KAMIND®

JANUARY 2021 | VOL. 1

TECHNOLOGY TIMES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY

Credit Card Stealer Discovered In Social Media Buttons

Web skimmer (Magecart) gangs find new ways to attack e-commerce stores and online shoppers.

Cyber-criminals have created a new type of web malware that hides inside images used for social media sharing buttons in order to steal credit card information entered in payment forms on online stores. The malware, known as a web skimmer, or Magecart script, was spotted on online stores in June and September this year by Dutch security firm Sanguine Security (SangSec).While this particular form isn't widely deployed, its discovery suggests that Magecart gangs are constantly evolving their bag of tricks.

STEGANOGRAPHY AND MALWARE ATTACKS

At the technical level, this particular script uses a technique known as steganography. Steganography refers to hiding information inside another format (i.e., text inside images, images inside videos, etc.).In the world of malware attacks, steganography is typically employed as a way to sneak malicious code past security scanners by placing the bad code inside seemingly innocent files. Over the past years, the most common form of steganography attacks has been to hide malicious payloads inside image files, usually stored in PNG or JPG formats. Malware gangs would add the malicious code inside the image, the image would be downloaded on a host system, extracted by another of the malware gang's components, and then executed.

In the world of web-based skimmers (Magecart scripts), steganography works because most web skimmers are typically hidden in JavaScript code and not inside image files.However, the

WHAT'S NEW INSIDE KAMIND IT

Make sure to join KAMIND IT **January 14th, 2021** for our upcoming webinar **"Getting Started with CMMC".** Register now at: kamind.com/getting-started-cmmc/

KAMIND IT has been certified and registered as a **CMMC Registered Practitioner.**

Join KAMIND IT for **Into The Breach, January 21st, 2021**. Visit **kamind.com/into-the-breach** and register today.

From all of us at KAMIND IT we wish you all a **happy and prosperous New Year!**

Credit Card Stealer Discovered In Social Media Buttons:

Continued from page one

technique has slowly been seeing some adoption among web skimmer gangs, with past steganographic attacks using site logos, product images, or favicons to hide payloads.

MALICIOUS CODE HIDDEN IN SVG IMAGES

But as steganography use grew, security firms also started looking and analyzing image files as a place they could find irregularities or hidden web skimmer payloads. The interesting detail in these recent attacks is that the malicious code wasn't hidden inside PNG or JPG files but in SVG files, a type of image file for loading vector-based images.

Vector images load and drawn graphics with the help of coordinates and mathematical functions, and they're a text-based format, rather than a binary format, which, in theory, would make the detection of malicious payloads even easier than with PNG and JPG files. However, SangSec says the threat actors were very clever when they designed their payload.

"The malicious payload assumes the form of an HTML < svg > element, using the < path > element as a container for the payload. The payload itself is concealed utilizing syntax that strongly resembles correct use of the < svg > element," SangSec said in a report last week."While skimmers have added their malicious payload to benign files like images in the past, this is the first time that malicious code has been constructed as a perfectly valid image.

The result is that security scanners can no longer find malware just by testing for valid syntax," the company added. SangSec said it found malware gangs testing this technique in June, and on live e-commerce sites in September, with the malicious payload hidden inside social media sharing icons for sites like Google, Facebook, Twitter, Instagram, YouTube, and Pinterest. On infected stores, once users accessed the checkout page, a secondary component (called a decoder) would read the malicious code hidden inside the social sharing icons and then load a keylogger that recorded and exfiltrated card details entered in the payment form.

USER PROTECTIONS

End users have very few options available at their disposal when it comes to web skimmer attacks, as this type of code is usually invisible to them and extremely hard to detect, even for professionals. Furthermore, users shopping on a site have no way

at their disposal to know how secure a site really is, and if the store owner invests in security at all.

The simplest way shoppers can protect themselves from web skimmer attacks is to use virtual cards designed for one-time payments. These cards are currently provided by some banks or payment apps, and they're currently the best way to deal with web-based skimming as even if attackers manage to record transaction details, the card data is useless as it was generated for one transaction only.

Ransomware gangs are now cold-calling victims if they restore from backups without paying

In attempts to put pressure on victims, some ransomware gangs are now cold-calling victims on their phones if they suspect that a hacked company might try to restore from backups and avoid paying ransom demands.

"We've seen this trend since at least August-September," Evgueni Erchov, Director of IR & Cyber Threat Intelligence at Arete Incident Response stated.

Ransomware groups that have been seen calling victims in the past include Sekhmet (now defunct), Maze (now defunct), Conti, and Ryuk, a spokesperson for cyber-security firm Emsisoft stated.

"We think it's the same outsourced call center group that is working for all the [ransomware gangs] as the templates and scripts are basically the same across the variants," Bill Siegel, CEO and co-founder of cyber-security firm Coveware stated. Arete IR and Emsisoft said they've also seen scripted templates in phone calls received by their customers.

According to a recorded call made on behalf of the Maze ransomware gang, the callers had a heavy accent, suggesting they were not native English speakers. Below is a redacted transcript of a call, provided by one of the security firms as an example, with victim names removed:

"We are aware of a 3rd party IT company working on your network. We continue to monitor and know that you are installing SentinelOne antivirus on all your computers. But you should know that it will not help. If you want to stop wasting your time and recover your data this week, we recommend that you discuss this situation with us in the chat or the problems with your network will never end."

ANOTHER ESCALATION IN RANSOMWARE EXTORTION TACTICS

The use of phone calls is another escalation in the tactics used by ransomware gangs to put pressure on victims to pay ransom demands after they've encrypted corporate networks.

Previous tactics included the use of ransom demands that double in value if victims don't pay during an allotted time, threats to notify journalists about the victim company's breach, or threats to leak sensitive documents on so-called "leak sites" if companies don't pay.

However, while this is the first time ransomware gangs have called victims to harass them into paying, this isn't the first time that ransomware gangs have called victims. In April 2017, the UK's Action Fraud group warned schools and universities that ransomware gangs were calling their offices, pretending to be government workers, and trying to trick school employees into opening malicious files that led to ransomware infections.

KAMIND IT
5200 Meadows Road
STE #150
Lake Oswego, OR 97035

8% of all Google Play apps vulnerable to old security bug

Around 8% of Android apps available on the official Google Play Store are vulnerable to a security flaw in a popular Android library, according to a scan performed this fall by security firm Check Point.

The security flaw resides in older versions of Play Core, a Java library provided by Google that developers can embed inside their apps to interact with the official Play Store portal. The Play Core library is very popular as it can be used by app developers to download and install updates hosted on the Play Store, modules, language packs, or even other apps.

Earlier this year, security researchers from Oversecured discovered a major vulnerability (CVE-2020-8913) in the Play Core library that a malicious app installed on a user's device could have abused to inject rogue code inside other apps and steal sensitive data — such as passwords, photos, 2FA codes, and more. Google patched the bug in Play Core 1.7.2, released in March, but according to new findings published today by Check Point, not all developers have updated the Play Core library that ships with their apps, leaving their users exposed to easy data pilfering attacks from rogue apps installed on their devices.

According to a scan performed by Check Point in September, six months after a Play Core patch was made available, 13% of all the Play Store apps were still using this library, but only 5% were using an updated (safe) version, with the rest leaving users exposed to attacks.

Apps that did their duty to users and updated the library included Facebook, Instagram, Snapchat, WhatsApp, and Chrome; however, many other apps did not. Among the apps with the largest userbases that failed to update, Check Point listed the likes of Microsoft Edge, Grindr, OKCupid, Cisco Teams, Viber, and Booking.com.

Check Point researchers Aviran Hazum and Jonathan Shimonovich said they notified all the apps they found vulnerable to attacks via CVE-2020-8913, but, three months later, only Viber and Booking.com bothered to patch their apps after their notification. "As our demo video shows, this vulnerability is extremely easy to exploit," the two researchers said. "All you need to do is to create a 'hello world' application that calls the exported intent in the vulnerable app to push a file into the verified files folder with the file-traversal path. Then sit back and watch the magic happen."

"This research shows, once again, that while users may be using an up-to-date version of their apps, that doesn't necessarily mean all of an app's inner components are up-to-date as well, with software supply chains often being in complete disarray, even at some of the world's biggest software/tech firms."

This monthly publication is provided courtesy of **Matt Katzer, CEO of KAMIND IT** & Amazon Best-Selling Author of ***"Securing Office 365 - Masterminding MDM and Compliance In The Cloud"***

KAMIND IT's Mission: "KAMIND IT Assists Organizations to Utilize Technology to Drive Innovation"

Inc. 5000 AMERICA'S FASTEST GROWING PRIVATE COMPANIES

Microsoft AEP Authorized Education Gold Partner