تقـــــرير

تحليل تقني وأمني بشأن موجة اختراق حسابات واتساب دون استخدام رموز التحقق

إعداد وتحليل: م. معاذ بوشغل

مدير شركة رايد ميدياتيك للحلول الرقمية

مختص في الأمن السيبراني والتحليل الرقمي

التاريخ: 16 أكتوبر 2026

1: موضوع التحليل

تتمثل الظاهرة محل التحليل في الاستيلاء غير المصرح به على حسابات واتساب، وفقدان أصحابها إمكانية الوصول إليها، رغم تأكيدهم عدم استخدام رموز التحقق التي وصلتهم أو مشاركتها مع أي طرف.

في الحالات التي جرى فحصها، لم يقتصر الأمر على تلقي رسائل تحقق غير مطلوبة، بل شمل فقداناً فعلياً للسيطرة على الحسابات، مع ظهور تغييرات في بيانات بعض الحسابات، من بينها إضافة عناوين بريد إلكتروني لا تعود إلى أصحابها.

وتشمل المعطيات المتاحة حالات على أجهزة تعمل بنظامي Android وiOS، وعبر شركات اتصالات مختلفة. كما أفاد عدد من المتضررين باستمرار عمل شرائح الاتصال لديهم، في حين وصلت إلى بعضهم رموز تحقق لم يطلبوها، ثم فقدوا الوصول إلى حساباتهم.

إن المسألة الأساسية هنا ليست إثبات وقوع الاستيلاء على الحسابات في الحالات التي جرى فحصها، وإنما تحديد الخلل التقني في مسار المصادقة أو تسجيل الحساب أو إدارة الوصول الذي أتاح حدوث ذلك.

الاستنتاج المركزي لهذا التحليل هو أن الحالات المدروسة تشير إلى خلل أمني في مسار الوصول إلى الحساب أو التحكم فيه، مع بقاء الآلية البرمجية الدقيقة التي سمحت بالاستيلاء بحاجة إلى تحديد تقني مباشر.

2: تحليل مسار المصادقة وتسجيل الحساب

يعتمد تسجيل حساب واتساب، في المسار المعتاد، على التحقق من ملكية رقم الهاتف باستخدام رمز تسجيل أو وسيلة تحقق أخرى يتيحها النظام في ظروف محددة. كما يوفر التطبيق طبقة إضافية من الحماية تُعرف بالتحقق بخطوتين.

عندما يصل رمز تحقق إلى صاحب الرقم، لكنه لا يستخدمه ولا يشاركه، ثم يفقد الوصول إلى الحساب، يصبح السؤال التقني الأساسي هو: ما الذي سمح بإتمام الاستيلاء على الحساب رغم عدم استخدام الرمز من طرف صاحبه، وفق المعطيات المتاحة؟

من منظور هندسة أمن المعلومات، ينبغي أن يخضع إتمام التسجيل لشروط مصادقة واضحة، وأن يكون الانتقال من مرحلة التحقق إلى مرحلة التسجيل المكتمل مرتبطاً باستيفاء تلك الشروط.

وتشمل مسارات التحقيق التقنية المحتملة:

- خلل في التحقق من استيفاء شروط المصادقة قبل إتمام التسجيل.
- خلل في إدارة جلسة التسجيل أو حالة طلب التحقق.
- وجود مسار بديل للمصادقة لم تُحدَّد آليته بعد.
- خلل في إدارة الصلاحيات أو الانتقال بين حالات تسجيل الحساب واسترجاعه.
- خلل في تطبيق متطلبات التحقق الإضافي ضمن مسار معين.

لا يمكن تعيين أحد هذه المسارات بوصفه السبب النهائي دون بيانات تقنية مباشرة، لكن هذه الاحتمالات تحدد النطاق الذي ينبغي أن يتركز عليه التحقيق.

وعليه، فإن موضع التحقيق الأساسي هو منظومة المصادقة والتحكم في الوصول إلى الحساب، وليس مجرد وصول رمز التحقق إلى هاتف المستخدم.

3: تحليل إضافة عناوين بريد إلكتروني مجهولة

يمثل ظهور عناوين بريد إلكتروني لا تعود إلى أصحاب بعض الحسابات مؤشراً مهماً في تحليل تسلسل الهجوم.

فإضافة بريد إلكتروني إلى الحساب قد تؤثر في وسائل استرجاعه وحمايته، بحسب الوظيفة التي يتيحها النظام لذلك البريد. وإذا أُضيفت بيانات لا يعرفها صاحب الحساب، فهذا يدل على حدوث تغيير غير مصرح به في الحالة الأمنية للحساب في الحالات التي جرى فيها التحقق من ذلك.

ومن الضروري التمييز بين مرحلتين:

1.الوصول الأولي :الآلية التي مكنت الطرف غير المصرح له من السيطرة على الحساب.

2.تثبيت الوصول أو استمراره :التغييرات التي قد يجريها بعد ذلك، مثل إضافة بريد إلكتروني أو تعديل وسائل الحماية والاسترجاع.

قد يكون البريد المجهول وسيلة لتسهيل الاحتفاظ بالوصول أو التأثير في استرجاع الحساب لاحقاً، لكنه لا يثبت وحده أنه كان سبب الاستيلاء الأولي.

ولهذا، فإن التوقيت الدقيق لإضافة البريد، وعلاقته بلحظة فقدان الوصول، من أهم العناصر التي يمكن أن تساعد في تحديد تسلسل الأحداث.

4: دلالة تعدد الأجهزة وشركات الاتصالات

إن تكرار الأعراض عبر أجهزة Android و iOSوشبكات اتصالات مختلفة يرفع أهمية البحث عن عامل مشترك بين الحالات.

وعندما تظهر المشكلة في بيئات متنوعة، يصبح من الضروري فحص المكونات المشتركة في مسار تسجيل الحساب وإدارته، بدلاً من حصر التحقيق في نظام تشغيل معين أو شركة اتصالات بعينها.

كما أن استمرار عمل شريحة الاتصال لدى عدد من المتضررين لا يتفق مع تفسير بسيط يفترض أن جميع الحالات ناتجة عن تبديل الشريحة وحده.

لكن استمرار عمل الشريحة لا يحدد بمفرده الآلية التي أدت إلى الاستيلاء. ولذلك، ينبغي أن يشمل التحقيق مسارات المصادقة وإدارة الحساب، مع فحص احتمال وجود عوامل أخرى بحسب الأدلة المتاحة في كل حالة.

5: رموز التحقق غير المطلوبة واختلاف لغة الرسائل

يشير وصول رمز تحقق لم يطلبه المستخدم إلى وجود طلب أو إجراء مرتبط بالتحقق من الرقم، وفق سياق الرسالة التي وصلت إليه.

لكن المؤشر الأهم في الحالات محل التحليل هو ارتباط بعض هذه المحاولات بفقدان فعلي للوصول إلى الحساب.

أما اختلاف لغة رسالة التحقق عن لغة واجهة التطبيق، فهو ملاحظة تستحق التوثيق والمقارنة بين الحالات. وقد يساعد حفظ النص الأصلي للرسالة، واسم المرسل، وتوقيت الوصول، ومصدر الرسالة الفعلي في اكتشاف أنماط مشتركة.

ومع ذلك، لا يمكن استنتاج موقع الطرف غير المصرح له أو لغة جهازه أو هويته من لغة الرسالة وحدها؛ فقد تتأثر اللغة بقالب الرسالة أو إعدادات الخدمة أو مسار الإرسال.

6: العلاقة المحتملة بالتحديثات الأخيرة

أشار مستخدمون إلى ظهور الحالات بالتزامن مع تحديثات حديثة لواتساب. ويجعل هذا التزامن مقارنة إصدارات التطبيق وتغييرات المصادقة وإدارة الحساب مساراً مهماً للتحقيق.

وينبغي مقارنة أرقام الإصدارات وتواريخ التحديث وتوقيتات الحوادث، والبحث عن اختلافات قابلة لإعادة الإنتاج في السلوك الأمني بين الإصدارات.

ولا يكفي التزامن الزمني وحده لإثبات أن تحديثاً معيناً تسبب في الخلل، لكنه يظل مؤشراً ينبغي أخذه في الحسبان عند تحليل الظاهرة.

7: ما دلالة الحالات المنشورة من مستخدمين آخرين؟

ظهرت على منصات عامة، ومنهاReddit ، منشورات في سبتمبر وأكتوبر 2026 تصف حالات فقدان الوصول إلى حسابات واتساب رغم تأكيد أصحابها عدم مشاركة رموز التحقق، وفي بعض الحالات رغم وجود وسائل حماية إضافية.

تتشابه بعض هذه الإفادات مع الحالات محل التحليل في تتابع طلبات التحقق أو الإشعارات ثم فقدان الوصول إلى الحساب، أو في ظهور بيانات أمنية غير معروفة.

تُعد هذه المنشورات قرائن مساعدة على وجود نمط من الأعراض المبلغ عنها لدى مستخدمين مختلفين، لكنها ليست بديلاً عن سجلات المصادقة أو الفحص الجنائي الرقمي المستقل، ولا تكشف وحدها الآلية البرمجية المسؤولة.

ومع ذلك، فإن تكرار الأعراض في حالات متعددة يجعل مقارنة تسلسل الأحداث ووسائل الحماية والإصدارات خطوة مهمة في تحديد العامل المشترك.

8: دور التحقق بخطوتين في تعزيز الحماية

إلى جانب رمز تسجيل رقم الهاتف، يوفر التحقق بخطوتين (Two-Step Verification) طبقة إضافية من الحماية تهدف إلى جعل الاستيلاء على الحساب أكثر صعوبة.

في مسار التسجيل المعتاد، يُستخدم رمز التسجيل للتحقق من ملكية رقم الهاتف، بينما يضيف التحقق بخطوتين متطلباً أمنياً إضافياً مرتبطاً بالحساب. وبذلك، فإن الحصول على رمز التسجيل وحده لا يكفي بالضرورة لإتمام عملية التسجيل عندما تكون طبقة التحقق الإضافية مطلوبة وفعالة.

وتكمن أهمية هذه الطبقة في أنها ترفع مستوى الصعوبة أمام أي طرف يحاول الاستيلاء على الحساب، خصوصاً إذا تمكن من الحصول على رمز التسجيل بطريقة غير مشروعة.

لكن يجب التمييز بين زيادة صعوبة الهجوم وبين ضمان منعه نهائياً. فإذا كان الخلل المحتمل يمس آلية التحقق الإضافي نفسها، أو يسمح بالانتقال إلى حالة تسجيل مكتملة دون تطبيق متطلباتها، فقد لا تكون هذه الطبقة كافية وحدها لوقف الهجوم.

كما لا يصح افتراض أن كل مسارات التسجيل تتطلب إدخال «رمزين» بالطريقة نفسها؛ إذ تختلف متطلبات المصادقة بحسب حالة الحساب والمسار المستخدم.

وعليه، يوصى بتفعيل التحقق بخطوتين وتحديثه إلى كلمة مرور قوية عندما تكون الميزة متاحة. والهدف هو إضافة حاجز أمني إضافي وتقليل المخاطر، لا اعتبار هذه الخطوة ضماناً مطلقاً ضد الخلل محل التحقيق.

9: التشفير من طرف إلى طرف وحماية المحادثات السابقة

من أكثر المخاوف التي تواجه المستخدم بعد فقدان حسابه السؤال التالي: هل أصبح الشخص الذي استولى على الحساب قادراً على قراءة جميع المحادثات والصور والملفات التي كانت موجودة فيه؟

للإجابة عن ذلك، يجب التمييز بين حساب واتساب نفسه وبين بيانات المحادثات المخزنة على الهاتف.

1.كيف يعمل التشفير من طرف إلى طرف؟

يعتمد واتساب على تقنية التشفير من طرف إلى طرف .(End-to-End Encryption) ويمكن تبسيطها من خلال تشبيه الرسالة بصندوق مغلق لا يستطيع فتحه إلا الطرف المقصود الذي يملك مفاتيح فك التشفير المناسبة.

عندما يرسل شخص رسالة، يقوم جهازه بتشفير محتواها قبل إرسالها. وتنتقل الرسالة عبر الإنترنت وخوادم الخدمة بصيغة مشفرة، ثم يستخدم جهاز المستلم مفاتيح التشفير المناسبة لفكها وعرض محتواها.

وهذا يعني أن الرسالة لا تُرسل عبر الشبكة في صورتها المقروءة العادية، وأن مجرد مرورها عبر خوادم الخدمة لا يمنحها القدرة على قراءة محتواها.

2.أين توجد المحادثات القديمة؟

عندما يستقبل المستخدم رسالة، تُحفظ المحادثة ضمن بيانات التطبيق على جهازه. ويختلف هذا التخزين المحلي عن عملية تسجيل رقم الهاتف على جهاز جديد.

إذا فقد المستخدم إمكانية الوصول إلى حسابه، ثم سجل شخص آخر الرقم على جهاز مختلف، فإن ذلك لا يعني أن قاعدة المحادثات المخزنة على الهاتف الأصلي انتقلت تلقائياً إلى الجهاز الجديد.

بعبارة مبسطة، فإن تسجيل الرقم يتيح الوصول إلى الحساب وفق حالة التسجيل وصلاحياته، لكنه لا ينسخ تلقائياً جميع الرسائل والصور والملفات القديمة من ذاكرة الهاتف الأصلي.

3.لماذا لا يكفي امتلاك الحساب لقراءة المحادثات القديمة؟

لأن قراءة الرسائل المشفرة تتطلب الوصول إلى البيانات والمفاتيح اللازمة لفك تشفيرها. ولا يؤدي تسجيل الرقم وحده إلى توفير مفاتيح فك التشفير الموجودة على الجهاز الأصلي أو استخراج قاعدة المحادثات المحلية منه.

لذلك، فإن فقدان الحساب لا يعني تلقائياً أن المحادثات السابقة أصبحت متاحة للشخص الذي استولى عليه.

4.هل توجد حالات أخرى يمكن فيها الوصول إلى المحادثات؟

نعم. فقد يصبح المحتوى معرضاً للخطر إذا تمكن الطرف غير المصرح له من الوصول إلى الهاتف الأصلي أو بيانات التطبيق ومفاتيحه، أو إلى نسخة احتياطية يمكن استعادتها، أو إلى جهاز مرتبط بالحساب أو مسار نقل للمحادثات.

وتختلف الحماية بحسب إعدادات المستخدم، وحالة الجهاز، وطريقة حفظ النسخ الاحتياطية، وما إذا كانت النسخة الاحتياطية مشفرة من طرف إلى طرف.

ولهذا، يجب عدم الخلط بين الاستيلاء على تسجيل الحساب وبين اختراق الهاتف أو استخراج بياناته؛ فهذه أحداث مختلفة تقنياً.

5.ماذا عن الرسائل الجديدة؟

حتى إذا لم يتمكن الطرف غير المصرح له من قراءة المحادثات القديمة المخزنة على الهاتف الأصلي، فقد يستطيع استخدام الحساب لإرسال رسائل جديدة أو استقبالها وفق حالة التسجيل والأجهزة المرتبطة.

ولهذا، ينبغي تنبيه جهات الاتصال عند الضرورة إلى احتمال انتحال هوية صاحب الحساب، وعدم الوثوق بطلبات مالية أو طلبات معلومات حساسة تصدر عنه خلال فترة فقدان السيطرة عليه.

الخلاصة : فقدان السيطرة على حساب واتساب لا يعني تلقائياً أن المحادثات القديمة والصور والملفات أصبحت مكشوفة. فالتشفير من طرف إلى طرف، إلى جانب تخزين المحادثات على الجهاز، يوفر حماية مهمة. لكن لا يمكن تقديم ضمان مطلق بأن البيانات لن تُكشف عبر أي مسار آخر، مثل الوصول إلى الجهاز الأصلي أو نسخة احتياطية أو وسيلة نقل للمحادثات.

10: الإجراءات الأمنية الموصى بها

للمستخدمين الذين لا يزالون يملكون الوصول إلى حساباتهم

1. تفعيل التحقق بخطوتين وتحديثه إلى كلمة مرور قوية وفريدة عندما تكون الميزة متاحة.
2. إضافة بريد إلكتروني شخصي موثوق والتحقق منه من داخل إعدادات واتساب.
3. إعداد مفتاح مرور (Passkey) إذا كان متاحاً.
4. مراجعة الأجهزة المرتبطة بالحساب وإزالة أي جهاز غير معروف.
5. تحديث الهاتف والتطبيقات، واستخدام قفل قوي للجهاز، وتأمين البريد الإلكتروني المرتبط.
6. تفعيل النسخ الاحتياطي المشفر من طرف إلى طرف عند الحاجة، وحفظ بيانات استرجاعه بطريقة آمنة.
7. عدم تجاهل رموز التحقق غير المطلوبة أو إشعارات التسجيل التي لم يبدأها المستخدم.

تضيف هذه الإجراءات طبقات حماية مهمة، لكنها لا تشكل ضماناً مطلقاً ضد جميع أشكال الخلل الأمني.

للمستخدمين الذين فقدوا حساباتهم

1. محاولة إعادة تسجيل الرقم من تطبيق واتساب الرسمي.
2. عدم مشاركة رمز التحقق مع أي شخص أو إدخاله في صفحات غير رسمية.
3. اتباع تعليمات الاسترجاع الرسمية إذا طُلب رمز التحقق بخطوتين لا يعرفه المستخدم.
4. بعد استعادة الحساب، مراجعة الأجهزة المرتبطة وبيانات البريد الإلكتروني ووسائل الحماية.
5. تنبيه جهات الاتصال عند الضرورة إلى احتمال انتحال الهوية أو إرسال رسائل احتيالية.
6. حفظ لقطات الشاشة والرسائل والتوقيتات ذات الصلة قبل حذف أي دليل.
7. التواصل مع دعم واتساب إذا استمرت المشكلة أو ظهرت مؤشرات على خلل غير معتاد.

11: الخلاصة المهنية

تشير الحالات التي جرى فحصها إلى استيلاء فعلي على حسابات واتساب، مع ظهور تغييرات غير مصرح بها في بيانات بعض الحسابات، رغم تأكيد أصحابها عدم استخدام رموز التحقق التي وصلتهم أو مشاركتها.

وتشير المؤشرات إلى أن التحقيق ينبغي أن يركز على منظومة المصادقة وإدارة الحساب، وبالأخص المسار الذي سمح بالاستيلاء على الحساب ثم إجراء تغييرات على بياناته أو وسائل استرجاعه.

إن تعدد الأجهزة وشركات الاتصالات، واستمرار عمل شرائح الاتصال لدى عدد من المتضررين، وظهور عناوين بريد إلكتروني مجهولة في بعض الحسابات، كلها عوامل تجعل فحص مسارات المصادقة والتسجيل وإدارة وسائل الاسترجاع أولوية تقنية.

أما تحديد المكوّن البرمجي الدقيق المسؤول عن الخلل، أو تسمية الثغرة، أو وصف آلية استغلالها، فيتطلب بيانات تقنية إضافية عن مسار التسجيل والمصادقة. ولا يمنع ذلك من تحديد نطاق التحقيق بصورة واضحة ومواصلة توثيق الحالات ومقارنتها.

التوصيف النهائي للتحليل :حالات استيلاء فعلي على حسابات واتساب تشير إلى خلل في مسار المصادقة أو التحكم في الوصول يستلزم تحديد آليته الدقيقة. وتتمثل الأولوية التقنية في تحليل نقطة الانتقال التي سمحت بالاستيلاء، لا الاكتفاء بتوثيق الأعراض أو افتراض أن مشاركة رمز التحقق هي التفسير الوحيد الممكن.

12: إرشادات عملية للمتضررين لاستعادة الحساب

إذا فقد المستخدم الوصول إلى حساب واتساب، فيوصى باتباع الخطوات التالية:

الخطوة الأولى: إعادة تسجيل الرقم من التطبيق الرسمي

افتح تطبيق واتساب على الهاتف، واختر تسجيل الدخول مجدداً أو متابعة عملية التسجيل، ثم أدخل رقم الهاتف بالصيغة الدولية الكاملة إذا طُلب منك ذلك.

أدخل رمز التحقق المكوّن من ستة أرقام الذي تتلقاه عبر الرسائل النصية أو المكالمة الهاتفية، وفق التعليمات التي يعرضها التطبيق.

وفقاً لتعليمات واتساب الرسمية، تؤدي إعادة تسجيل الرقم بنجاح باستخدام رمز التسجيل إلى تسجيل خروج الأجهزة الأخرى المرتبطة بالحساب.

الخطوة الثانية: إذا طلب التطبيق رمز التحقق بخطوتين لا تعرفه

قد يكون الطرف الذي استولى على الحساب قد فعّل التحقق بخطوتين. إذا لم تكن تعرف الرمز المطلوب، فاتبع تعليمات واتساب الرسمية. وتوضح الشركة أنه قد يلزم الانتظار سبعة أيام قبل إعادة المحاولة في بعض الحالات التي لا يتوفر فيها رمز PIN الصحيح.

لا تشارك رمز التسجيل أو كلمة المرور مع أي شخص، ولا تدفع لأشخاص يدّعون قدرتهم على استعادة الحساب بطرق غير رسمية.

الخطوة الثالثة: التواصل مع دعم واتساب عند استمرار المشكلة

إذا تعذر استرجاع الحساب، أو ظهرت تغييرات غير معروفة في بياناته، أو لم تنجح خطوات إعادة التسجيل، يمكن التواصل مع الدعم الرسمي وإرفاق المعلومات ولقطات الشاشة ذات الصلة عبر القنوات التالية:

- **صفحة استعادة الحساب المخترق:**
https://faq.whatsapp.com/1131652977717250/
- **نموذج التواصل الرسمي مع دعم واتساب:**
https://www.whatsapp.com/contact/?subject=messenger
- **من داخل التطبيق:**
واتساب ← الإعدادات ← المساعدة ← اتصل بنا.

في رسالة الدعم، ينبغي توضيح أن الحساب فقد الوصول إليه دون مشاركة رمز التحقق، مع ذكر رقم الهاتف بالصيغة الدولية، ونوع الجهاز، ونظام التشغيل، وتوقيت الحادث، ووصف التغييرات التي ظهرت على الحساب.

يمكن إرفاق لقطات الشاشة التي توثق رسائل التحقق غير المطلوبة، ورسالة إخراج الحساب، وأي بريد إلكتروني أو جهاز غير معروف ظهر أثناء محاولة الاسترجاع.

قبل إرسال الصور : يجب حجب رموز التحقق وكلمات المرور وأي بيانات حساسة غير لازمة، مع الإبقاء على نص الرسالة واسم المرسل والتوقيت والمعلومات الضرورية لفهم الحادث. ولا ترسل رمز التحقق نفسه لأي شخص يدّعي أنه من الدعم.

ينبغي كذلك تنبيه جهات الاتصال إلى عدم الوثوق بأي طلبات مالية أو رسائل مشبوهة قد تصدر من الحساب خلال فترة فقدان السيطرة عليه.

المراجع

- مركز مساعدة واتساب: كيفية استرداد حساب تم اختراقه https://faq.whatsapp.com/1131652977717250/
- مركز مساعدة واتساب: التسجيل والتحقق بخطوتين https://faq.whatsapp.com/506595211487528/
- التواصل الرسمي مع دعم واتساب https://www.whatsapp.com/contact/?subject=messenger

ملاحظة : يستند هذا التقرير إلى الحالات التي جرى فحصها والمعطيات المتاحة حتى تاريخ إعداده. ويحدد نطاق الخلل الأمني المحتمل ومسارات التحقيق ذات الأولوية، مع بقاء تحديد الآلية البرمجية الدقيقة رهيناً بتوفر أدلة تقنية إضافية.

X

Mouad Bouchghal
Directeur général de la société RYD Mediatech