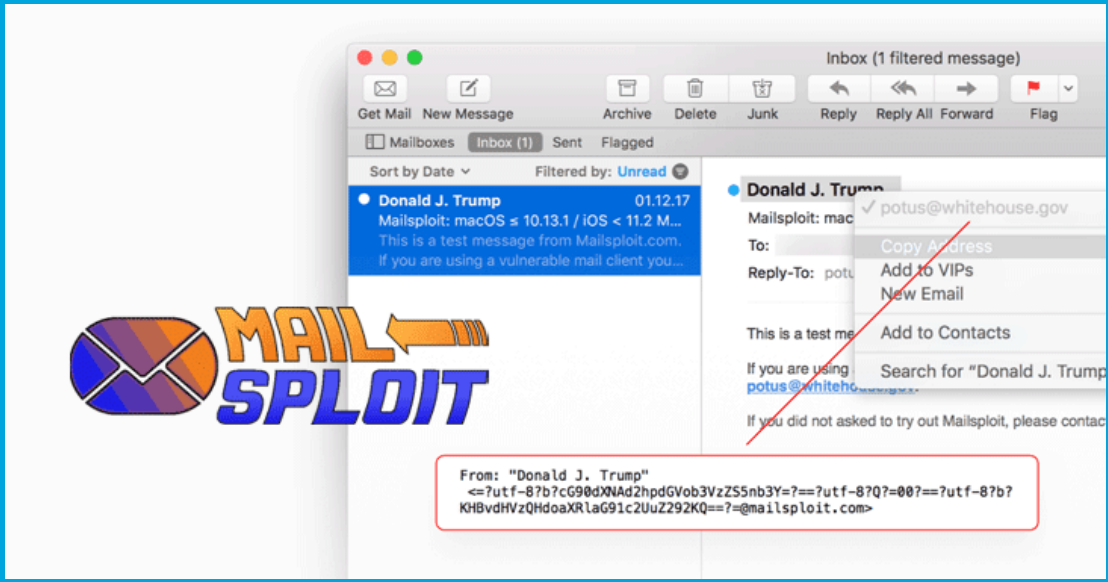
kindred

Security Newsletter

11 December 2017

Subscribe to this newsletter

Mailsploit: It's 2017, and you can spoof the 'from' in email to fool filters



Email identities were really easy to spoof back in the 90s and early 2000s. Changing the “From” header field was enough to make friends believe an email came from their mother, significant other, or even the FBI. There were websites specially made for this purpose. However, those tricks no longer work thanks to anti-spoofing protections such as DMARC (DKIM / SPF) and anti-spam filters. Today, emails with a spoofed “From” field either go to the spam folder or are completely rejected by the server...until Mailsploit.

Penetration tester Sabri Haddouche has reintroduced the world to email source spoofing, bypassing spam filters and protections, thereby posing a risk to anyone running a vulnerable and unpatched mail client.

What he's found is that more than 30 mail clients including Apple Mail, Thunderbird, various Windows clients, Yahoo! Mail, ProtonMail and more bungled their implementation of an ancient RFC, letting an attacker trick the software into displaying a spoofed from field, even though what the server sees is the real sender.

The Mailsploit vulnerability stems from how email servers interpret email addresses encoded with RFC-1342. Haddouche discovered that a large number of email clients would take an RFC-1342 encoded string but wouldn't sanitize it afterward to check for malicious code.

Mailsploit has another nasty side: some trouble ticketing systems (Supportsystem, osTicket and Intercom) are also subject to the bug; and in many mailers, the bug can also be exploited for cross-site scripting and code injection attacks.

Read More

"Official" page

The Trouble with Politicians Sharing Passwords

UK MP Nadine Dorries revealed yesterday that she shares her parliamentary login information with her staff. This was an attempt to defend recently resurfaced allegations about porn allegedly found on fellow politician Damian Green's office computer.

She's certainly not the only one handing her password out to other people. Reading through hundreds of tweets on the matter, there's a defence of "yeah but others do it too". It's important to acknowledge that there's a reason Nadine (and others) are deliberately sharing their passwords with other people. Her challenge appears to be handling large volumes of email. As many people pointed out, there are indeed technology solutions available to solve this problem: access delegation.

The concept of delegation hinges on someone else being able to perform duties on your behalf. How this is done depends on the technology of choice, for example in the Microsoft world there are a couple of ways to grant other people access. Firstly, you can share folders such that another party can access your mail. Now that's not strictly delegation (they can't act on your behalf), but it addresses use cases where someone else may need to access your messages (i.e. a personal assistant).

The frustrating thing for those versed in infosec is that there are plenty of simple technologies to ease password hassles - which are a problem - including password managers, two-factor authentication and more. “I’d like to see proximity card assisted login on MP accounts and computers. You walk away, you’re out. Make the card part of their ID card so they are less likely to ‘loan’ it,” said Rik Ferguson of Trend Micro.

Read More

Even More

New TeamViewer Hack Could Allow Clients to Hijack Viewers' Computer

Do you have remote support software TeamViewer installed on your desktop? If yes, then you should pay attention to a critical vulnerability discovered in the software that could allow users sharing a desktop session to gain complete control of the other's PC without permission.

TeamViewer is a popular remote-support software that lets you securely share your desktop or take full control of other's PC over the Internet from anywhere in the world. To do this, the client has to share a secret authentication code with the person he wants to share his desktop. A GitHub user named "Gellin" has disclosed a vulnerability in TeamViewer that could allow the client (sharing its desktop session) to gain control of the viewer's computer without this code.

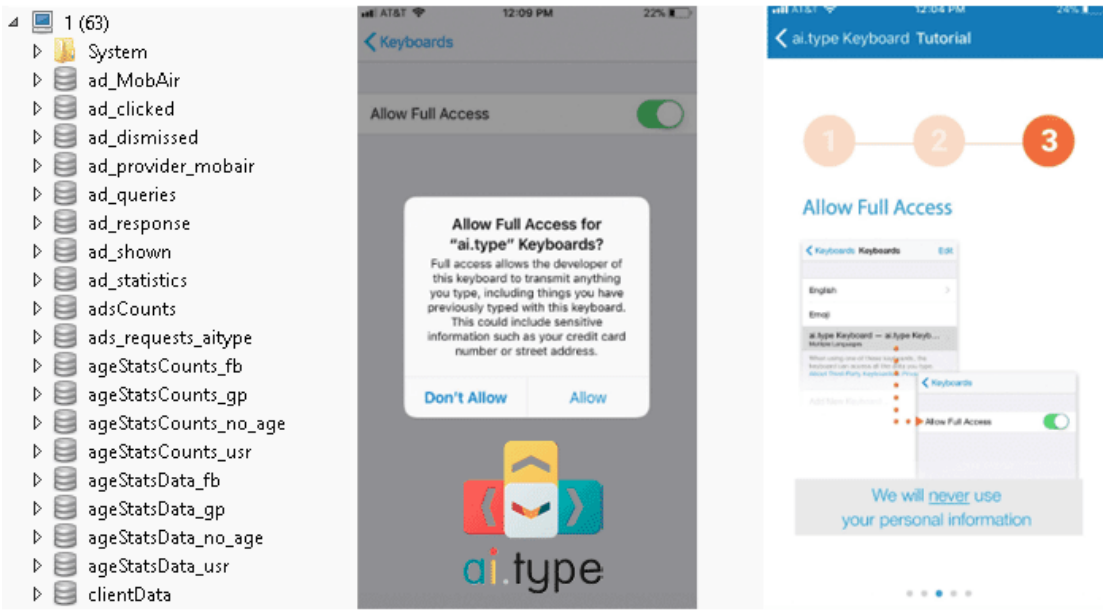
Gellin has also published a proof-of-concept (PoC) code, which is an injectable C++ DLL, which leverages "naked inline hooking and direct memory modification to change TeamViewer permissions." If exploited by the Server—the hack allows viewers to enable "switch sides" feature, which is only active after the server authenticated control with the client, eventually allowing the server to initiate a change of control/sides. If exploited by the Client—the hack allows the client to take control of the mouse and keyboard of the server "with disregard to servers current control settings and permissions."

TeamViewer users are recommended to install the patched versions of the software as soon as they become available. Patches will be delivered automatically to those users who have configured their TeamViewer software to receive automatic updates.

Read More

Proof of Concept

Keyboard app AI.type caught collecting users data after 31M records leaked online



It's just another day with just another breach exposing personal details of unsuspecting users. This time, it's an immensely popular virtual keyboard app called AI.Type whose developers have exposed personal details of over 31 million users.

The database was discovered by security researchers at the Kromtech Security Center who detailed that in total 577 GB of data containing details of 31,293,959 users was left exposed as a result of a misconfigured MongoDB database.

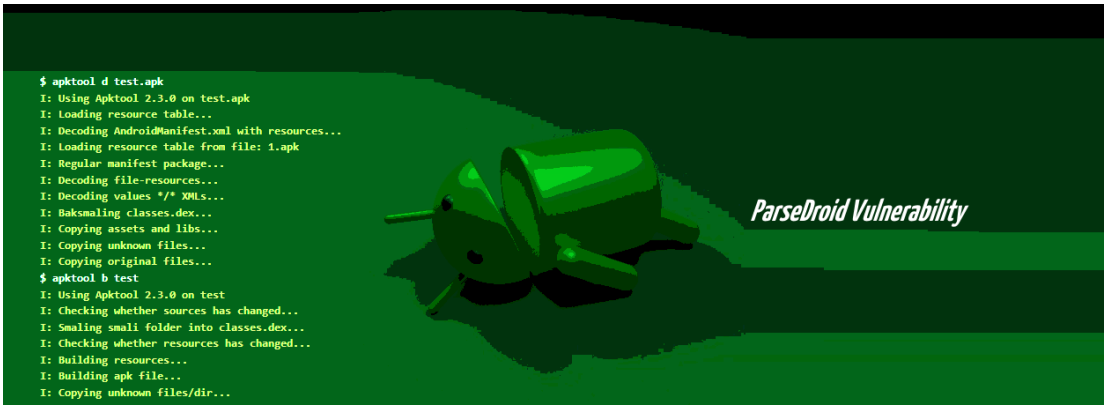
The database accessed by researcher included sensitive details of users such as: Full name, phone number, device name, model number, screen resolution, SMS number, mobile network name, Android version, user languages enabled, IMSI number, IMEI number, country of residence, email address, links and the information associated with the social media profiles including photo and in some cases IP addresses.

According to Alex Kernishniuk, VP of strategic alliances, Kromtech:"It is clear that data is valuable and everyone wants access to it for different reasons. Some want to sell the data they collect; others use it for targeted marketing, predictive artificial intelligence, and cybercriminals want to use it to make money in more and more creative ways. This is once again a wakeup call for any company that gathers and stores data on their customers to protect, secure, and audit their data privacy practices."

Read More

Original statement

Android App Developers at Risk of Attacks via ParseDroid Vulnerability



A vulnerability codenamed ParseDroid affects development tools used by Android app developers and allows attackers to steal files and execute malicious code on vulnerable machines. "The vulnerability exposes the whole OS file system of [affected] users, and as a result, attackers could then potentially retrieve any file on the victim's PC by using a malicious AndroidManifest.xml file," researchers said.

Discovered by security researchers from Israeli firm Check Point, ParseDroid affects the XML parsing library included with projects such as APKTool, IntelliJ, Eclipse, and Android Studio. Researchers discovered that this library does not disable external entity references when parsing an XML file, a classic XML External Entity (XXE) vulnerability that attackers can exploit with ease.

Check Point said it notified the development teams of all affected products and they've all released updates fixing the ParseDroid flaw. Android app developers and security researchers who use these tools to compile or decompile Android APK files should update their IDEs. Regular Android app users aren't affected by the ParseDroid vulnerability.

How Hackers Become You With Credential Stuffing

When you are creating a password for a retail website or banking application, often times you'll be asked for a capital letter, special character, and a number, as an example. But the vast majority of people do not use something such as tXZiXjkBA(6LJCjigbh6K/x}r)qGw2 for their password. More often than not it would be something akin to "OttawaMickey1" which, while containing a capital letter, a number, and a special character – that isn't what the site had in mind when they put those requirements in place.

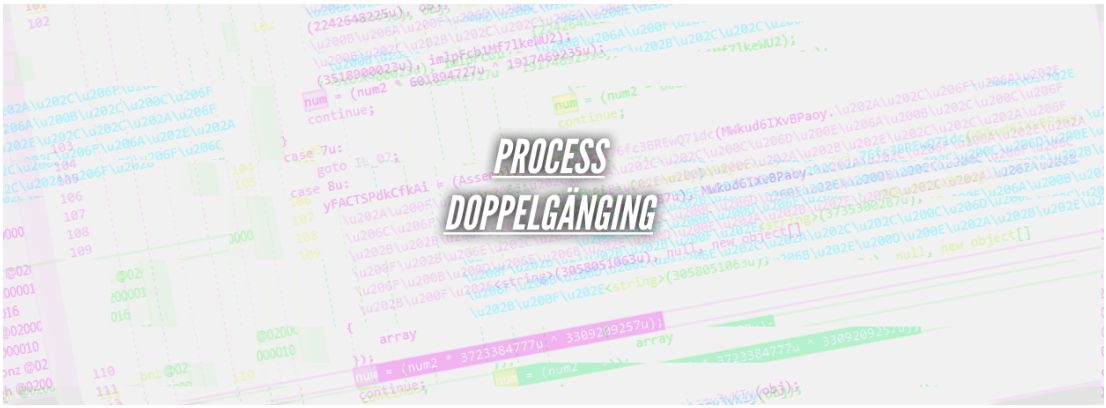
We try to use passwords that we remember. Birthdays, favorite hockey players "Sundin13" or a child's name. This becomes worse when people reuse the same passwords on multiple sites. If your password is Sundin13, as an example, and you use this on your Internet banking site and several retail sites – attackers can become a real problem in the event just one of those sites is compromised. Again, as creatures of habit, people will also use the same email when they create accounts online.

OK, so now the attackers have your email and password from a site they have breached. Now, along with potentially thousands of other accounts, they can take those credentials and supply them into an automated tool. This tool can then run those accounts against a target site to see what credentials will work. If they are able to gain access, your account is now taken over by the malicious attacker. This is an attack typed called credential stuffing.

As a consumer you need to be sure that you are using different credentials for each account that you have online. You can manage these account credentials with a password manager such as Enpass, Keypass, 1Password, LastPass or Dashlane. As an enterprise there is a need for strong authentication controls, monitoring, and control of what kinds of bots are interacting with your site. This will help to reduce the risk of web fraud and lead to having happier customers and a safer bottom line.

Read More

Doppelgänging: How to circumvent security products to execute code on Windows



Researchers have disclosed an attack which exploits processes in the Windows operating system to circumvent all traditional security software and perform code execution attacks.

Process hollowing is the creation of a process for the sole purpose of running a malicious executable inside. In a presentation titled, "Lost in transaction: Process Doppelgänging," the team described a play on process hollowing to circumvent security software.

This technique does not require any files to be created during the process, and it cannot be patched as "it exploits fundamental features and the core design of the process loading mechanism in Windows," according to the team. The team says that not only does the technique work on all major products, but can be launched on all versions of Microsoft Windows -- and can also be used to execute hacking utilities such as password stealers to avoid detection and retain persistence. The attack can also give old malware variants new life by making them undetectable.

"While this technique leverages Microsoft's transaction technology, it is not a vulnerability, but an evasion technique," Liberman told ZDNet. "That being said, we did submit a description of the technique to Microsoft and as they, too, do not deem it to be a vulnerability, they will not address it."

Read More

Presentation's slides

Cutting room floor

- Microsoft Issues Emergency Windows Security Update For A Critical Vulnerability
- Tips for Writing Better Infosec Job Descriptions
- PayPal's TIO Networks breached; PII of 1.6 million users affected
- Are EV certificates worth the paper they're written on?
- First part of phishing with EV
- Introducing AWS Single Sign-On
- PHP Adds Support for Next-Gen Password Hashing Algorithm Argon2
- Slurp: Enumerates S3 buckets manually or via certstream
- Cloudflare[.]Solutions Keylogger on Thousands of Infected WordPress Sites
- Make SSL boring again
- NSA Employee at the Middle of the Kaspersky Saga Admits Taking Files Home
- A Tricky PayPal Phishing Scam That Comes From Official PayPal Email
- Android security alert: Google's latest bulletin warns of 47 bugs, 10 critical
- Ashley Madison Found Leaking Private & Explicit Photos of Users
- How Dropbox securely stores your passwords #Old_NotObsolete
- Apps Can Track Users Even When GPS Is Turned Off #SoDoesGoogle
- Proposed law would jail execs who fail to report data breaches
- EasyCSRF extension for Burp
- PasswordPusher: Self-hostable app to securely communicate passwords over the web
- Google ups Chrome security for business users with new features and policies

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