kindred

Security Newsletter

4 September 2017

Subscribe to this newsletter

Is your email in the latest cache of 711 million pwnd addresses?

A massive database of 630 million email addresses used by a spambot to send large amounts of spam to has been published online in what appears to be one of the biggest data dumps of its kind.

A French security researcher, who uses online handle Benkow, has spotted the database on an "open and accessible" server containing a vast amount of email addresses, along with millions of SMTP credentials from around the world.

As the researcher explained, he found "a huge list of valid SMTP credentials"—around 80 millions—which is then used to send out spam emails to the remaining 630 million accounts via internet provider's mail servers, making them look legitimate that bypass anti-spam measures.

The exposed database has been verified by Troy Hunt, added the leaked email addresses to his breach notification site. At the time of writing, it is unclear who is behind the Onliner Spambot. Users can check for their email addresses on the site and those affected are advised to change their passwords for their email accounts and enable two-factor authentication if you haven't yet.

Read More

Technical write-up

Have I Been Pwned?

How to buy MacBook for $1, or hacking SAP POS

Security researchers have devised a way to offer steep discounts or steal goods by hacking vulnerable point-of-sale systems.

The researchers at cybersecurity firm ERPScan, which has a commercial stake in the space, found that SAP's point-of-sale (POS) systems don't authenticate or check internal commands, allowing anyone with access to the store's network unrestricted access to the checkout system. That might not be so difficult when various devices and machines around the store are also ethernet-connected, making a plug and play-style attack easier than others.

That access allows the unauthenticated hacker to change prices, set discounts, or take other malicious actions against the systems -- including remotely shutting down the checkout machines, or unmasking credit card numbers.

SAP has since fixed the vulnerabilities and rolled out patches.

Read More

Original write-up

Welcome to 2017: Pacemaker Patients Told to Visit Doctors to Receive Security Patches

Patients with pacemakers manufactured by Abbott — formerly St. Jude Medical's — are advised to reach out to their doctors and inquire about the availability of a security update for their implanted medical devices.

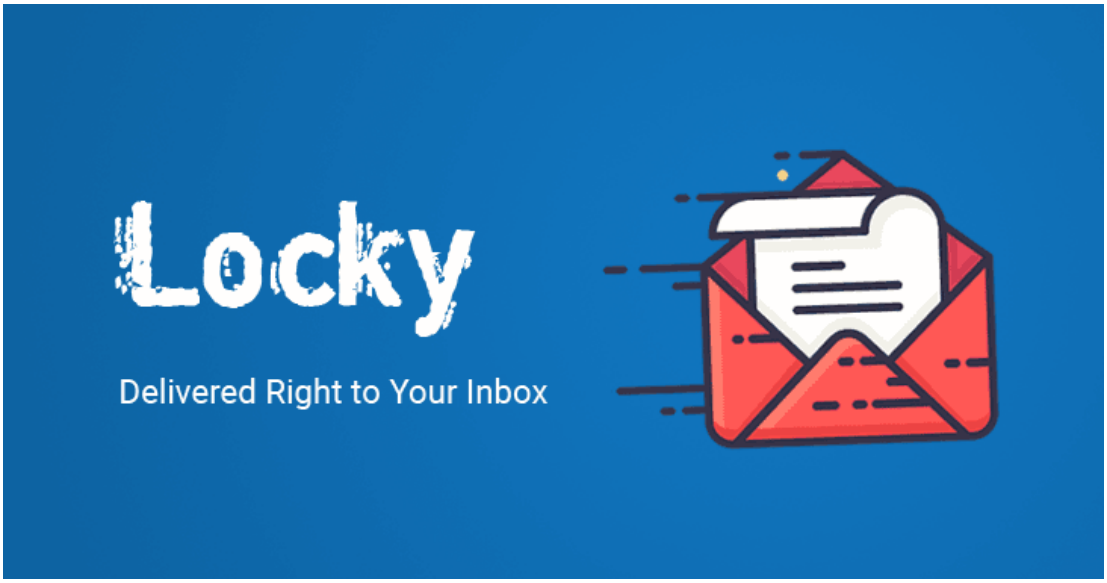
The security update will fix three vulnerabilities discovered last year by MedSec Holdings Ltd.. The flaws are detailed in a security alert issued by the Department of Homeland Security's CERT team. We're talking about a total of 465,000 implanted devices that are affected by the firmware flaws, which leave the devices vulnerable to tampering that could cause them to pace at potentially dangerous rates or fail by rapidly draining their batteries.

Abbott estimates it would take around three minutes for doctors to install the update by placing an RF wand over the pacemaker. Pacemakers manufactured from August 28 2017 will have this update pre-loaded in the device and won't need the update.

Read More

Even More

Massive Email Campaign Sends Locky Ransomware to Over 23 Million Users



Sometimes cyberattacks are incredibly sophisticated. They succeed through careful planning and methodical execution. Other times hackers will launch wholesale attacks, setting as many traps as possible and waiting to see how many people walk into them.

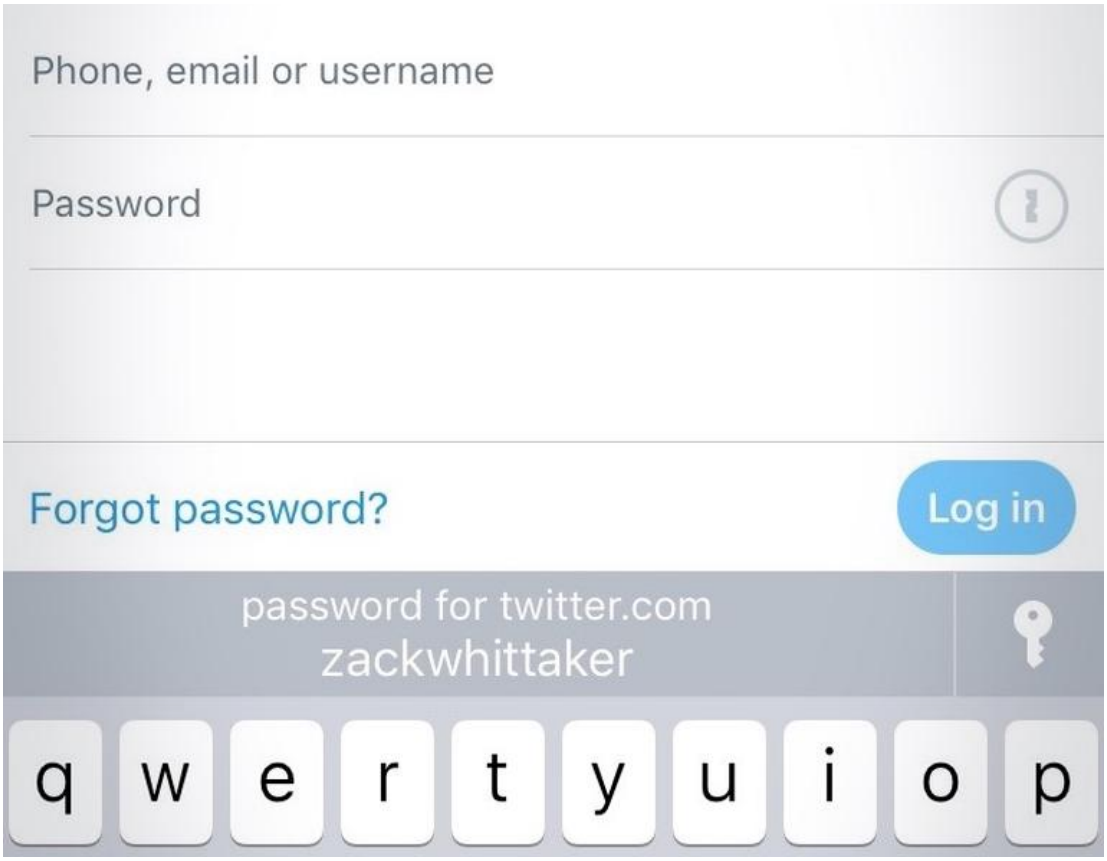
The latter is the approach taken by cybercriminals with a recent email barrage that is spreading a nasty new strain of the notorious Locky ransomware. Security experts at AppRiver have been watching the campaign unfold. In just 24 short hours, their systems have watched the attack fire off a jaw-dropping 23 million infected emails.

The sample email posted by AppRiver looks like minimal effort was put into its creation. The only text in it is the words "download it here" and a bogus sender's name. The subject line of the email is randomly chosen, albeit from a very simplistic list. Most are just one word: documents, photo, images, scans, pictures. The most complex has two: please print. Those are very obvious red flags, but with 23 million potential targets there's bound to be a few ill-advised clicks.

Read More

Even More

iOS 11's most underrated security feature? A password manager



Apple's iOS 11 comes with a new feature that could finally make passwords less cumbersome. The iPhone and iPad software comes with a password manager, which lets users access their account details for apps and websites.

Whenever a login box appears -- including in apps -- a small key-prompt will appear, allowing the user to open their bank of passwords. The password manager is protected by the user's device passcode, or Touch ID if it's enabled, to prevent others from snooping.

Many users new to iOS 11 will find that their password manager already be populated with login information. That's because passwords that were saved in Safari are now stored in the iOS 11's password manager. The key difference is that the saved passwords now work within apps, too.

Although the feature is a boon for personal user security, at the time of writing, the password manager feature doesn't allow users to generate passwords, a feature of most other password managers.

Read More

Webserver hardening: How to install and enable ModSecurity with NGINX

ModSecurity is toolkit for real time web application monitoring, logging, and access control. This open source Web Application Firewall (WAF) module does an outstanding job of protecting web servers (Apache, NGINX, and IIS) from attacks that target potential vulnerabilities in various web applications.

This article walks you through the process of installing both ModSecurity and NGINX, so you can ensure your web server is better capable of standing up against certain attacks.

Read More

Core Rule Set

Git-secret: Store secrets in Git repositories the right way

There's a known problem in server configuration and deploying, when you have to store your private data such as: database passwords, application secret-keys, OAuth secret keys and so on, outside of the git repository. Even if this repository is private, it is a security risk to just publish them into the world wide web.

Storing them separately has a lot of drawbacks. These files are not version controlled. Filenames change, locations change, passwords change from time to time, some new information appears, other is removed. Also, when building the automated deployment system there will be one extra step: download and place these secret-configuration files where they need to be. So you have to maintain an extra secure server, where everything is stored.

How does git-secret solve these problems? Git-secret encrypts files and stores them inside the git repository, so you will have all the changes for every commit. Git-secret doesn't require any other deploy operations rather than git secret reveal, so it will automatically decrypt all the required files.

Read More

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.