



Security Newsletter

2 October 2017

[Subscribe to this newsletter](#)

Deloitte Hacked — Exposing Clients' Emails (and their bad security practices)



One of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential emails and plans of some of its blue-chip clients. Deloitte provides auditing, tax consultancy and high-end cybersecurity advice to some of the world's biggest banks, multinational companies, media enterprises, pharmaceutical firms and government agencies.

Deloitte has sought to downplay the incident, saying it impacted "very few" clients. But according to a source close to the investigation, the breach dates back to at least the fall of 2016, and involves the compromise of all administrator accounts at the company as well as Deloitte's entire internal email system.

The source told KrebsOnSecurity they were coming forward with information about the breach because, "I think it's unfortunate how we have handled this and swept it under the rug. It wasn't a small amount of emails like reported. They accessed the entire email database and all admin accounts. But we never notified our advisory clients or our cyber intel clients." This same source said forensic investigators identified several gigabytes of data being exfiltrated to a server in the United Kingdom. The source further said the hackers had free reign in the network for "a long time" and that the company still does not know exactly how much total data was taken.

The breach revealed really poor security practices. A pile of researchers have uncovered worrying security practices at the accounting, audit and consulting firm. These include open ports for fragile services, and clear-text passwords stored in plain sight.

Ironically, Deloitte Touche Tohmatsu Ltd. is (was?) the world's No. 1 security consulting group.

[Read More](#)[Even More](#)

Extreme Vetting: Evaluating The Security Posture Of Third-Party Vendors



We outsource data processing and other work to third parties because of their expertise in a specific area, but not necessarily because of their security capabilities. Is there a way for companies to enforce security standards on service providers?

These types of issues are typically resolved through special contracts. Popular data security standards such as PCI DSS or the NIST 800 series even ask companies to enforce security controls on service providers through legal contracts. For data that falls under data security and privacy laws – say, HIPAA regulations in the U.S. for medical information or EU rules on consumer data like the fast-approaching General Data Protection Regulation (GDPR) – there are additional requirements to have contracts containing specific data protection and privacy provisions. In other words, it's illegal not to have these contracts with outside service providers. If they can't sign the contract, find another provider!

This article will go through useful tips to design proper contract clauses, security controls and SLA clauses you should have with your third parties.

[Read More](#)

How I hacked hundreds of companies through their helpdesk



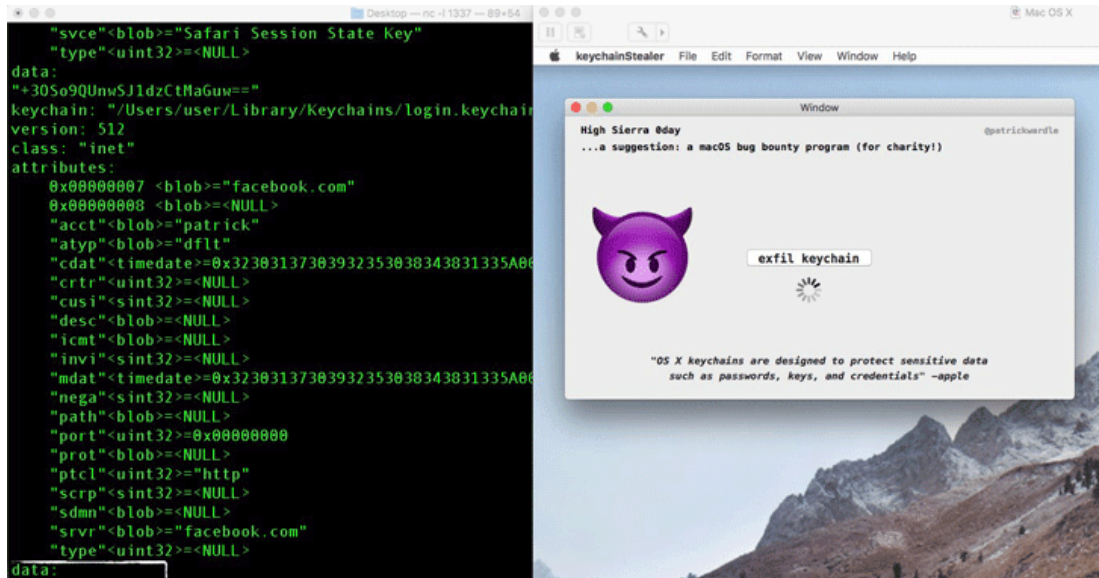
Months ago, the author discovered a flaw hackers can use to access a company's internal communications. The flaw only takes a couple of clicks to potentially access intranets, social media accounts such as Twitter, and most commonly Yammer and Slack teams.

The bug is still out there. It isn't something that can be fixed right away. Over the past few months, he contacted dozens of companies and affected vendors as part of their bug bounty programs in order to get their setup fixed. Due to the number of affected companies it was not possible to contact everyone. On the recommendation of some of his hacker heroes, and with approval of the affected vendors, he's publishing this blog so everyone affected can act immediately. Introducing what he has been calling Ticket Trick.

We need to keep looking for security issues in all possible places. This vulnerability existed for years in hundreds of websites screened by security professionals, but as far as he knows, nobody found it.

[Read More](#)

Apple macOS Exploit Lets Hackers Steal Keychain Passwords in Plaintext



Discovered by former NSA hacker Patrick Wardle, the exploit allows an attacker to steal the entire contents of a macOS Keychain in plain text. To make matters even worse, Wardle was able to steal passwords using an unsigned app downloaded and installed from the internet.

As if a flaw that lets hackers get at the entire contents of your Keychain password vault isn't bad enough, it's not just High Sierra that's vulnerable: Older versions of macOS and OS X can be exploited in the same way. This is just one of the many flaw discovered on MacOS systems recently. Apple recently silently patched a vulnerability that allowed the bypass of the Apple Quarantine and the execution of arbitrary Javascript code without restrictions, iOS is transmitting Exchange credentials in plain text, the Secure Enclave has been hacked, and dozens of iOS apps allow man-in-the-middle intercepts.

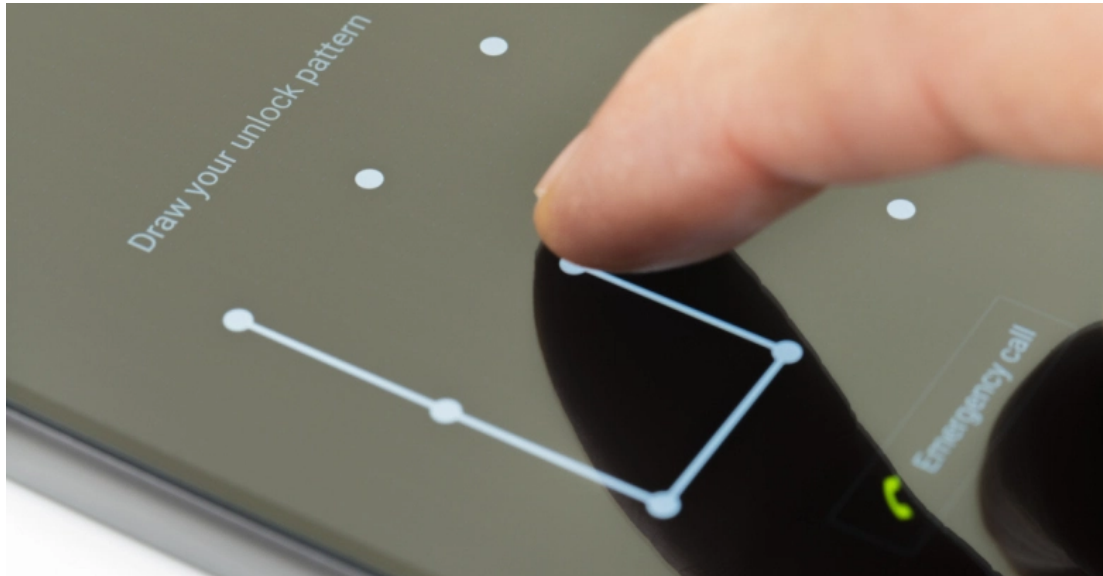
"Every time I look at macOS the wrong way something falls over," Wardle said. He added that Apple marketing has done a great job of convincing consumers that its products are secure. Recent revelations speak to the contrary, though: Apple has a security problem.

[Read More](#)

[Mac OS X Local Javascript Quarantine Bypass](#)

[\[Infographic\] More Mac malware than ever before](#)

Android unlock patterns are too easy to guess



A new report (PDF) from security researchers at the US Naval Academy and the University of Maryland Baltimore County has quantified just how absurdly easy it is to do an over-the-shoulder glance that accurately susses out an Android unlock pattern. In a nutshell: it is far easier for an attacker to shoulder surf a pattern than a PIN.

While there are 389,112 possible patterns you could draw using four to nine nodes, when researcher Marte Løge analyzed 3400 user-selected patterns, she found that the most commonly selected patterns used just four. To make it even worse, most people do swipes in predictable patterns: they go from left to right, top to bottom, typically starting in a corner, often create patterns in the shape of a letter, and rarely backtrack over the space their fingers have already traversed.

The best approach to securing your device is to use the longest PIN it will allow and the shortest lock out time you can stand. But is it feasible? As it is, exhausted users are increasingly just rolling over and playing dead, numbed by alarm fatigue at all the security protocols/security warnings/data getting crowbarred out of companies that can't seem to figure out how to keep their data safe. After all, patterns are better than no protection at all.

[Read More](#)

[Even More](#)

Google Discloses Critical Wi-Fi Flaws Affecting iOS, Android, with PoC for iPhone 7



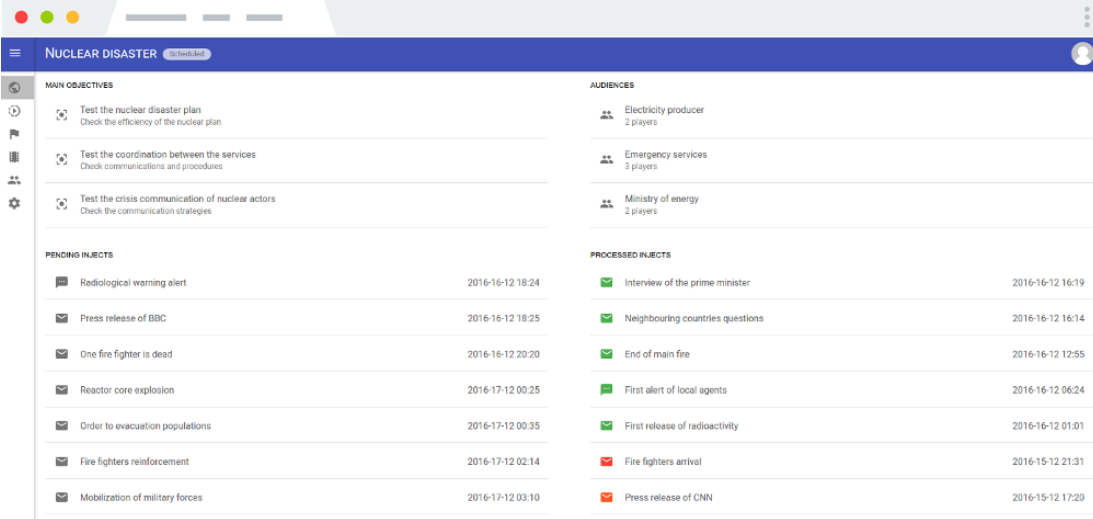
A Google security researcher has published proof-of-concept code for a vulnerability that can be exploited remotely via a WiFi connection to take over iPhone 7. The exploit gains code execution on the Wi-Fi firmware on handset.

The exploit works remotely, no user interaction needed, and can be used to target any user attempting to connect to a rogue WiFi network. While the demo code works on iPhone 7 devices, the vulnerability at the heart of the issue affects a broad range of products, such as Android handsets, smart TVs running tvOS, and other devices with Broadcom WiFi chips.

Apple released security updates for iOS last week. The issue affects all iOS versions but was fixed with the release of iOS 11.

[Read More](#)[Technical details](#)

OpenEX: Open Source Crisis management exercises platform.



The screenshot displays the OpenEX interface for a 'NUCLEAR DISASTER' exercise. It features a sidebar with navigation icons and a main content area divided into several sections:

- MAIN OBJECTIVES:** A list of three objectives with checkboxes and descriptions: 'Test the nuclear disaster plan', 'Test the coordination between the services', and 'Test the crisis communication of nuclear actors'.
- AUDIENCES:** A list of three audience groups: 'Electricity producer', 'Emergency services', and 'Ministry of energy', each with a player count.
- PENDING SUBJECTS:** A table of pending events with timestamps.
- PROCESSED SUBJECTS:** A table of completed events with timestamps.

PENDING SUBJECTS	
☐ Radiological warning alert	2016-16-12 18:24
☐ Press release of BBC	2016-16-12 18:25
☐ One fire fighter is dead	2016-16-12 20:20
☐ Reactor core explosion	2016-17-12 00:25
☐ Order to evacuation populations	2016-17-12 00:35
☐ Fire fighters reinforcement	2016-17-12 02:14
☐ Mobilization of military forces	2016-17-12 03:10

PROCESSED SUBJECTS	
☑ Interview of the prime minister	2016-16-12 16:19
☑ Neighbouring countries questions	2016-16-12 16:14
☑ End of main fire	2016-16-12 12:55
☑ First alert of local agents	2016-16-12 06:24
☑ First release of radioactivity	2016-16-12 01:01
☑ Fire fighters arrival	2016-15-12 21:31
☑ Press release of CNN	2016-15-12 17:20

Software under open source licence designed to plan and conduct exercises. Many builtin features and ISO 22398 compliant.

The events of the exercise scenario are automatically sent by the platform at the scheduled time. The scenario can be played in accelerated speed before exercise to check its sequencing and rhythm. Players can be grouped by audience and receive only the events especially created for them. Checks on the players' means of communication are automatic and can be launched at any time. The available communication vectors are modular: SMS, emails, phone calls etc. Real-time indicators and statistics allow exercise control team to constantly adjust the relevance of the scenario.

[Read More](#)

Cutting room floor

- [Hackers Exploiting Microsoft Servers to Mine Monero - Makes \\$63,000 In 3 Months](#)
- [Mystique, automatically extract malware infection markers](#)
- [Breach at Sonic Drive-In May Have Impacted Millions of Credit, Debit Cards](#)
- [Cisco IOS Software Network Address Translation Denial of Service Vulnerability](#)
- [Patch alert! Easy-to-exploit flaw in Linux kernel rated 'high risk'](#)
- [Permissions Loophole Lets iOS Apps Extract Location Details From Image Metadata](#)
- [7% of All Amazon S3 Servers Are Exposed, Explaining Recent Surge of Data Leaks](#)
- [Dark-Web Drug Dealer Arrested After He Travelled US for World Beard Championships](#)
- [Hacker Hides Backdoor Inside Fake WordPress Security Plugin](#)
- [How I got \\$13337 bounty From Google](#)



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>