kindred

Security Newsletter

05 June 2017

OneLogin Password Manager Hacked; Users' Data Can be Decrypted

OneLogin, an online service that lets users manage logins to sites and apps from a single platform, says it has suffered a security breach in which customer data was compromised, including the ability to decrypt encrypted data.

"Customer data was compromised, including the ability to decrypt encrypted data," reads the message OneLogin sent to customers. According to Motherboard, the message also directed customers to a list of required steps to minimize any damage from the breach, such as generating new API keys and OAuth tokens (OAuth being a system for logging into accounts), creating new security certificates as well as credentials; recycling any secrets stored in OneLogin's Secure Notes feature; and having end-users update their passwords.

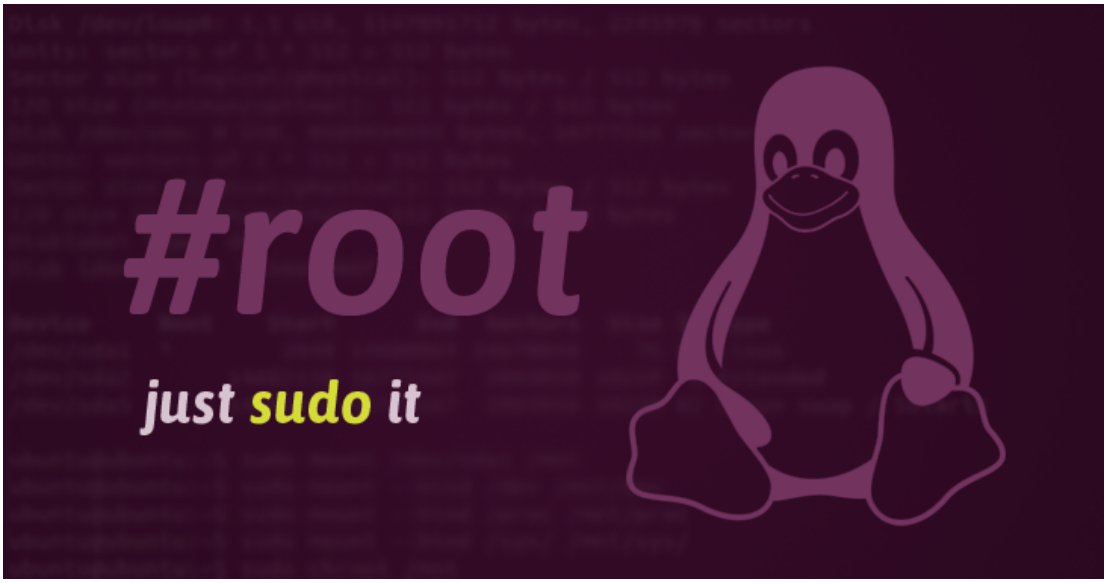
A threat actor obtained access to a set of AWS keys and used them to access the AWS API from an intermediate host with another, smaller service provider in the US. Through the AWS API, the actor created several instances in our infrastructure to do reconnaissance. The threat actor was able to access database tables that contain information about users, apps, and various types of keys. While they encrypt certain sensitive data at rest, at this time they cannot rule out the possibility that the threat actor also obtained the ability to decrypt data.

If they do things correctly, they should have leveraged "Zero Knowledge Privacy" of user data, which means user data is encrypted locally and sent without the key to their servers. If this is the case, the risk of the data being compromised resides in the robustness of the master password. That's why it is so important to use a very long, unique master password for those kind of service, in addition to enforcing 2 factor authentication. You really don't want to be put in a situation where you have to change 300+ credentials in a hurry.

Read More

Even More

Linux Distros Patch Dangerous Vulnerability in Sudo Command



A high-severity vulnerability has been reported in Linux that could be exploited by a low privilege attacker to gain full root access on an affected system. The issue, tracked as CVE-2017-1000367, came to light two days ago when security researchers from Qualys published an advisory on the matter.

Sudo, stands for "superuser do!," is a program for Linux and UNIX operating systems that lets standard users run specific commands as a superuser (aka root user), such as adding users or performing system updates.

Researchers say that an attacker that is in the position to run bash commands can create malformed sudo commands that will allow him to overwrite any file on the system, even root-owned content. In other words, the attacker gains the root-level privileges.

Read More

Technical details

Hacker, Hack Thyself

We've read so many sad stories about communities that were fatally compromised or destroyed due to security exploits. Jeff Atwood from CodingHorror explains that they took that lesson to heart when they founded the Discourse project; we endeavor to build open source software that is secure and safe for communities by default, even if there are thousands, or millions, of them out there.

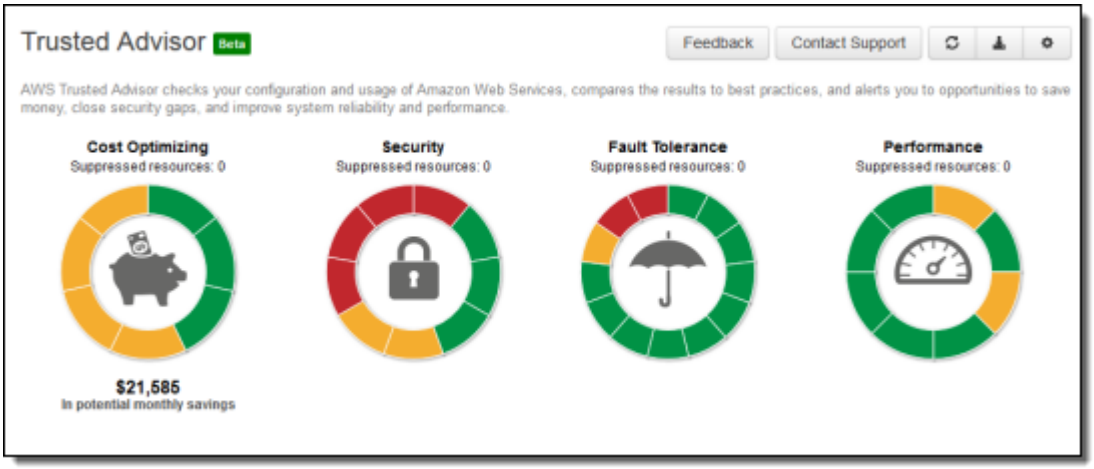
This blog post goes through their default settings for password storage, tries to estimate how hard it would be with modern cracking hardware to find users' password, then verify these assumptions by asking a pentester to cry cracker a 12, 000 users database for 3 weeks.

While we don't know if the pentester was a professional password cracker and knew all the tricks attackers actually use to be efficient at cracking passwords, the results are very encouraging. This leads to thinking that enforcing longer passwords and blacklisting common offenders, such as what NIST is starting to recommend, is the way to go if you really want to protect your user's accounts.

Read More

Previous article about password length

Free tools for auditing the security of an AWS account



Amazon Web Services (AWS) is generally secure by default, but can be misconfigured and the initial setup lacks enforcement of some best practices. This post provides a survey of the existing tools available to help you discover potential security improvements with AWS accounts.

There are three ways to gather information about an AWS account: Make a bunch of AWS API calls to understand how an account currently exists; Monitor CloudTrail logs and alert when potentially concerning changes are made; Use AWS Config logs to understand how an account currently exists. The projects discussed here are all based on making a bunch of API calls.

There currently is not a single tool that includes all of the checks from the other tools, and none of the tools do much for explaining why you should do what the check is looking for, or how to do it. The general advice is first to look at the AWS Trusted Advisor for your account. Do that right now if you've never done it, as it's a built-in service to easily point out security issues quickly to you, along with potential cost savings, performance, and fault tolerance issues. It may even spot storage snapshots that you made publicly available without noticing...

Read More

Introduction to public AWS EBS snapshots

DevOps and SecOps: The Perks of Collaboration

Some proponents see DevOps as a faster path to market. Some feel that DevOps encourages faster innovation. Others suggest that entire organizations can literally move faster by virtue of using DevOps for product development. And still others who even think DevOps is TOO fast. Clearly, it's all about speed.

There's nothing wrong with getting things done fast -- especially in the midst of demanding markets with brutal competition. DevOps provides fantastic results for organizations willing to build their product and IT delivery on the model. Yet, this focus on speed has often resulted in short-shrift being given to proper security practices.

In a 2016 study conducted by digital certificate company Venafi, 79% of CIOs surveyed indicated that they "expect the speed of DevOps to make it more difficult to know what is trusted and what is not." Security and the people who manage it share some culpability in this. SecOps evolves slowly and are often not prepared to address today's cloud-centric world, where security solutions must be agile, lightweight, loosely coupled, and extensible.

Read More

Fireball Malware Infects Nearly 250 Million Computers Worldwide

Security researchers have discovered a massive malware campaign that has already infected more than 250 million computers across the world, including Windows and Mac OS.

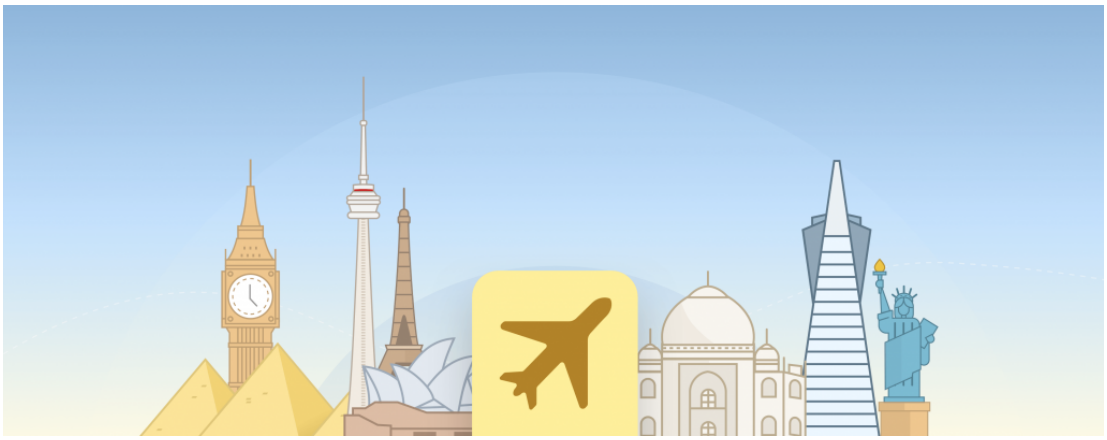
The malware, called Fireball, acts as a browser-hijacker but and can be turned into a full-functioning malware downloader. Fireball is capable of executing any code on the victim machines, resulting in a wide range of actions from stealing credentials to dropping additional malware.

Fireball is spread mostly via bundling i.e. installed on victim machines alongside a wanted program, often without the user's consent. The operation is run by Chinese digital marketing agency. Top infected countries are India (10.1%) and Brazil (9.6%). Details on how to remove the malware as well as IoC are available in CheckPoint's paper.

Read More

CheckPoint's original statement

Digital Privacy at the U.S. Border



The U.S. government reported a fve-fold increase in the number of electronic media searches at the border in a single year, from 4,764 in 2015 to 23,877 in 2016. Every one of those searches was a potential privacy violation.

Our devices carry records of private conversations, family photos, medical documents, banking information, information about what websites we visit, and much more. Moreover, people in many professions, such as lawyers and journalists, have a heightened need to keep their electronic information confidential. How can travelers keep their digital data safe?

Some companies are already taking actions to help their customers protect their secrets, such as 1Password introducing Travel Modes, which wipe all password vaults from your device so that you don't have anything left you may be compelled to hand over to authorities. If you want to go further, you can take a look at the EFF paper.

EFF paper

1Password Travel Mode

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.