NIKSUN, Inc.
100 Nassau Park Blvd.
Princeton, NJ 08540 USA
Tel: +1 (609) 936-9999
www.NIKSUN.com

Three of Philly Regions' Banks Target of Iranian Cyber Attack

Seven banks in total, three in the Philadelphia region – PNC Bank, Bank of America, and BB&T Corp. – were targeted by a series of distributed denial of service (DDoS) attacks linked to the Iranian government. The U.S. Department of Justice in Manhattan issued an indictment unsealed on March 24, 2016.[i]

DDoS attacks are used by hackers in various ways, including hacking into a targeted device, and using the attacks as a smoke screen. In the first example, the attacks are intent on crippling a customer's critical servers (in this case the bank's servers) so that users cannot perform their everyday functions with their banks. In the second example, DDoS attacks are used as a diversion tool, where the DDoS attacks flood the network, and security personnel focus on managing these attacks; meanwhile the attacker sneaks into the network undetected to get control of an internal machine or gain access to the network.

The indictment charged seven Iranians in an extensive campaign of over 176 days of DDoS attacks. Ahmad Fathi, 37; Hamid Firoozi, 34; Amin Shokohi, 25; 23-year-old Sadegh Ahmadzadegan, aka Nitr0jen26; Omid Ghaffarinia, aka PLuS, 25; Sina Keissar, 25; and Nader Saedi, aka Turk Server, 26, launched DDoS attacks between 2011 and mid-2013 against 46 victims, primarily U.S financial services companies.

Is it Possible to Detect and Mitigate Such Attacks? N.J. Cyber Security Company, NIKSUN, Says Yes

Why did the breach go undetected for so long? CEO and Founder of NIKSUN, Inc., a Princeton, New Jersey based cyber security company, believes it stemmed from the lack of total protection on these businesses' networks. "For the past two decades we have been working with government agencies, financial institutions, large ISPs, and enterprises to prevent such breaches from happening in the first place," says Dr. Pruthi. "In fact, we assisted a large bank back in the fall of 2012 that ran into this same scenario. They were victims of DDoS attacks over a period of time, and when they finally brought us in, we pinpointed exactly what happened, when it happened, and how it happened."

NIKSUN develops products designed to act as a camera and recorder to protect networks. Since introducing their flagship product, NetVCR, in 1997, the company hasn't stopped innovating, and security experts working for private companies, as well as the U.S. government, are noticing. NIKSUN's newest creation, Supreme Eagle, the world's first ever 100 Gbps real-time capture device, was recently

chosen by the Department of Defense (DoD) as part of its Joint Regional Security Stacks (JRSS) efforts toward making the nation immune from such insidious attacks.

Supreme Eagle gives JRSS the ability to create and store copies of all of the traffic flowing in and out of the military's networks, and examines the data for signs of malicious activity. If malware or abnormal behavior is detected, users are alerted and can remedy the situation immediately. In addition, Supreme Eagle offers the ability to "go back in time" by replaying traffic so that malware activity can be exposed after the fact as well.

In addition to Supreme Eagle, NIKSUN offers a variety of solutions to fit all sizes of networks — from small branch networks to large Internet Service Provider (ISPs) — offering cost-effective solutions to detect and mitigate DDoS attacks as well as numerous other types of cyber attacks, no matter how small or large your organization may be.

Taking proactive, preventative action in securing your organization's network is far superior than suffering through the financial drain and reputational damage of a targeted cyber attack. For the majority of businesses, being a victim of a cyber security breach is not a matter of "if" but a matter of "when." Securing your network in advance could make all the difference in keeping your organization's critical assets safe, while giving you peace of mind.

About NIKSUN, Inc.

NIKSUN is the recognized worldwide leader in making the Unknown Known. The company develops a highly scalable array of real time and forensics-based cyber security and network performance management solutions for government & intelligence agencies, service providers, financial services companies, and large enterprises such as retailers and manufacturers. NIKSUN's award-winning appliances deliver unprecedented flexibility and packet capture power. The company's patented real-time analysis and recording technology is the industry's most comprehensive solution for secure and reliable network infrastructure and services. NIKSUN, headquartered in Princeton, New Jersey, has sales offices and distributors throughout the US, Europe, the Mid East and Asia-Pacific.

[i] https://www.justice.gov/opa/file/834996/download