US 20240214419A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2024/0214419 A1

NEUHOF et al. (43) Pub. Date: Jun. 27, 2024

(54) **DETECTING A SPOOFED ENTITY BASED ON COMPLEXITY OF A DISTRIBUTION OF EVENTS INITIATED BY THE SPOOFED ENTITY**

(71) Applicant: **Microsoft Technology Licensing, LLC**, Redmond, WA (US)

(72) Inventors: **Moran NEUHOF**, Tel-Aviv (IL); **Shay KELS**, Givatayim (IL); **Peleg HADAR**, Tel-Aviv (IL); **Jonathan BAR OR**, North Bend, WA (US)

(21) Appl. No.: **18/086,440**

(22) Filed: **Dec. 21, 2022**

Publication Classification

(51) **Int. Cl.**
H04L 9/40 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1483*** (2013.01); ***H04L 63/1416*** (2013.01); ***H04L 63/20*** (2013.01)

(57) **ABSTRACT**

Techniques are described herein that are capable of detecting a spoofed entity based on complexity of a distribution of events initiated by the spoofed entity. Frequencies with which events of event types are initiated are determined by an entity during a designated period of time. Complexity of a distribution of the events among the event types is determined based at least on the frequencies with which the events of the event types are initiated by the entity during the designated period of time. Based at least on the complexity of the distribution of the events among the event types being less than or equal to a complexity threshold, the entity is identified as a spoofed entity associated with a spoofing attack. A security action is performed with regard to the entity based at least on the entity being identified as the spoofed entity associated with the spoofing attack.