DeMISTIfying Infosec: War Dialing

February 16, 2016

@katherinert15

By Katherine Teitler(https://twitter.com/@katherinert15)

War Dialing

War dialing, also known as "demon dialing" was a hacking technique that emerged in the late 1980s as a method for attackers to identify unauthorized or non-secure modems within an enterprise that provided access the company's voice or data network or its Intranet. Originally a manual process (think: prank calling when you were a kid), technologies rapidly evolved and new software allowed attackers to automatically scan a large block of random telephone numbers for unprotected user names or passwords. Some of the programs used in war dialing would also automatically log and enter successful connections into a database when they were found so attackers could return at a later time to leverage unauthorized access.ense in depth is a practical strategy for achieving information assurance in today's highly networked environments (https://www.nsa.gov/ia/_files/support/defenseindepth.pdf), as defined by the NSA, which first applied the long-standing military strategy to

network security. The basic premise of defense in depth is that layering security controls within a computing environment helps slow down an attacker's progress should s/he gain access.

The goal of war dialing was to weaken the security of enterprise voice and data networks or find a backdoor into the company's Intranet, which might be chock full of proprietary or sensitive information.

Used throughout the '90s (and purportedly named after the movie "WarGames (http://training.misti.com/acton/ct/10465/e-116b-1602/Bct/g-036f/l-tst:1/ct12_0/1?sid=lCgV5ii7Q)" starring Matthew Broderick), war dialing died off after the Telecommunications Consumer Protection Act of 2003 (http://training.misti.com/acton/ct/10465/e-116b-1602/Bct/g-036f/l-tst:1/ct13_0/1?sid=lCgV5ii7Q) was passed. Around that time, the use of modems in enterprises also started to wane (though many security professionals might be surprised to find a rogue connection or two still in use), and the attack morphed into scanning for VoIP systems that might be connected to the Internet through the same physical Ethernet cables and switches as networked computers or servers.

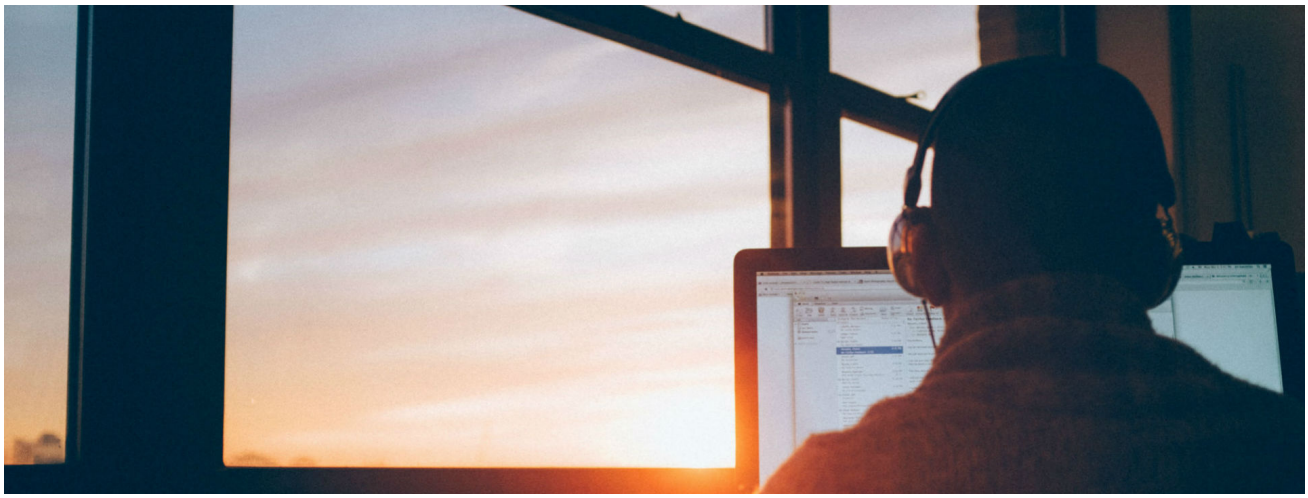
While war dialing is long since thought of as a legacy type of attack, security teams should consider including it as part of regular vulnerability scanning and penetration tests (http://training.misti.com/acton/ct/10465/e-116b-1602/Bct/g-036f/l-tst:1/ct14_0/1?sid=lCgV5ii7Q). The "new" war dialing is "war driving," the act of locating and exploiting vulnerable wireless access points.

Katherine Teitler

Katherine Teitler is an industry thought leader and the current Director of Content for Edgewise Networks (https://www.edgewise.net/).

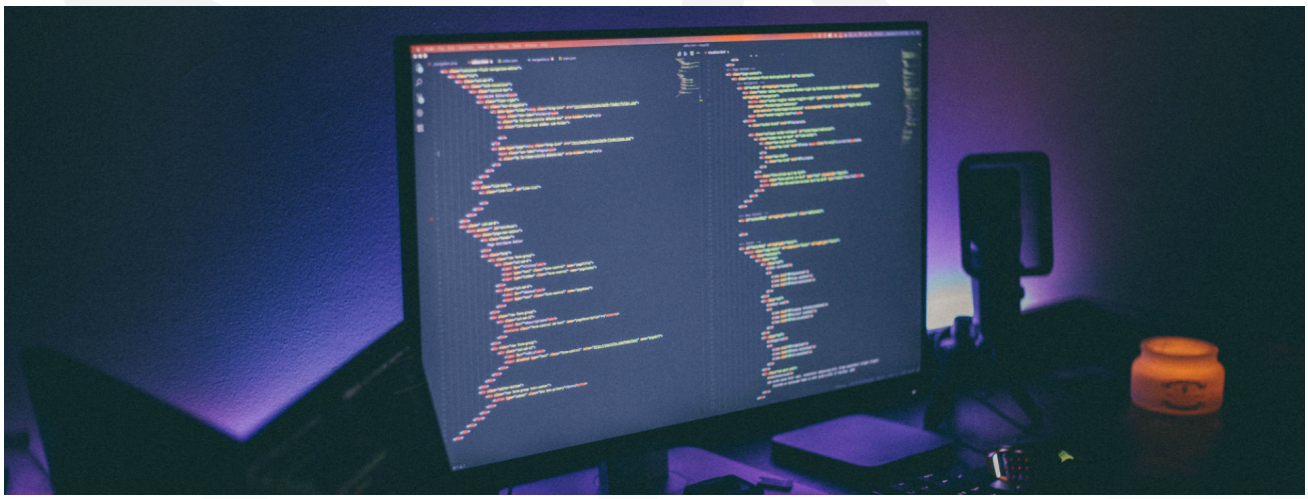
Related Events

Impact of COVID-19 on Enterprise Security Controls - ITG223 (/event-details?eventID=18287&orgCode=10)
November 5–6, 2020

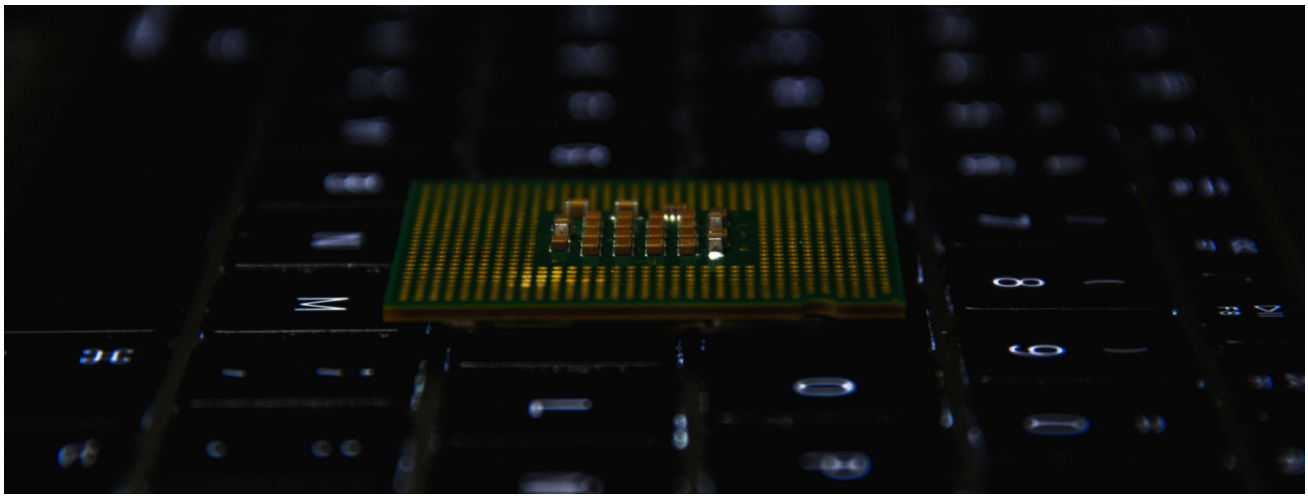


What Every IT Risk Assessment Should Include – OAR686WEB (/event-details?eventID=17777&orgCode=10)
November 9, 2020

Related Articles



Code Signing: A Security Control that Isn't Secured (/infosec-insider/code-signing-a-security-control-that-isn-t-secured)



Cloud Security and Privacy Audits: A 360 Degree Crash Course (/infosec-insider/cloud-security-and-privacy-audits-a-360-degree-crash-course)