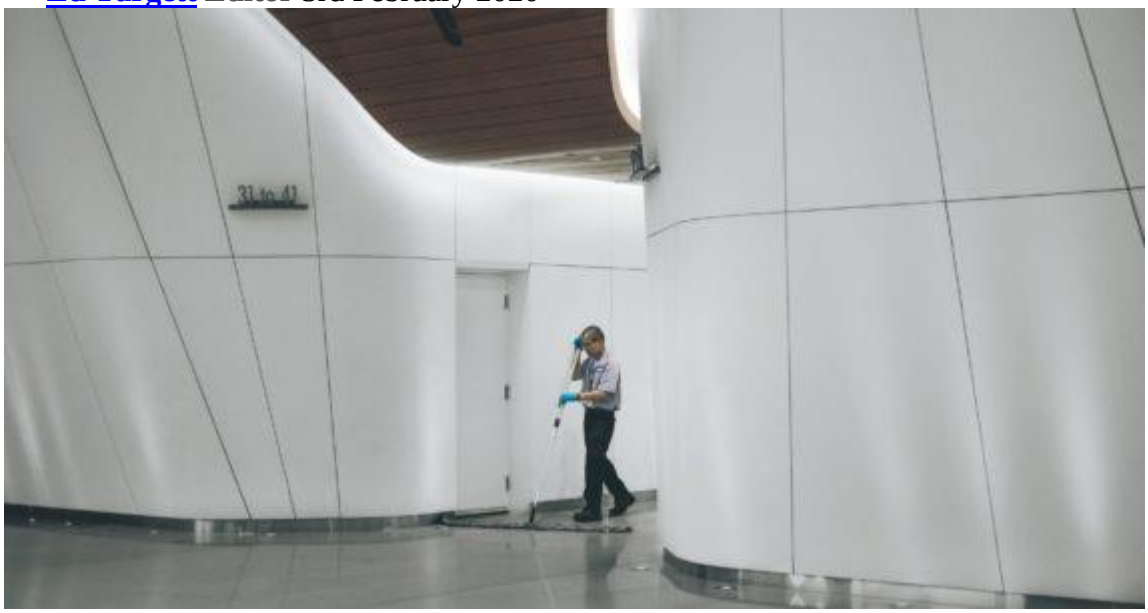
Accessed on 21/10/20: https://www.cbronline.com/cybersecurity/threats/cyber-criminals-cleaners/

Police Warning: Cyber Criminals Are Using Cleaners to Hack Your Business

- **Ed Targett** **Editor** 3rd February 2020



"They think we'll go to the ICO. We won't!"

Criminal gangs are planting "sleepers" in cleaning companies so that they can physically access IT infrastructure, a senior police officer with responsibility for cyber crime has warned, urging businesses to bolster their physical security processes in the face of the growing threat.

Shelton Newsham, who manages the Yorkshire and Humber Regional Cyber Crime Team, told an audience at the SINET security event that he was seeing a "much larger increase in physical breaches" as cyber crime groups diversify how they attack and move laterally inside institutions.

(Recent reports suggest that cybercrime will cost firms $6 trillion annually by 2021 – making it more profitable than the global drugs trade.)

Cleaners and USB Sticks

"Exploitation of staff is a key area", Newsham said.

"Organised crime groups are planting 'sleepers' in cleaning companies that a procurement team may look at bidding for. There's no way of auditing their vetting. They'll also using people in painting and decorating firms; anyone who has out-of-hours access to a building is fair game.

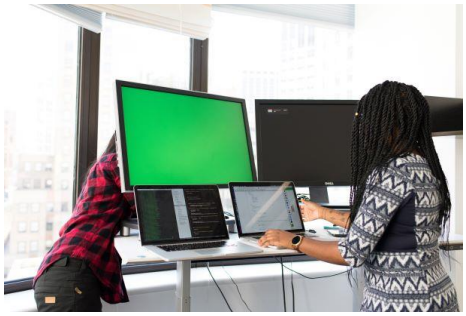
“Even the old ‘drop a USB stick’ is back.”

(Newsham was referring to the technique of lacing a USB stick with malware, dropping it in an office car park and waiting for a curious staff member to plug it in).

Badges and Biometrics

One senior CISO added: “Over last few years, cyber criminals are really ramping up how organised they are. They can get through your vetting and recruitment processes to get inside your organisation.

“Regular red teaming and purple teaming; capture the flag exercises [all help]”, biometrics too, although there’s no point having cutting edge systems running on an old Windows server.”



They added: “Culture and process are really central. In my career I’ve seen so many people under desks lifting stuff out and nobody saying ‘hello, who are you?’”

It was a point echoed by physical intrusion specialist Tim Roberts of wehackpeople.com, who told Computer Business Review in a DM: “Data mediums may change, but physically accessing said data or the threat of safety will not.

“Typically weaknesses are due to the human element and social engineering risks. You can have the most expensive access controls, but improper deployment or a poor security culture can and often is the window in (tailgating, being let in, bypassing electronic access via physical methods etc).”

He added: “Security awareness should be a culture, not just a process or annual training. Improved technology does not matter if the previous statement stands. The human elements rarely changes.”

Read this: "Think 'Evil', But Get the Scope Crystal Clear"

In the UK agency-level cooperation has vastly improved, as has the ability of the police to respond fast to cyber intrusions, most agreed.

But it takes two to tango.

The Achilles Heel…

As Shelton Newsham (who operates as one of 12 "spokes" of the NCSC at the regional cyber crime level) told Computer Business Review on a later call: "Communication with corporations is still the Achilles heel. People aren't proactive in coming to us when there's been a breach. They think we'll go to the ICO. We won't! That's your responsibility."

He added: "These criminals almost have daily meetings with set objectives, and people are held responsible if these aren't met.

"Security teams might meet up fully once a month: they're already 30 days behind. With cyber criminals consistently pushing for access, for lateral movement, it's very hard for CISOs to stay on top of this.

"But it's a basic: with any procurement, is there a strict policy in place about who has access to the building? Is the policy and the service level agreement that goes along with it audited, so we can vet it? One of my teams can do an audit of that every three months."

Business can report live cyber crime to Action Fraud, 24/7.

This goes to a central repository that police and other government agencies use to understand and respond to real-time attacks around the country.

https://www.actionfraud.police.uk/