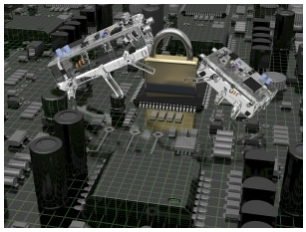
20% of cyber-attacks attributed to Conficker worm

20% of cyber-attacks attributed to #Conficker worm

Detected in everything from police body cameras to the business internet of things (IoT) landscape, now do you give a configuration fick?



The notorious Conficker worm has been gaining an ever-wider reputation for destruction. Last month SCMagazineUK.com reported on this comparatively old malware's presence as it started to appear pre-installed inside police body cameras.

Not content with infecting the security forces' use of Internet of Things devices, Conficker has continued to turn its venom towards the business landscape in general. October of this year saw Conficker ranked by security vendor Check Point as the most common malware used to attack British and international organisations.
Check Point suggests that as many as 20 percent of all attacks globally can be attributed to Conficker in the period identified.
Also known as by the name Downadup, Conficker was first identified as far back as 2008. It targets the Windows operating system and can form a botnet to infect a computer and spread itself to other machines across a network automatically, without human interaction.

Undead, still walking

As noted on The Register, networks belonging to the French Navy, the British House of Commons and Greater Manchester Police were all laid low by the malware. "Its recent resurgence hasn't caused anything like the same amounts of problems but still highlights the generally poor state of corporate security," wrote John Leyden.

How does the Conficker worm spread?

Microsoft's own advisory states that the Conficker worm spreads by copying itself to the Windows system folder. The firm notes, "It might also spread through file sharing and through removable drives, such as USB drives (also known as thumb drives), especially those with weak passwords."

What marks Conficker's resurgence now, in the dying days of 2015, is not only its brute-force attack ability on passwords but also its longer term ability to still cause impact. As botnets and remote control PC attacks now still grow, the prevalence of ransomware and data-stealing malware also continues to rank highly among the reported threats as measured by the security industry.

Common tools democratise hacking

Fraser Kyne, principal systems engineer at Bromium contacted SC to say that the use of common tools in this way democratises hacking, as it provides a framework for mounting similar attacks across a range of vectors.
"Re-purposing the tools of the past is a simple model for attackers, and one that is difficult to detect. We see some vendors claiming to be able to look for telltale signs of these models – but realistically they're playing a losing game where the attacker is always several steps ahead," said Kyne.
As a related note, Bromium Labs has recently blogged on the resurgence of malware that uses macros in Office documents, particularly Dridex. In this sense, malware is analogous to malaria. As vaccines become available, the disease morphs.
"The only practical (and sustainable) model for defending against malware is isolation. This needs to be done outside of the operating system. Modern hardware has the capability to do this securely, efficiently and invisibly for the user – and we're seeing proof of the success of this approach. In this model, the mosquito bites a crash test dummy, not the real user, and there's no impact to the business," he said.

Actually, you're failing miserably

Richard Cassidy, technical director EMEA, Alert Logic told SC that the proliferation of Conficker highlights organisations' continuing failure across the board to get it right when it comes to key security practices and policy enforcement.
"With the plethora of incredible security technologies today, from network access control to micro-visor security containers at the host process level, through to big data analytics platforms, all poised to detect advanced malware variants of C2C, botnet and remote control infection, it is a wonder therefore that organisations (including governments) are not only being successfully infected with malware, but also for inordinate periods of time before detection," said Cassidy.
He surmises that ultimately we have to assume that we will be infected, even if we manage to get all the required parts aligned.
"With this mindset, therefore, we will drive better protection of key data assets from being easily compromised and will work to ensure we are better poised to detect compromise activity, should a particular user not have adhered to a 'no-download' policy from untrusted sources," he said.
This article originally appeared on SC Magazine UK.

Réagissez à cet article
Source : http://www.scmagazine.com/20-of-cyber-attacks-attributed-to-conficker-worm/article/458392/