تعديل مثبّتات Q-Dir وDesktopOK لتوزيع برمجية تحكم عن بُعد مكتوبة بلغة Python



أفادت AhnLab بأن مثبّتات Q-Dir وDesktopOK على موقع SoftwareOK الرسمي جرى العبث بها وتوقيعها، لتنشر برمجية تحكم عن بُعد بلغة Python. وعلى من ثبّت الأداتين أو حدّثهما حديثًا اعتبار جهازه مخترقًا محتملاً.

- قنوات التوزيع الرسمية لأداتي Q-Dir وDesktopOK وزّعت مثبّتات معدّلة، شملت التنزيلات الجديدة وتحديثات النسخ المثبّتة.
- المثبّتات المعدّلة موقّعة رقميًا بشهادة صادرة للمطوّر الشرعي.
- الإصدارات المذكورة: Q-Dir 12.83.0.0 و12.84.0.0 و12.85.0.0، وDesktopOK 12.82.0.0 و12.85.0.0، ولم تكن كل الإصدارات المدرجة مصابة.
- تثبّت البرمجية بقاءها عبر مهمة مجدولة، وتنفّذ أوامر shell وشيفرات Python، وتنقل الملفات، وتلتقط لقطات شاشة، وتبلّغ عن منتجات الحماية المثبّتة.

- لم يتمكن ASEC من تحديد كيفية استبدال المثبّتات ولا المدة التي وُزّعت خلالها.

أكد باحثو مركز ASEC التابع لشركة AhnLab أن مثبّتات أداتين لنظام Windows هما Q-Dir وDesktopOK، الموزَّعتين عبر موقع SoftwareOK الرسمي، تعرضت للاختراق. يطوّر الأداتين Nenad Hrg، وهما ليستا من المنتجات واسعة الانتشار، لكن يستخدمهما مختصو تقنية المعلومات ومديرو الأنظمة والمستخدمون المتقدمون، ما يجعلهما ذات صلة ببيئات المؤسسات.

ما الذي تم رصده

تنشر المثبّتات المعدّلة برمجية تحكم عن بُعد (RAT) مكتوبة بلغة Python. وهي موقّعة رقميًا بشهادة صادرة للمطوّر الشرعي، لذا لا يكفي التوقيع الصحيح وحده دليلاً على سلامة الملف. وقد أُنتجت الملفات الخبيثة عند التنزيل من الصفحة الرسمية وعند تحديث النسخ المثبّتة مسبقًا.

يذكر ASEC أن الإصدارات المتأثرة هي Q-Dir 12.83.0.0 و12.84.0.0 و12.85.0.0، وDesktopOK 12.82.0.0 و12.85.0.0، مع الإشارة إلى أن بعضها فقط كان مصابًا. ونشر قيم SHA-256 للتمييز بين المثبّتات السليمة والخبيثة.

تسجّل البرمجية مهمة مجدولة لضمان بقائها، ويمكنها تنفيذ أوامر shell وشيفرات Python ونقل الملفات والتقاط لقطات الشاشة، كما تجمع معلومات النظام ومنها منتجات الحماية العاملة. وتتضمن قائمة من 1,206 اسم عملية مرتبطة بأدوات مكافحة الفيروسات وEDR، وترسل النتائج إلى خادم القيادة والتحكم.

ما لا يزال مجهولاً

لم يتمكن ASEC من تحديد كيفية استبدال المثبّتات ولا الفترة التي توفرت فيها النسخ الخبيثة. ولم يصل رد من المطوّر على استفسار BleepingComputer وقت النشر.

ينصح ASEC باعتبار أي جهاز ثبّت إحدى الأداتين أو حدّثها حديثًا مخترقًا محتملاً، ويحذّر من أن إزالة الأداتين لا تزيل الـRAT، ولذلك ينبغي فحص الأجهزة بحثًا عن بيئات Python غير متوقعة ومهام مجدولة واتصالات شبكية خارجية.

ما يجب فعله الآن

1. حصر الأجهزة، وخاصة محطات عمل مديري الأنظمة وتقنية المعلومات، التي تحتوي على Q-Dir وDesktopOK وتسجيل الإصدارات وتواريخ التثبيت أو التحديث.
2. مقارنة قيم SHA-256 للمثبّتات بما نشره ASEC وما هو منشور على صفحة التنزيل الرسمية، وعدم الاكتفاء بالتوقيع الرقمي.
3. اعتبار الأجهزة التي ثبّتت الأداتين أو حدّثتهما حديثًا مخترقة محتملاً، وعزلها وبدء إجراءات معالجة الحادث.
4. البحث عن بيئات Python غير متوقعة ومهام مجدولة جديدة واتصالات خارجية غير معتادة، لأن إزالة الأداتين لا تزيل الـRAT.
5. مراجعة بيانات الاعتماد والجلسات ذات الصلاحيات المرتفعة على أجهزة الإدارة المتأثرة وتغييرها عند احتمال انكشافها.
6. تمرير تثبيت الأدوات المساندة من أطراف خارجية عبر عملية معتمدة لإدارة البرمجيات تتضمن التحقق من قيم التجزئة.