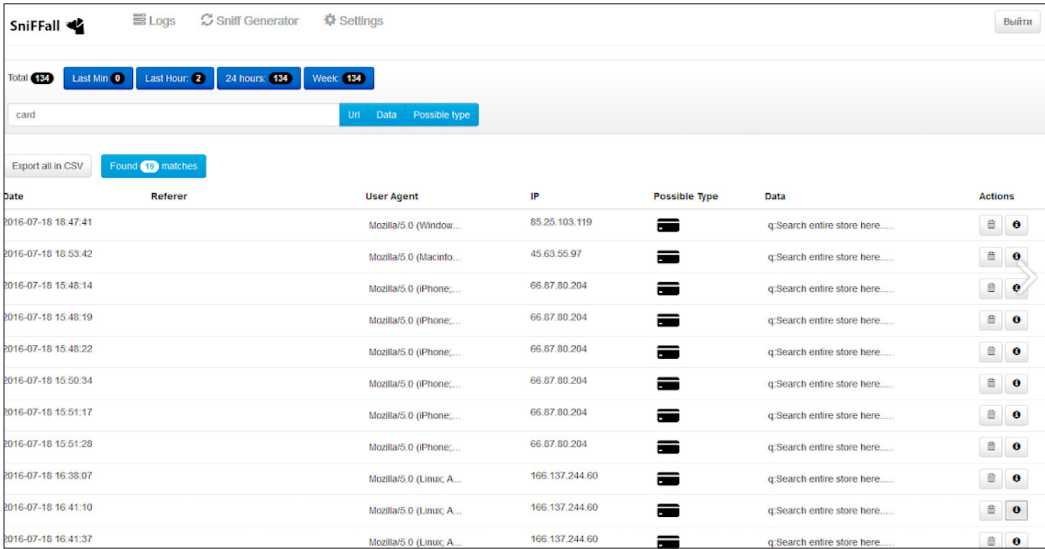


Figure 3: Sniffer admin panel displays compromised payment card field recognition settings.

The image shows the main interface of the sniffer tool. At the top, there are tabs for 'Sniff Generator' and 'Settings', and a 'BuildIt' button. Below the tabs, there are statistics for 'Total' (134) and filters for 'Last Min', 'Last Hour', '24 hours', and 'Week'. A search bar is present with filters for 'Uri', 'Data', and 'Possible type'. Below the search bar, there is a table of results. The table has columns for Date, Referrer, User Agent, IP, Possible Type, Data, and Actions. The data shows multiple entries from various user agents (Mozilla/5.0) and IP addresses, all with a 'Possible Type' of 'q:Search entire store here....'.

| Date | Referrer | User Agent | IP | Possible Type | Data | Actions |
|---------------------|----------|--------------------------|----------------|--------------------------------|------|---------|
| 2016-07-18 18:47:41 | | Mozilla/5.0 (Windows... | 85.25.103.119 | q:Search entire store here.... | | |
| 2016-07-18 10:53:42 | | Mozilla/5.0 (Macinto... | 45.63.55.97 | q:Search entire store here.... | | |
| 2016-07-18 15:48:14 | | Mozilla/5.0 (iPhone;... | 66.87.80.204 | q:Search entire store here.... | | |
| 2016-07-18 15:48:19 | | Mozilla/5.0 (iPhone;... | 66.87.80.204 | q:Search entire store here.... | | |
| 2016-07-18 15:48:22 | | Mozilla/5.0 (iPhone;... | 66.87.80.204 | q:Search entire store here.... | | |
| 2016-07-18 15:50:34 | | Mozilla/5.0 (iPhone;... | 66.87.80.204 | q:Search entire store here.... | | |
| 2016-07-18 15:51:17 | | Mozilla/5.0 (iPhone;... | 66.87.80.204 | q:Search entire store here.... | | |
| 2016-07-18 15:51:28 | | Mozilla/5.0 (iPhone;... | 66.87.80.204 | q:Search entire store here.... | | |
| 2016-07-18 16:38:07 | | Mozilla/5.0 (Linux; A... | 166.137.244.60 | q:Search entire store here.... | | |
| 2016-07-18 16:41:10 | | Mozilla/5.0 (Linux; A... | 166.137.244.60 | q:Search entire store here.... | | |
| 2016-07-18 16:41:37 | | Mozilla/5.0 (Linux; A... | 166.137.244.60 | q:Search entire store here.... | | |

Figure 4: Sniffer interface with compromised data can be sorted out by date, IP address, and user agent.

Initially, poter priced the sniffer at several thousand dollars, but later lowered the price to just a few hundred to attract more users. On July 16, 2018, poter announced that they had enough customers and returned the initial price for the sniffer of several thousand dollars.

During our investigation, Recorded Future did not identify evidence of the three threat actors detailed above using or selling compromised carding data retrieved from their customized sniffers. However, given that the purpose of sniffers is to steal payment card information and that information only has value if it is monetized, it is very likely that the card information must have been either sold or used to purchase goods online which are then resold. An example of how monetization works is the use of both techniques by threat actors behind Magecart. Research has [linked](#) Magecart-related infrastructure and compromised data to at least one dark web carding shop, Trump's Dumps, as well as threat actor [recruiting](#) mules to receive and re-ship merchandise purchased with stolen credit cards.

Magecart

Magecart is a modus operandi used by security researchers and the media to group different threat actors targeting e-commerce sites with JS-based credit card web skimmers used to steal CNP data. The name Magecart itself is a reference to these actors targeting sites running vulnerable plugins for the Magento platform. FlashPoint and RiskIQ indicated that Magecart was initially a single threat actor group who began operating in 2015. A second

distinct group was observed in 2016, and many more have turned up since then. All types of companies, from small to large, across multiple sectors have fallen victim to Magecart-related vulnerabilities since July 2019, including Macy's, Sweaty Betty, Volusion, and Claire's.

Between October 2018 and the time of this report, Recorded Future analysts observed threat activity tied to Magecart operators targeting at least 95 online retail websites. Frequently, the different threat actor groups using various types of sniffers have been referred to generically as Magecart. Although this attack vector seems prevalent, given that there are at least 12 Magecart-related groups and reported attacks have continued, there are only a few threat actors who actually build, sell, and maintain these sniffers.

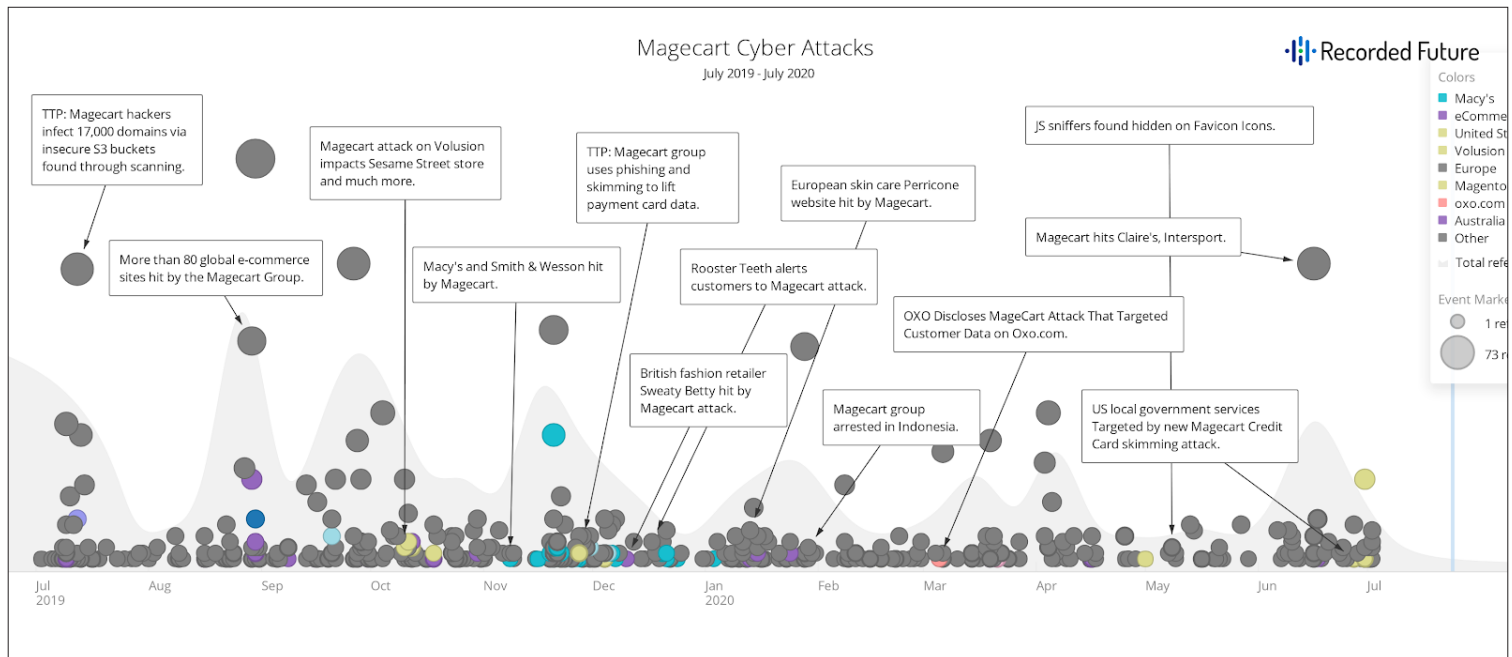


Figure 5: Notable Magecart activities and attacks from July 2019 to July 2020. (Source: Recorded Future)

Over the span of 2019 and into 2020, Magecart operators transitioned from targeting third-party suppliers in an attempt to reach primary targets to injecting their JS sniffer code directly into e-commerce websites to collect payment data, later transferring the data to a command-and-control (C2) server or designated domain.

Over the first quarter of 2020, Magecart credit card sniffing operations have continued to flourish despite highly publicized law enforcement arrests in Indonesia that occurred in December 2019. Interpol [reported](#) on January 27, 2020 that three individuals identified as conducting Magecart card sniffing operations were arrested by Indonesian federal police. Group-IB, which supplied law enforcement with information leading to the arrests, named the Magecart subgroup involved “GetBilling.” Another security firm, Sanguine Security, [reported](#) that it was also tracking the group.

We observed references to three of these sample domains within our data set in addition to three new domains not previously disclosed by Sanguine Security. The JS sniffer operators associated with this latest campaign use injected JS on compromised retail websites and have been using a common set of JS functions over the course of this campaign. Of the 95 impacted websites observed during our research, 28 remained actively compromised in January 2020.

Similar to the incident above, a Magecart-related group named “Keeper” (due to the use of the domain fileskeeper[.]org to inject malicious JS into the website’s HTML code) was [identified](#) by Gemini Advisory as having successfully operated 64 attacker and 73 exfiltration domains that impacted at least 570 websites across 55 countries from April 2017 to the present. Of the impacted websites, an estimated 85 percent [operated](#) the content management system Magento, for which Recorded Future has confirmed at least 10 validated malicious incidents since September 2018.

The scale, sophistication, and length of the abovementioned Magecart attacks indicate that Magecart threat actors are technically savvy, are able to adapt their TTPs based on improvements in website securities, and opportunistically exploit vulnerabilities (both publicly known and unknown) in payment and content management systems on websites.

Outlook and Mitigation Strategies

As global business is migrating toward conducting more transactions online, threat actors have become more invested in identifying and exploiting vulnerabilities in website payment processing systems and interfaces, particularly ones that permit threat actors to inject malicious JavaScript (JS) and exfiltrate customer data and payment card details.

The dark web has become more specialized and is being used to advertise customizable tools and services and provide feedback to enhance these tools, and for threat actors to showcase their technical skills and prowess so as to gain financial reward. Due to multiple attack vectors that threat actors can use to inject malicious JS code as well as the publicly known financial successes associated with Magecart attacks, threat actors are not only likely to continue to target payment process systems on vulnerable websites but are likely to continue to develop and sell customized sniffers that are capable of defeating updated security measures and alerts. Dark web sources (forums, markets, and encrypted messengers) will continue to serve as bridges between threat actors and customers for the foreseeable future.

Below are [mitigation strategies](#) that can assist in detecting and preventing a sniffer attack:

- Perform regular audits of your website, including test purchases to identify any suspicious scripts or network behavior.
- Implement protection client-side such as web skimming or malware protection.
- Prevent any non-essential externally loaded scripts from loading on checkout pages.
- Evaluate how third-party plugins use their code, servers, and external communications on your e-commerce website, and monitor for any changes in their code or behavior.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.