Hacker Tamagotchi Eats User IDs and Passwords on Wi-Fi Networks

While people use Wi-Fi networks, this hacker version of the virtual pet Tamagotchi steals user ID's and passwords. However, this attack can be stopped.

Actual Tamagotchi Virtual Pet "Egg Watch"

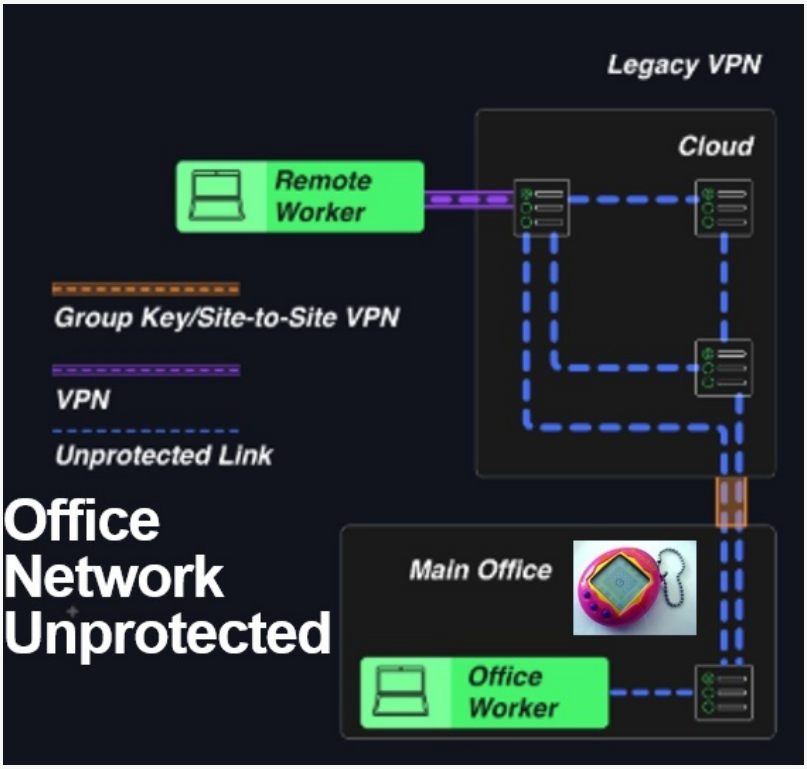
DURHAM, NC, UNITED STATES, November 21, 2025 /EINPresswire.com/ -- One of the latest risks to your identity and data security comes in the form what is being called a “hacker’s Tamagotchi”. This device feeds on capturing the login and passwords of users while a person simply walks around an office, hotel, coffee shop, or airport lounge with this device attached to their backpack or belt. The original Tamagotchi is a brand of handheld digital pets that quickly became a major toy fad. The original Tamagotchi, meaning “egg watch”, is a small egg-shaped handheld video game with an interface consisting of three buttons, with the goal of raising the pet as it goes through different life stages. The owner had to feed it or it would die.

> What is needed to address hacker Tamagotchi’s and other more sophisticated listening devices is to have what is called ‘end-to-end’ encrypted communications”
>
> *Billy Moon, CTO and Founder of WhiteStar.*

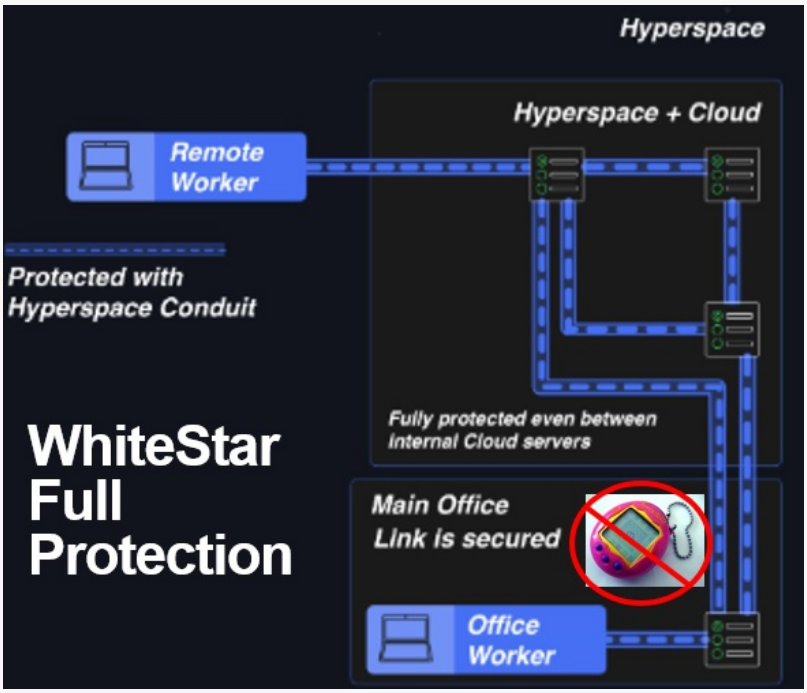
Actual Tamagotchi’s do not collect Wi-Fi data. However, the hacker version passively listens to the data being transferred inside a building between user computers and devices and the router they connect to in order to reach the corporate networks or the internet. What can be done about this?

Security expert, Billy Moon, with over 300 mobile phone and internet patents to his name, explains the issue. “Wi-Fi networks are wonderful things in the home, office, mall or airport. However, they are not inherently secure. Someone with a listening device can capture the most sensitive information, such as passwords.” He continues, “What these hacker Tamagotchi’s do is essentially kick someone off the network forcing their device to automatically log back onto the router to which they were connected. When this ‘handshake’ of user ID and password occurs, the hacker Tamagotchi captures the information.”

This seems incredible that public spaces and corporate offices are so wide open to hacker attacks. Moon explains, “Most networks are like M&M’s. They have a hard shell protecting their perimeter, but they have a soft inside that is unprotected. If you are ‘inside’ the perimeter, then the data flowing over the Wi-Fi can be captured quite easily.” He continues, “Most remote workers use what is called a VPN, a Virtual Private Network, which gives a low degree of security for their connection. However, that protection stops at the perimeter of the network, basically the building’s walls. From that point on their data is unprotected as it travels across the network reaching whatever server they are trying to reach.” Data protection is such a challenge if even using a VPN someone inside a company with a hacker Tamagotchi or more sophisticated listening device can capture not only user ID’s and passwords, but sensitive information as well.



Remote Worker accessing unprotected office



Remote Worker using always on / always secure VPN

Billy Moon is also the founder and CTO for secure network platform provider, WhiteStar Communications that provides network security with its flagship offering, HyperSpace™, to the finance, health care, legal, infrastructure, and defense industries. “What is needed to address hacker Tamagotchi’s and other more sophisticated listening devices is to have what is called ‘end-to-end’ encrypted communications.” WhiteStar provides this capability, and much more, so that whether a person is a remote worker using the internet to reach back into a company or is inside of that company using the Wi-Fi, their data communication is secure. “People think in terms of having a VPN and assume they have security. That’s not the case. VPN’s just provide access. However, with HyperSpace™ it is as if you have an always on, always secure VPN. Whether you

are outside or inside the perimeter of the network the data is always secure."

WhiteStar Communications is empowering societies with trusted, secure, private communications that scale to meet enterprise needs. WhiteStar is based at Research Triangle Park, Durham, NC. It is engaged with enterprises in the finance, health care, legal, infrastructure, and defense sectors. WhiteStar Secure Network Platform (SNP) and HyperSpace™ are WhiteStar's flagship offerings. Learn more at www.whitestar.io or e-mail info@whitestar.io.

James Massa
7039293160 ext.
email us here
WhiteStar Communications
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X
