kindred

Security Newsletter

16 July 2018

Subscribe to this newsletter

Ticketmaster breach was part of a larger credit card skimming effort, analysis shows

A recent breach at Ticketmaster was just "the tip of the iceberg" of a wider, massive credit card skimming operation, new research has found. At least 800 e-commerce sites are said to be affected, after they included code developed by third-party companies and later altered by hackers, according to security firm RiskIQ.

Yonathan Klijnsma, a threat researcher at RiskIQ, said Magecart has a larger reach "than any other credit card breach to date, and isn't stopping any day soon." By targeting each third-party code supplier, the hackers can in some cases get "nearly 10,000 victims instantly," said the research. Cast your mind back last week to the Ticketmaster breach. The ticket selling giant admitted that some customers had their payment data compromised because its website was running code from Inbenta, a customer support software company, which hackers had altered. It's not uncommon for websites to rely on third-party code, hosted on other sites and services, to support their own. But they present a single point of failure, which, if breached, can affect every site that the code is loaded on.

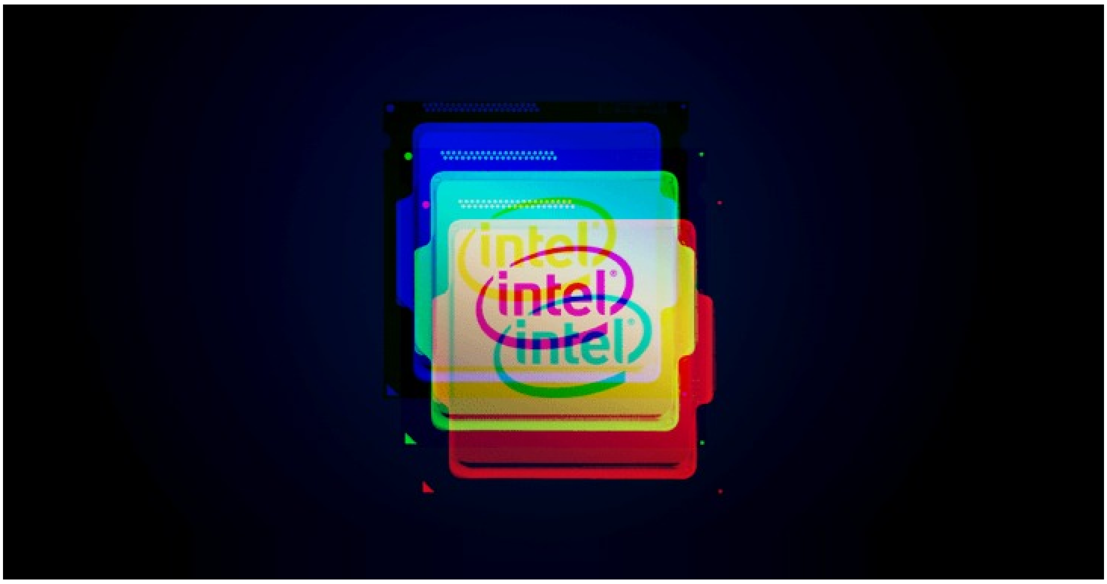
According to RiskIQ, code hosted by social analysis company SociaPlus had also been breached. The hackers had changed the code to quietly skim the credit cards entered at the checkout of any site that the code was served on. The hackers had obfuscated their malicious code at the end of the Javascript library. Any button or form is hooked so when a user clicks a button or submits a form the fields on the page, the skimmer extracts the name and value of the fields, combines them, and sends them to the drop server owned by the Magecart actors.

Klijnsma said that it wasn't clear how each company was compromised. With so many companies affected, a co-ordinated disclosure was impossible, he said. But he said the Magecart threat group "extends well beyond Ticketmaster," discovering close to 100 top-tier sites, like large brands and online shops, but did not name any specific companies. "Personally I don't trust a single online store anymore," he said.

Read More

Even More

Two New Spectre-Class CPU Flaws Discovered —Intel Pays $100K Bounty



Intel has paid out a $100,000 bug bounty for new processor vulnerabilities that are related to Spectre variant one (CVE-2017-5753). The new Spectre-class variants are tracked as Spectre 1.1 (CVE-2018-3693) and Spectre 1.2, of which Spectre 1.1 described as a bounds-check bypass store attack has been considered as more dangerous.

Spectre flaws take advantage of speculative execution, an optimization technique used by modern CPUs, to potentially expose sensitive data through a side channel by observing the system. Speculative execution is a core component of modern processors design that speculatively executes instructions based on assumptions that are considered likely to be true. If the assumptions come out to be valid, the execution continues, otherwise discarded.

Spectre 1.1 is very similar to the Spectre variant 1 and 4, but the two researchers who discovered the bug say that "currently, no effective static analysis or compiler instrumentation is available to generically detect or mitigate Spectre 1.1." As for Spectre 1.2, researchers say this bug can be exploited to write to CPU memory sectors that are normally protected by read-only flags. "As a result [of malicious Spectre 1.2 writes], sandboxing that depends on hardware enforcement of read-only memory is rendered ineffective," researchers say.

Though ARM has also acknowledged the existence of Spectre 1.1 flaw in its blog post published today, the chip maker has not explicitly mentioned which ARM CPUs are especially vulnerable to Spectre 1.1 and Spectre 1.2. AMD has yet to acknowledge the issues. No patches are available for either bugs at the moment.

Read More

Even More

Cutting room floor

- Facebook Faces £500,000 Fine in U.K. Over Cambridge Analytica Leak
- Arch Linux AUR Repository Compromised
- Thought two-factor auth completely locks down Office 365? Not quite
- Here's Why Your Static Website Needs HTTPS
- Now Pushing Malware: NPM package dev logins slurped by hacked tool popular with coders
- Patch Tuesday, July 2018 Edition
- BlackTech APT Steals D-Link Cert for Cyber-Espionage Campaign
- Uncovering Foreign Trolls (Trying) To Influence French Elections on Twitter
- Dark web marketplace found selling access to airport's security system
- Adobe Released Security Updates & Fixes for 112 Vulnerabilities that Affected Adobe Products
- Default router password leads to spilled military secrets
- Google enables Chrome site isolation by default

#Tech and #Tools

- VDiscover: large-scale vulnerability discovery through machine learning
- How to trick CSP in letting you run whatever you want
- Sniff-Paste: OSINT Pastebin Harvester
- Frida 12.0 Released
- ZOHO - A Story Of Where Not To Store Keys
- Weaponization of a JavaScriptCore Vulnerability
- RFID Thief v2.0: Long range RFID cloner

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us