Professor Yuval Shavitt, CTO of BGProtect – SECU Session February 20, 2019

My name is Yuval Shavitt, I am a Professor of Electrical Engineering at Tel Aviv University, and part of the Blavatnik Interdisciplinary Cyber Research Center. I am also the founder and CTO of BGProtect, a company that was established to defend nations and enterprises against attacks on their routing and thus their connectivity.

IP hijack attacks, also known as deflection attacks, are severe attacks since they enable the many variants of Man-in-the-Middle Attacks, including espionage, downgrade attacks, decryption, impersonation, and more. Financial institutions are one of the prime targets for such attacks since they are lucrative for both criminal organizations and foreign governments. In recent years past, we have documented deflection attacks on many financial organizations, which include many mid to large size banks, as well as stock exchanges, insurance companies, and financial news organizations. These attacks were not limited to BGP hijack attacks and included stealth traffic manipulations at exchange points and at large Internet Service Providers (ISPs). Some of these attacks lasted for weeks without ever being noticed by its victims.

What can be done? First of all, the financial sector should carefully monitor routing towards its crucial IP space, which includes public facing IP addresses and servers, such as, mail, DNS, and VPN. Secondly, there should be national level monitoring of the routing infrastructure to make sure data from financial organizations are not hijacked outside of the country. Finally, there should be a national sector CERT (the American term is a Fusion-Center) where data about attacks can be shared by financial organizations at multiple levels of anonymity.

Federal regulation can also play a role in managing the risk associated with IP Hijack Attacks. Laws need to be updated in order to regulate who is allowed to own data-communications infrastructure in any given constitution. For example, there are international ISPs such as China Telecom, that have locations (POPs) around the world, however, China does not allow foreign ISPs to establish a local presence on their soil. This lack of symmetry provides China Telecom with an unfair advantage. Making matters worse, even when the culprit is identified, they can very easily claim that it was a configuration error and avoid prosecution.

As I mentioned, I am also the CTO of a company called BGProtect. BGProtect is the leader in the detection and mitigation of IP Hijack & Data-Plane Attacks. Our platform and services are currently in use by global financial institutions, governments, intelligence agencies, service providers and international news agencies. Recent hijack attacks are not limited to BGP, but also of data-plane attacks, (e.g., compromising routers). Our system provides the only available service that can identify all types data-diversion attacks regardless of the technique that is used. We have hundreds of software agents on servers located around the world and more than 600M IP router address geo-locations in our database that we use to provide measurement results in real time to analyze global and local routes with our proprietary AI rules engine for anomalies.

With regards to the Huawei issue, it is important to note that essentially all networking and telecommunications equipment can be vulnerable to hacking and backdoors, and the best way to reduce and mitigate these risks is to invest in traffic monitoring equipment, as the saying goes *"an ounce of prevention is worth a pound of cure".*