kindred

Security Newsletter

26 August 2019

Subscribe to this newsletter

PokerTracker.com Hacked to Inject Payment Card Stealing Script

A curious case of web-based card skimming activity revealed that the Poker Tracker website had been compromised and loaded a Magecart script - code that steals payment information from customers. Online poker enthusiasts use the Poker Tracker software suite to improve their winning chances by making decisions based on statistics compiled from the opponents' gameplay.

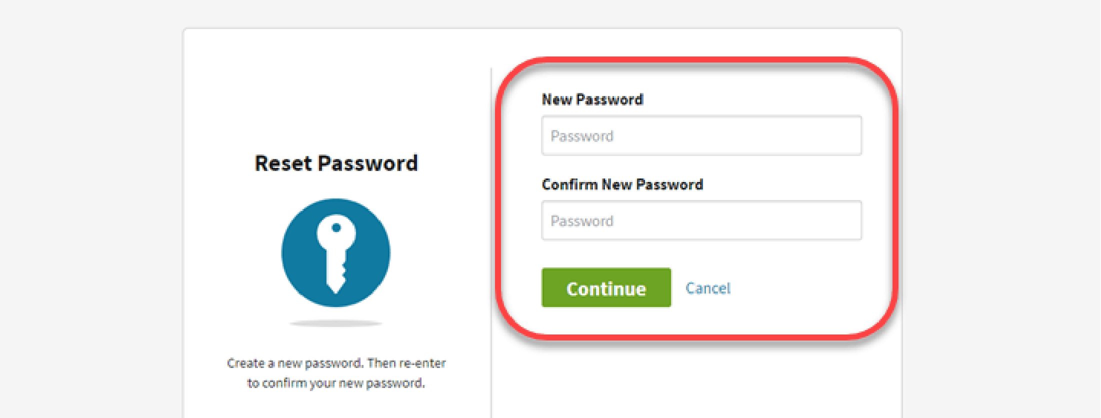
One early theory was that the application had been compromised. This would have been an unusual development for web skimmers since their presence has been observed only on websites. However, a closer look at the software showed that it can load and display web pages from the PokerTracker subdomain 'pt4.pokertracker.com.' Both sources had been hacked and injected with the malicious code causing the software to load it at every launch. Any payment made through the application or its website would copy the attacker with the payment details.

The compromise was possible because PokerTracker.com was running Drupal 6.3.x, an outdated version that has security vulnerabilities. The latest release for the platform is 8.6.17, available since June 17. Looking at the attacker's server, Segura found multiple skimmers all of them customized for each victim. The owners of PokerTracker have been contacted and they acted promptly to fix the problem. Malwarebytes was told that the site has improved the Content Security Policy (CSP), a web security standard that allows controlling the resources loaded for specific web pages.

Read More on BleepingComputer

Even More from Malwarebytes Blog

Forced Password Reset? Check Your Assumptions



Reset Password

Create a new password. Then re-enter to confirm your new password.

New Password

Password

Confirm New Password

Password

Almost weekly now I hear from an indignant reader who suspects a data breach at a Web site they frequent that has just asked the reader to reset their password. Further investigation almost invariably reveals that the password reset demand was not the result of a breach but rather the site's efforts to identify customers who are reusing passwords from other sites that have already been hacked. But ironically, many companies taking these proactive steps soon discover that their explanation as to why they're doing it can get misinterpreted as more evidence of lax security. This post attempts to unravel what's going on here.

The reality is Facebook, Netflix and a number of big-name companies are regularly combing through huge data leak troves for credentials that match those of their customers, and then forcing a password reset for those users. Some are even checking for password re-use on all new account signups. The idea here is to stymie a massively pervasive problem facing all companies that do business online today: Namely, "credential-stuffing attacks," in which attackers take millions or even billions of email addresses and corresponding cracked passwords from compromised databases and see how many of them work at other online properties.

So how does the defense against this daily deluge of credential stuffing work? A company employing this strategy will first extract from these leaked credential lists any email addresses that correspond to their current user base. From there, the corresponding cracked (plain text) passwords are fed into the same process that the company relies upon when users log in: That is, the company feeds those plain text passwords through its own password "hashing" or scrambling routine. If a user's plain text password from a hacked database matches the output of what a company would expect to see after running it through their own internal hashing process, that user is then prompted to change their password to something truly unique.

I can't stress this enough: Do not re-use passwords. And don't recycle them either. Recycling involves rather lame attempts to make a reused password unique by simply adding a digit or changing the capitalization of certain characters. Crooks who specialize in password attacks are wise to this approach as well.

Read More on KrebsOnSecurity

More #News

- Massive MoviePass database found exposed on public server
- Breach at Hy-Vee Supermarket Chain Tied to Sale of 5M+ Stolen Credit, Debit Cards
- Employees connect nuclear plant to the internet so they can mine cryptocurrency
- Chrome devs propose Privacy Sandbox to balance ad targeting and user privacy
- UK cybersecurity agency warns devs to drop Python 2 due to looming EOL & security risks
- Canada's New and Irresponsible Encryption Policy
- Apple, Google, and Mozilla block Kazakhstan's HTTPS intercepting certificate
- Visa Adds New Threat Detection to Prevent Payment Fraud
- Is Apple's Top $1 Million Bug Bounty Too Much?
- One simple action you can take to prevent 99.9 percent of attacks on your accounts
- Cyberbullying: What schools and teachers can do
- 80 suspects arrested in massive business email scam takedown
- Thieves caught using keyless hack to steal £90,000 Tesla in 30 seconds.

#Patch Time!

- Unpatched Squid Servers Exposed to DoS, Code Execution Attacks
- Valve patches recent Steam zero-days, calls turning away researcher 'a mistake'
- Cisco Warns of Public Exploit Code for Critical Switch Flaws
- Bitdefender Fixes Privilege Escalation Bug in Free Antivirus 2020
- Second Steam Zero-Day Impacts Over 96 Million Windows Users
- Microsoft Patches Vulnerable Android Remote Desktop App
- Claroty Releases Free Diagnostic Tool for Urgent/11 Vulnerabilities
- Bumper Cisco patches fix four new ‘critical’ vulnerabilities

#Tech and #Tools

- npm Pulls Malicious Package that Stole Login Passwords
- Backdoor code found in 11 Ruby libraries
- Here We Go Again: A DEF CON 2019 Retrospective
- One Bug To Rule Them All: Modern Android Password Managers and FLAG_SECURE Misuse
- The Imitation Game: Attacker Emulation (Caldera)
- Gaining persistent access to Burp Suite's Collaborator sessions - a step-by-step guide
- Entry #1: Leveraging Osquery For Enhanced Incident Response & Threat Hunting (Free Video Training)
- BitDefender Antivirus Free 2020 - Privilege Escalation to SYSTEM
- AuthCov: Web app authorization coverage scanning.
- DejaBlue: Analyzing a RDP Heap Overflow
- Managing Secrets in AWS using Systems manager (SSM)
- Logging Cheat Sheets

- DeTT&CT: aims to assist blue teams in using ATT&CK to score and compare data log source
- Using osquery for remote forensics
- Deep infrastructure visibility with OSquery and Fleet
- EventList: Combining Microsoft Security Baselines with MITRE ATT&CK and generating hunting queries for your SIEM system

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

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 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 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