1700 - Here to stay: Gaining persistency by abusing advanced authentication mechanisms

Saturday at 17:00 in 101 Track
45 minutes | Demo

Marina Simakov*Security researcher, Microsoft*

Igal Gofman*Security researcher, Microsoft*

Credentials have always served as a favorite target for advanced attackers, since these allow to efficiently traverse a network, without using any exploits.

Moreover, compromising the network might not be sufficient, as attackers strive to obtain persistency, which requires the use of advanced techniques to evade the security mechanisms installed along the way.

One of the challenges adversaries must face is: How to create threats that will continuously evade security mechanisms, and even if detected, ensure that control of the environment can be easily regained?

In this talk, we briefly discuss some of the past techniques for gaining persistency in a network (using local accounts, GPOs, skeleton key, etc.) and why they are insufficient nowadays.

Followed by a comprehensive analysis of lesser known mechanisms to achieve persistency, using non-mainstream methods (such as object manipulation, Kerberos delegation, etc.).

Finally, we show how defenders can secure their environment against such threats.
Marina Simakov
Marina Simakov is a security researcher at Microsoft, with a specific interest in network based attacks.

She holds an M.Sc in computer science, with several published articles. Gave a talk at BlueHat IL 2016 regarding attacks on local accounts.

@simakov_marina
Igal Gofman
Igal Gofman is a security Researcher at Microsoft. Igal has a proven track record in network

security, research oriented development and threat intelligence.

His research interests include network security, intrusion detection and operating systems.

Before Microsoft, Igal was a Threat Response Team Lead at Check Point Software Technologies leading the development of the intrusion detection system.

@IgalGofman

#defcon25/by_track/101/saturday #defcon25/By_Day/_saturday