PewDiePie printer hackers strike again

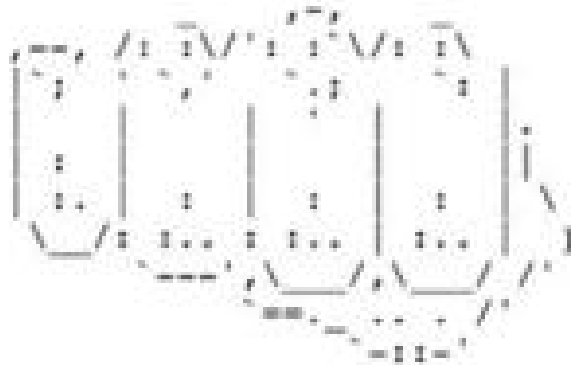By Joe Tidy
BBC Cyber-security reporter

🕐 16 December 2018

Hackers have taken control of printers around the world.

It is the latest in a series of such attacks, but this time they say they have the power to destroy the machines.

The stunt was first carried out last month, when one member claimed to have forced about 50,000 printers to create posters supporting his favourite vlogger PewDiePie.

The latest incident again urges support for the YouTuber, but also calls on victims to improve their security.

"I've been trying to show that 'hacking' isn't a game or toy, it can have serious real-life consequences," the original hacker told the BBC, speaking anonymously online.

"We really want people to pay attention to this because causing physical damage is very much a possibility."

He explained that flaws in the printers' firmware meant that he could continuously force data to be written to their chips.

"These chips have a limited lifetime of 'writes'," he explained.

"If you keep the loop on enough, the chip will fry and the printer will no longer function."

Hijacked files

The potential financial costs to this are obvious but the hacker also pointed to another danger that his stunt has thrown up.

"The fallout goes beyond print-outs, we could also be capturing sensitive documents as they get printed or even modify documents as they get printed."

Although the hacker can geo-locate the countries that he is affecting, it's not clear whether or not a targeted attack on an individual company or household is possible.

> 🐦
>
> My Dymo printer just told me that I need to subscribe to [@pewdiepie](#) but I'm already a subscriber 😂 [pic.twitter.com/Hm7veeyEiO](#)
>
> — Jéssica Llinares (@Thrillka) December 15, 2018

Report

The hackers claim to have printed out their latest message on more than 100,000 machines.

The BBC has not been able to verify the claim, but people from countries including the UK, US, Argentina, Spain, Australia and Chile have posted pictures on social media of the latest print-outs.

More people are expected to notice their printers have created copies of the poster when they return to work on Monday.

It reads: "PewDiePie is in trouble and he needs your help to defeat T-Series!"

The message then instructs readers to subscribe to the YouTuber before adding: "Seriously. Fix your printer. It can be abused!"

PewDiePie has been YouTube's most subscribed to creator since 2013. He currently has about 77 million followers on the platform.

Over recent months, the Indian music label and movie studio T-Series has come close to overtaking his lead, which has led some PewDiePie fans to mount stunts to attract new subscribers.

'Act now'

Security vendors say that the stunt shows just how vulnerable some organisations can be to attack through the plethora of connected devices that fill modern office spaces.

Their advice is to:

- carry out regular audits of connected devices

- install the latest security patches

- question whether or not everything connected to the internet really needs to be

"The risk of causing financial damage in this case is as real as it gets," commented Bob Reny from the security firm ForeScout.

"And all of this because organisations or individuals installed a connected device without really taking the time to audit the implications this has on their existing network security infrastructure."

The hackers provided contact details on the latest print-outs as a way to allow people to get in touch if they needed further help fix the exploited flaw.

One told the BBC that they believed they were breaking the law, but still thought their act was justified.

"While authorities might not see eye to eye with us, what we're doing is much better than someone destroying printers and offices around the world in an attempt to hold printers ransom or something."

Vulnerabilities in network printers have been known about for years but many people are unaware of the risks.

One security researcher who has studied the problem confirmed it was possible to destroy the machines by sending them commands from afar.

"These devices should never be directly reachable over the internet," said Jens Mueller from Ruhr-University in Germany.

"Who is to blame? [In offices] definitely the network administrators allowing direct access to their devices over the internet."

Related Topics

Cyber-security	YouTube	Cyber-attacks

Share this story About sharing

More on this story

PewDiePie in battle with T-Series to keep top YouTube spot
3 December 2018

Smart device security guidelines 'need more teeth'
7 March 2018

How 'the invisible network' poses a major security threat
22 September 2017

Related Internet links

Ruhr University

The BBC is not responsible for the content of external Internet sites