April 2026
Issue 04 Volume 16

frogworks

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Fresh Android Devices Infected With Stealthy Backdoor

Have you thought about how secure your company's digital tools really are? Learn more about the recent surge of Android devices infected with stealthy backdoor malware.

Even Brand-New Devices Aren't Safe

Always buy your Android phones, tablets, and laptops from a reputable, manufacturer-approved source.

Researchers from Kaspersky warn that some devices come preinstalled with malicious software that can take over the operating system, steal your data, alter app settings, and more. The particular malware variant involved in these cases is Keenadu, a type of "backdoor" program that allows easy unauthorized access.

An even more alarming discovery stems from hackers also deploying Keenadu at the firmware level, meaning they installed it below the OS and before manufacturers even released the devices on the market.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Fresh Android Devices Infected With Stealthy Backdoor

Why Is This Type of Malware so Dangerous?

A firmware-level Android malware threat can do more damage than the ones deployed through malicious APKs because of the following:

- It's nearly undetectable by traditional antivirus software and endpoint security tools.
- It may persist through complete system reformatting and hard drive replacements.
- Infiltrating the firmware layer grants attackers "root-level" access or better.

The Keenadu Android malware infection, in particular, can access every app installed on the infected device, install new apps from APK files, and unlock all permissions. In other words, all media, messages, banking credentials, and other sensitive information become compromised.

Is Your Business Safe?

How can you tell if you have Android devices infected with stealthy backdoor programs? Kaspersky has identified 13,000 infected endpoints so far, with most located in Japan, Germany, Russia, Brazil, and the Netherlands.

The malware first checks the device's language and time zone. If it finds an association with China, it won't integrate, likely because the threat actors are based there. Some signs you have a preinstalled Android backdoor on new devices include:

- Unexplained device behavior, such as apps crashing or running unusually slow
- Increased data usage without any clear reason
- Unfamiliar applications installed on the device that you did not authorize
- Battery drains faster than expected, even with normal usage
- Suspicious network activity, including connections to unrecognized servers
- Difficulty in accessing certain settings or applications due to restrictions imposed by malicious software

Fresh Android Devices Infected With Stealthy Backdoor

What To Do Next

Kaspersky has already notified the affected vendors, and they are likely working on releasing clean firmware patches. The cybersecurity specialists recommend deactivating all system apps and not using the infected devices in the meantime.

Android Device Security Risks and Protection

Even if your company doesn't operate in the mentioned regions, it never hurts to stay cautious. Regularly update devices, use modern antivirus software, and educate employees on cyber threats.

A proactive approach reduces risks and keeps your company better protected from Android devices infected with stealthy backdoor malware.

Word Search

H G Q H H T X P H T V M P Q U G J D M I
P G Z E S J V M H D C C T L M O V Q A F
S R V C N G Q X P J B X J Z G P B K L O
H U B D L R I W A C A I J Y M N U D W P
S U N Q N V U Y L Y C A J F Q X Y L A L
K B S S D P T B D D K T E E N M L L R I
S L F Y H S P B N M D W B D B T I L E Y
H O D P C I H L E Y O G O C W A Y E M J
U S J S V O N V X L O T W J U V I H U X
Q S H P L A M E X Y R Q D R S N C F N Y
V O C M B D P P F X G A R D E N Q T A W
K M P R D J C Q R M W N G R O W T H U L
L M L Y D M T V P O L L E N X L A F T P
W B B V G P X L A U M D P V N F H U H M
G H P M K P I X K I Z I P D D M Q K O V
U N D S T E A L T H Y B S U J U H O R F
Z C J W T S J A D J F L X E Z W B A I B
S L N R E N E W A L Z O N N D M D B Z D
K S D T X F C Y I Z I O A W M T G Q E Z
F I R M W A R E Y N G M Y A Q J Y Q D W

unauthorized
compromised
backdoor
firmware
stealthy
malware
sunshine
renewal
pollen
growth
garden
blossom
bloom

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter