CAE Forum

Wednesday, April 6, 2022

SHADOWMOVE: A STEALTHY LATERAL MOVEMENT STRATEGY (1:00 - 1:50 pm EST)

Introduction To Operational Security (2:00 – 2:50 pm EST)

Mark your calendar and come join us for CAE Forum! CAE Forum is a live, real-time, online, academic forum where members of the CAE community give non-technical presentations on topics of value to the CAE community. CAE Forum is about sharing your ideas, knowledge, and expertise to empower and strengthen our community. It's that simple. CAE Forum presentations are normally held on the third Wednesday of each month during the Fall and Spring semesters.

PRESENTATION #1

Title/Topic: SHADOWMOVE: A STEALTHY LATERAL MOVEMENT STRATEGY

Time: 1:00 - 1:50 pm EST

Location: https://caecommunity.zoom.us/my/caeforum

Just log in as "Guest" and enter your name. No password required.

Audience: Students, Professors, Govt.

Presenter(s): Dr. Jinpeng Wei, University of North Carolina at Charlotte

Description: Advanced Persistent Threat (APT) attacks use various strategies and techniques to move laterally within an enterprise environment; however, the existing strategies and techniques have limitations such as requiring elevated permissions, creating new connections, performing new authentications, or requiring process injections. Based on these characteristics, many host and network-based solutions have been proposed to prevent or detect such lateral movement attempts. In this talk, I will present a novel stealthy lateral movement strategy, ShadowMove, in which only established connections between systems in an enterprise network are misused for lateral movements. It has a set of unique features such as requiring no elevated privilege, no new connection, no extra authentication, and no process injection, which makes it stealthy against state-of-the-art detection mechanisms. ShadowMove is enabled by a novel socket duplication approach that allows a malicious process to silently abuse TCP connections established by benign processes. We design and implement ShadowMove for current Windows and Linux operating systems. To validate the feasibility of ShadowMove, we build several prototypes that successfully hijack three kinds of enterprise protocols, FTP, Microsoft SQL, and Window Remote Management, to perform lateral movement actions such as copying malware to the next target machine and launching malware on the target machine. We also confirm that our prototypes cannot be detected by existing host and network-based solutions, such as five top-notch anti-virus products, four IDSes and two Endpoint Detection, and Response systems.

PRESENTATION #2

Title/Topic: Introduction To Operational Security

Time: 2:00 - 2:50 pm EST

Location: https://caecommunity.zoom.us/my/caeforum

Just log in as "Guest" and enter your name. No password required.

Audience: Students, Professors, Govt.

Presenter(s): Aaron Jones, University of Advancing Technology

Description: Privacy is the buzz word of the day. There is a dire concern that every person on the planet is being surveilled in perpetuum. Businesses, classrooms, and our private lives are at constant risk of exposure to enemies both foreign and domestic. Members of the media have decried encryption, privacy, and personal freedom in the hopes of encouraging members of the public to give up their freedoms in exchange for an illusion of safety. What can we do to ensure our personal safety in an age of always on connections, constant monitoring, and the potential for a major cyber terrorism event looming over us like a poisonous cloud?

A recording of the live presentation will be available following the pre of the presentation at: https://www.caecommunity.org/resources/cae-forum-resources

Contact us at: caeforum@caecommunity.org