1600 - The Adventures of AV and the Leaky Sandbox

Friday at 16:00 in Track 2
45 minutes | Demo, Tool
Itzik Kotler*Co-Founder & CTO, SafeBreach*

Amit Klein*VP Security Research, SafeBreach*

Everyone loves cloud-AV. Why not harness the wisdom of clouds to protect the enterprise? Consider a high-security enterprise with strict egress filtering - endpoints have no direct Internet connection, or the endpoints' connection to the Internet is restricted to hosts used by their legitimately installed software. Let's say there's malware running on an endpoint with full privileges. The malware still can't exfiltrate data due to the strict egress filtering.

Now let'also assume that this enterprise uses cloud-enhanced anti-virus (AV).You'd argue that if malware is already running on the endpoint with full privileges, then an AV agent can't degrade the security of the endpoint. And you'd be completely wrong.

In this presentation, we describe and demonstrate a novel technique for exfiltrating data from highly secure enterprises which employ strict egress filtering. Assuming the endpoint has a cloud-enhanced antivirus installed, we show that if the AV employs an Internet-connected sandbox in its cloud, it in fact facilitates such exfiltration. We release a tool implementing the exfiltration technique, and provide real-world results from several prominent AV products. We also provide insights on AV in-the-cloud sandboxes. Finally we address the issues of how to further enhance the attack, and possible mitigations.

Itzik Kotler

Itzik Kotler is CTO and Co-Founder of SafeBreach. Itzik has more than a decade of experience researching and working in the computer security space. He is a recognized industry speaker, having spoken at DEF CON, Black Hat USA, Hack In The Box, RSA, CCC and H2HC. Prior to founding SafeBreach, Itzik served as CTO at Security-Art, an information security consulting firm, and before that he was SOC Team Leader at Radware. (NASDQ: RDWR).

@itzikkotler
www.ikotler.org

Amit Klein

Amit Klein is a world renowned information security expert, with 26 years in information security and over 30 published technical papers on this topic. Amit is VP Security Research at SafeBreach, responsible for researching various infiltration, exfiltration and lateral movement

attacks. Before SafeBreach, Amit was CTO for Trusteer (acquired by IBM) for 8.5 years. Prior to Trusteer, Amit was chief scientist for Cyota (acquired by RSA) for 2 years, and prior to that, director of Security and Research for Sanctum (acquired by Watchfire, now part of IBM security division) for 7 years. Amit has a B.Sc. from the Hebrew University in Mathematics and Physics (magna cum laude, Talpiot program), recognized by InfoWorld as a CTO of the year 2010 , and has presented at BlackHat USA, HITB, RSA USA, OWASP, CertConf, BlueHat, CyberTech, APWG and AusCERT.

www.securitygalore.com

#defcon25/by_track/track2/friday #defcon25/By_Day/_Friday