kindred

Security Newsletter

9 October 2017

Subscribe to this newsletter

It's 3 Billion! Yes, Every Single Yahoo Account Was Hacked In 2013 Data Breach

If you had an account on Yahoo back in the days of August 2013, then it is most probably one of the 3 billion email accounts that were hacked in one of the biggest data theft feats of that time. It was this particular data hack that forced Yahoo to lower its assets price when it was being sold to Verizon in February 2017 since the buyer lowered the original offer by $350 million.

In December 2016, Yahoo issued a statement that just 1 billion accounts were compromised in the 2013 data hack. But, later the company initiated a thorough investigation in collaboration with Verizon, law enforcement agencies, and cyber-security firms to identify the full scope of the data breach. On Tuesday, Yahoo stated that all the 3 billion accounts on Yahoo, which included Tumblr, Yahoo Email, Flickr, and Fantasy, were hacked after the company became a victim of huge data theft. This is undoubtedly the largest data breach in digital history as far as the size of stolen data is concerned.

Yahoo claimed that the data hacked includes email addresses, names and passwords only and financial information was not stolen. Still, it is unclear who perpetrated the hack attack against Yahoo back in 2013.

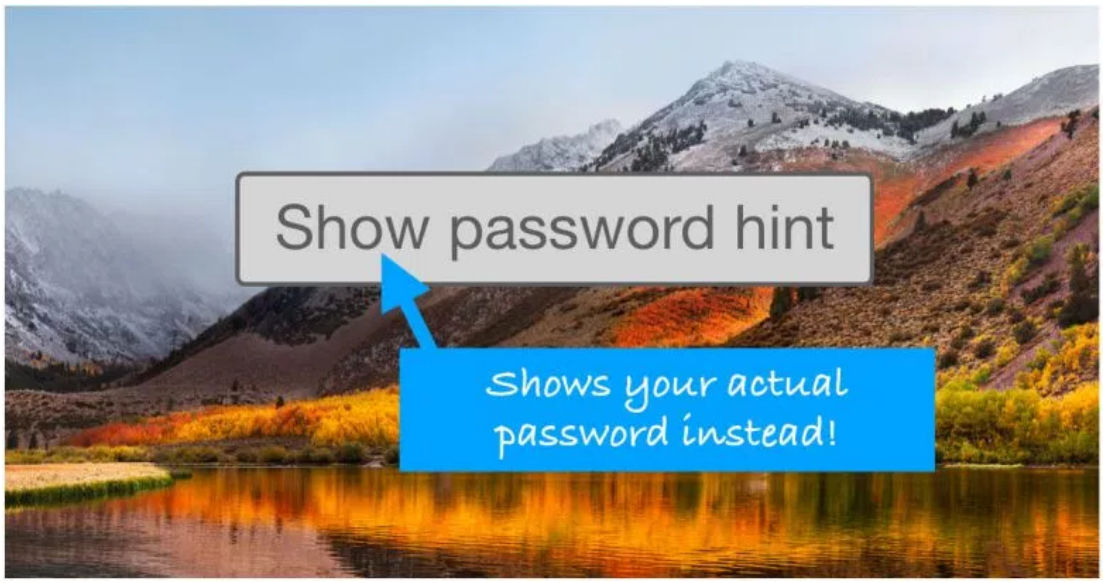
Meanwhile, big three credit bureau Equifax added 2.5 million more victims to its roster of 143 million Americans who had their Social Security numbers and other personal data stolen in a breach earlier this year. At the same time, Equifax's erstwhile CEO informed Congress that the breach was the result of even more bone-headed security than was first disclosed. **Assume you're compromised, and take steps accordingly.**

Read More

Fear Not: You, Too, Are a Cybercrime Victim!

Less Than Half of Consumers Take Protective Steps Post-Breach

Crazy but true – Apple's "show hint" button reveals your actual password



It's only eight days since Apple's latest and greatest macOS 10.13 release, better known as High Sierra. But the first security update has already come out, and we suggest you apply it urgently.

The update is called High Sierra 10.13 Supplemental Update, detailed in the security advisory APPLE-SA-2017-10-05-1. A local attacker may gain access to an encrypted APFS volume. If a password hint was set in Disk Utility when creating an APFS encrypted volume, the password was stored as the hint.

If you haven't created any new APFS encrypted volumes since upgrading to High Sierra, you are OK. If you created an APFS encrypted volume but didn't specify a hint, you are OK. If you created an AFPS encrypted volume using diskutil you are OK. If you upgraded to High Sierra from an earlier version of macOS, your disk will have been converted to APFS, but any hint you had before is left untouched (so far as we can tell), so you are OK. If you had set a hint with Disk Utility, then for all you know someone who knew the [Show Hint] trick might have seen your password, so you ought to change it.

Read More

Apple fixes two High Sierra password bugs

Social Security numbers are 'flawed system,' need modern tech replacement

At a recent cyber conference, White House cybersecurity coordinator Rob Joyce said a replacement for Social Security numbers that could include a 'modern cryptographic identifier. The biggest issue with traditional social security numbers, Joyce said, is that they cannot be changed if they become compromised. He also said that he believed his own Social Security number had been compromised at least four times in his life.

To remedy these issues, Joyce said that the White House is looking into modern alternatives. These could include a "modern cryptographic identifier" Joyce said, which could power a private key-based system, for example. What exactly this could turn out to be, though, remains up for debate. The replacement could include the use of blockchain technology, biometric security, or some other form of identification.

Should we replace the social security number for that purpose? Probably, but that's not easy, either. There are a couple of relevant National Academies reports on questions that need to be answered before any national ID system could be deployed, and Who Goes There? Authentication Through the Lens of Privacy, on the privacy properties of various authentication systems. Basically, running any sort of national identity scheme is hard, and it's not clear that the replacement would have fewer problems than what we have now. Even well-engineered systems, such as the Estonian national ID card, have been reported vulnerable.

What, then, can we do? The problem underlying identity theft is not the existence of social security numbers, but rather, how little authentication is done for a person requesting credit. A digital national ID card could perhaps solve that

Read More

Replacing Social Security Numbers Is Harder Than You Think

Google Finds 7 Security DNS/DHCP Flaws in Widely Used Dnsmasq

Security researchers have discovered a total of seven security vulnerabilities in the popular open source Dnsmasq network services software, three of which could allow remote code execution on a vulnerable system and hijack it.

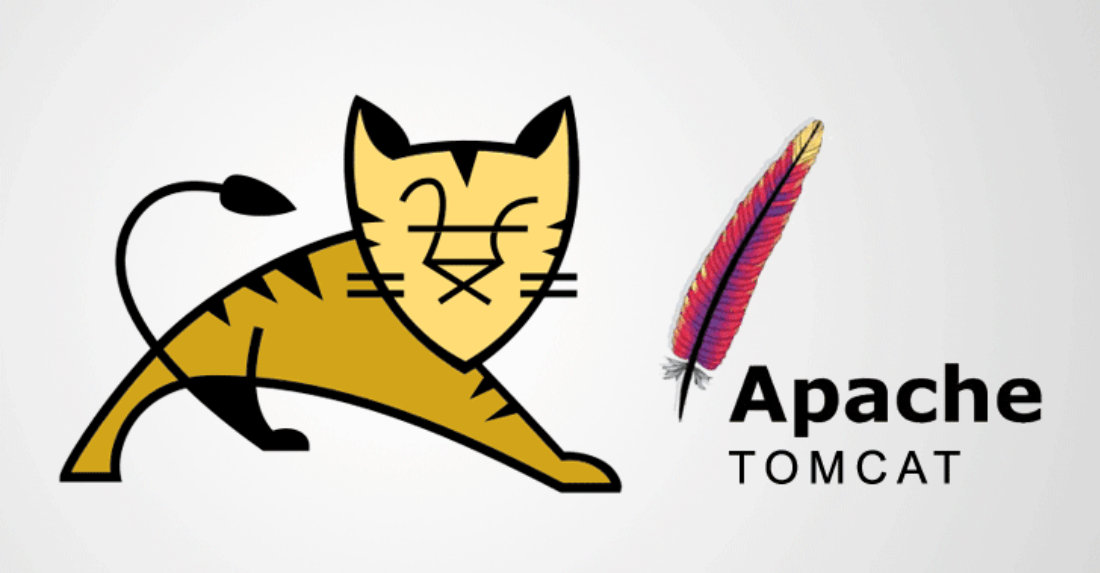
Dnsmasq is a widely used lightweight network application tool designed to provide DNS (Domain Name System) forwarder, DHCP (Dynamic Host Configuration Protocol) server, router ads and network boot services for small networks. Dnsmasq comes pre-installed on various devices and operating systems, including Linux distributions such as Ubuntu and Debian, home routers, smartphones and Internet of Things (IoT) devices. A shodan scan for "Dnsmasq" reveals around 1.1 million instances worldwide.

Since all the issues have already been addressed with the release of Dnsmasq 2.78, Dnsmasq users are advised to update their installations as soon as possible. Proofs of concept are provided so you can check if you are affected by these issues, and verify any mitigations you may deploy.

Read More

Initial statement

Apache Tomcat Patches Important Remote Code Execution Flaw



The Apache Tomcat team has recently patched several security vulnerabilities in Apache Tomcat, one of which could allow an unauthorised attacker to execute malicious code on affected servers remotely. The critical Remote Code Execution (RCE) vulnerability (CVE-2017-12617) discovered in Apache Tomcat is due to insufficient validation of user-supplied input by the affected software.

Apache Tomcat, developed by the Apache Software Foundation (ASF), is an open source web server and servlet system, which uses several Java EE specifications like Java Servlet, JavaServer Pages (JSP), Expression Language, and WebSocket, and provides a "pure Java" HTTP web server environment for Java concept to run in.

Only systems with HTTP PUTs enabled (via setting the "read-only" initialization parameter of the Default servlet to "false") are affected. Exploiting this vulnerability requires an attacker to upload a maliciously crafted Java Server Page (JSP) file to a targeted server running an affected version of Apache Tomcat, and the code contained in the JSP file would be executed by the server when the file is requested.

This RCE vulnerability, marked as "important," impacts all Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81, and has been addressed with the release of Tomcat versions 9.0.1 (Beta), 8.5.23, 8.0.47 and 7.0.82.

Read More

Bug 61542 - Apache Tomcat Remote Code Execution via JSP Upload bypass

Managing PowerShell in a modern corporate environment

Since its incarnation in 2006, PowerShell has grown to be a powerful and extensible management tool, allowing for large-scale automation of system administration and maintenance tasks with ease.

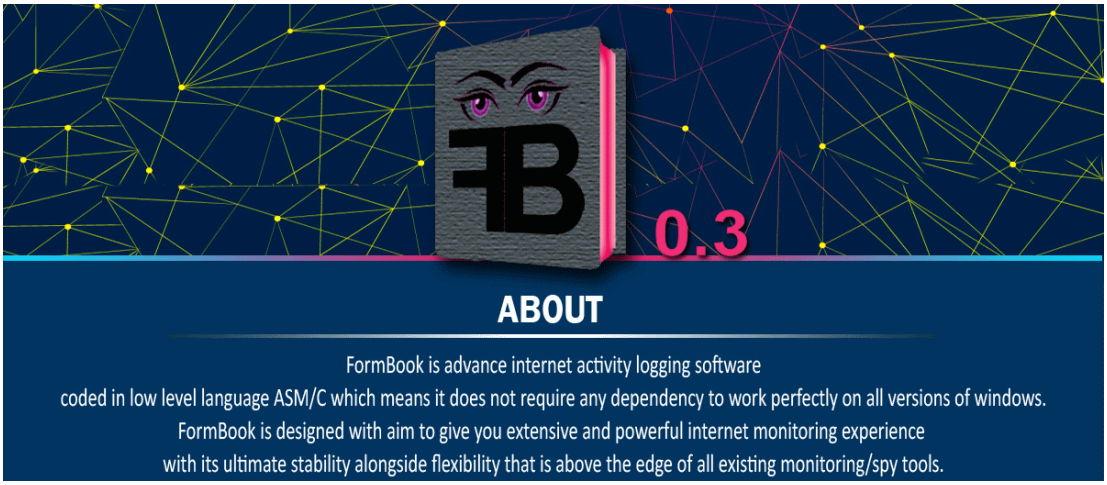
However, analysis by Carbon Black of several breach reports identified that nearly 38 per cent of recent cyberattacks made use of PowerShell in some form. In addition, a large number of affected organisations did not detect the use of PowerShell until it was identified during post-incident response activities. The data gathered by Carbon Black also revealed that social engineering was the favoured delivery technique for malicious PowerShell payloads.

In the Fall of 2016 and Spring of 2017, Daniel Bohannon (@danielhbohannon) released Invoke-Obfuscation and Invoke-CradleCrafter, two open-source PowerShell obfuscation frameworks. The goal of this research and these frameworks was to highlight the limitations of a purely signature-based approach to detecting attackers' usage of PowerShell. The extreme levels of randomization in Invoke-Obfuscation have led defenders to look for a new, scalable means of generically detecting both known and unknown obfuscation techniques. Revoke-Obfuscation is the final hand-crafted product of these efforts.

Read More

Revoke-Obfuscation

FormBook Infostealer Sold on Hacking Forums Is Becoming Quite a Threat



During the past few months, malware campaigns distributing a previously unknown infostealer have ramped up, according to reports by Arbor Networks, FireEye, and the Internet Storm Center (ISC SANS). The malware is named FormBook and has been sold on an infamous underground hacking forum since mid-July.

The malware is not sold as a builder that crooks download on their PCs and use it to create unique FormBook samples, but as a PHP control panel. Users can rent access to a hosted version of this panel, or they can buy it and host it on their own servers. The malware is rented for $29/week, $59/month, and $99/three months. Buying the panel for self-hosted cases costs someone $299.

One of the malware's most interesting features is that it reads Windows' ntdll.dll module from disk into memory, and calls its exported functions directly, rendering user-mode hooking and API monitoring mechanisms ineffective. Most of the emails bearing FormBook malware carry file attachments in a wide variety of formats, such as PDF, DOC, XLS, ZIP, RAR, ACE, and even ISO. The documents either contain links to the FormBook EXE or they drop and execute the malware's binary on infected hosts.

FormBook is neither sophisticated, nor difficult-to-detect malware, so the best way to protect yourself from this malware is to keep good antivirus software on your systems, and always keep it up-to-date.

Cutting room floor

- Myths and Legends of SPF
- New Rowhammer Attack Bypasses Previously Proposed Countermeasures
- PoCs for Two Magento Bugs Released (CSRF+XSS)
- Applied Crypto hardening
- Intro to Return Oriented Programming
- FBI Can Keep Details of iPhone Hack Secret: Judge
- Lay of the Land with BloodHound
- VMWare escapology - How to houdini the hypervisor
- Video Streams Leak What You're Watching to Attackers With Over 95% Accuracy
- Three WordPress Plugin Zero-Days Exploited in the Wild
- Netgear fixes 50 vulnerabilities in routers, switches, NAS devices

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