kindred

Security Newsletter

19 November 2018

Subscribe to this newsletter

Beyond Passwords: 2FA, U2F and Google Advanced Protection

This post will be partly about 2FA in general, but also specifically about Google's Advanced Protection program because of the masses of people dependent on them for Gmail. Your email address is the skeleton key to your life (not just "online" life) so protecting that is absolutely paramount.

2FA is two-factor authentication. For some quick perspective, a password alone is 1FA in that when you authenticate merely by entering a secret, all you require is one factor - "something that you know". If someone obtains the thing that you know then it's (probably) game over and they have access to your account. Adding a second factor typically means either requiring "something that you have" or "something that you are". The former is a physical device. MFA is multi-factor authentication. Strictly speaking, 2FA is MFA in that obviously, it's more than one factor. It's a subset of MFA.

2-Step authentication does not necessarily require 2 discrete factors. Entering 2 different passwords, for example, might be 2-step but is entirely predicated on "something you know". U2F is Universal 2nd Factor and is an open authentication standard that strengthens and simplifies two-factor authentication (2FA) using specialized USB, NFC or Bluetooth devices based on similar security technology found in smart cards.

Read More on Troy Hunt's blog

Google Advanced Protection Program

One in five Magecart-infected sites get reinfected within days

Online stores that have been infected with the Magecart malware --known to record and steal credit card details from checkout forms-- often get reinfected after clean-up operations, a recent report has revealed.

Researchers have tracked Magecart-like infections on more than 40,000 domains since 2015. The researcher says that during August, September, and October, his scanner detected Magecart-like card skimming malware on over 5,400 domains. 21.3 percent of the cleaned shops got reinfected. A large number of reinfections occurred within the first day, or after a week, but on average, the reinfection time was 10.5 days.

"This shows that countermeasures taken by merchants and their contracted security firms often fail. There are multiple reasons for this," the researcher said. The expert listed: 1/ Magecart operatives often litter a hacked store with backdoors and rogue admin accounts. 2/ Magecart operatives use reinfection mechanisms such as database triggers and hidden periodic tasks to reinstate their payload. 3/ Magecart operatives use obfuscation techniques to make their presence indistinguishable from legitimate code. 4/ Magecart operatives utilize unpublished security exploits (aka 0days) to hack sites, exploits for which there are no patches. "All in all, it takes some very keen eyes and a lot of effort to clean all traces of a breach," he said.

Read More on ZDNet

How Magecart groups are stealing your card details from online stores

More #News

- A leaky database of SMS text messages exposed password resets and two-factor codes
- Most ATMs can be hacked in under 20 minutes
- Firefox Now Shows Warnings On Sites with Data Breaches
- Hackers Abuse Critical Bug in Microsoft Office Online Video Feature To Deliver Malware
- Misconfigured Docker Services Actively Exploited in Cryptojacking Operation
- Understanding Evil Twin AP Attacks and How to Prevent Them
- Oracle and "Responsible Disclosure"
- Malware of the 90s: Remembering the Michelangelo and Melissa viruses
- Cloudflare's 1.1.1.1 DNS service with DoH now available on iOS and Android
- HTTP/3: Come for the speed, stay for the security
- 7 New Meltdown and Spectre-type CPU Flaws Affect Intel, AMD, ARM CPUs
- Google goes down after major BGP mishap routes traffic through China

#Patch Time!

- Popular AMP Plugin for WordPress Patches Critical Flaw – Update Now
- Patch Tuesday, November 2018 Edition - 63 flaws, including (former) 0-days
- Adobe Published Security Updates for Flash Player, Adobe Acrobat and Photoshop
- Deserialization issues also affect Ruby, not just Java, PHP, and .NET
- ADBHoney: Low interaction honeypot designed for Android Debug Bridge over TCP/IP

#Tech and #Tools

- Kube Hunter: Hunt for security weaknesses in Kubernetes clusters
- The rise of multivector DDoS attacks
- VirtualBox E1000 Guest-to-Host Escape tech details
- Add-ons, Extensions and CSP Violations: Playing Nice with Content Security Policies
- New variant in wp-gdpr-compliance vulnerability and fixing it with virtual patching
- Privilege Escalation in gVisor, Google's Container Sandbox
- Arecibo: an Out of Band exfiltration tool (DNS and HTTP)
- Canarytokens.org - Quick, Free, Network Breach Detection for the Masses
- FCL - Fileless Command Lines
- Building simple DNS endpoints for exfiltration or C2
- XSStrike: Advanced XSS Detection Suite
- How to deploy modern TLS in 2018?
- UAC Bypass by Mocking Trusted Directories

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