Israeli National Police

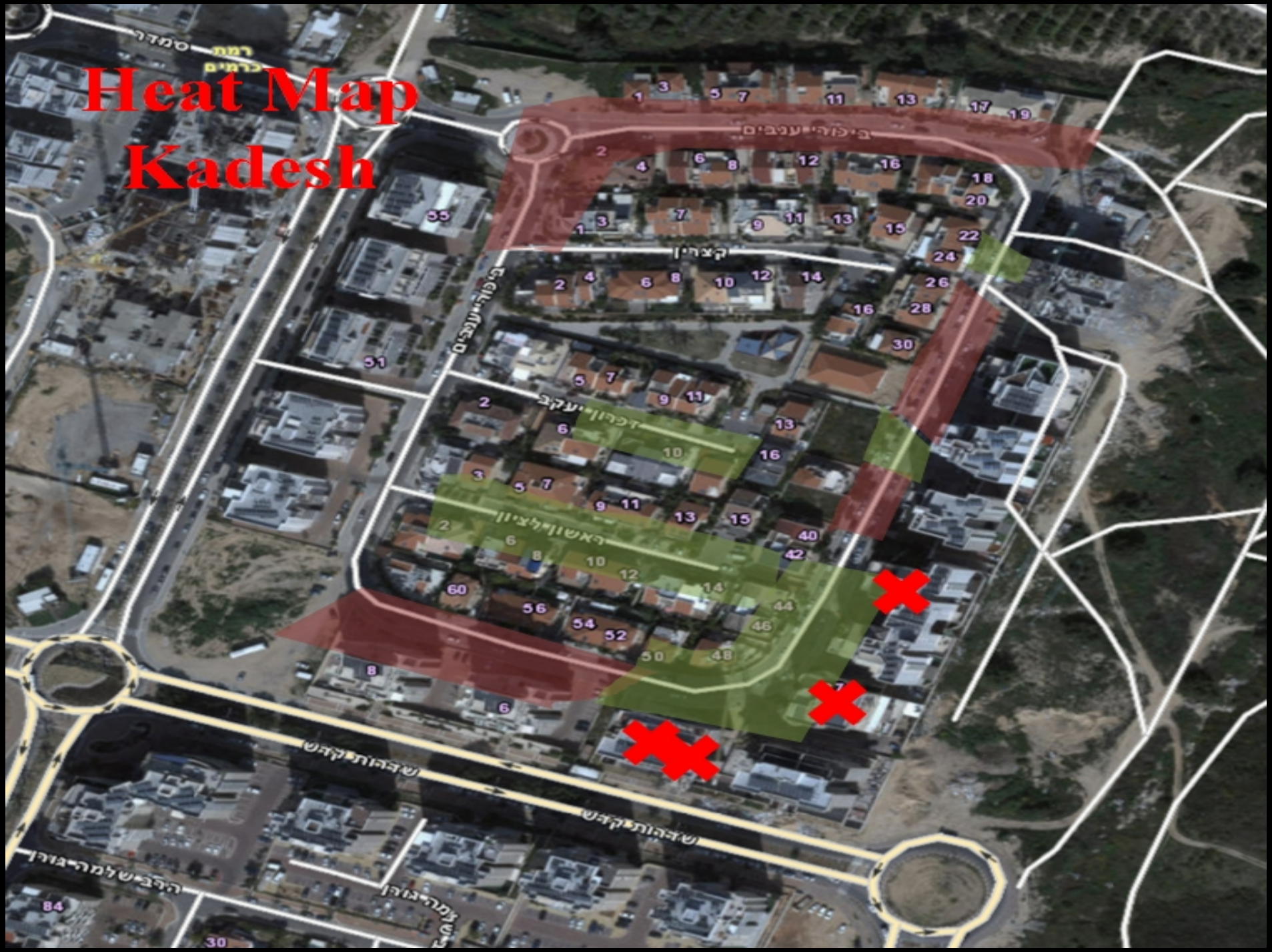
National Cyber Unit

Case study

801 INVESTIGATION – SUMMARY

- From early 2015 through March 2017, over 2,000 “Swatting” calls were made to more than 16 countries around the world. The suspect would call Schools, Hospitals, Airports and more, with bomb/ shooting threats in order to cause an emergency reaction by special forces (ex: SWAT team).
- This case was an international investigation which started after the Israeli CFC received more than four 24x7 requests regarding swatting attacks that lead to the same area in Israel.
- After reviewing all the information received, an investigation in the Israeli Cyber Crime Unit was opened, and after a joint operation with the FBI, the Australian and New Zealand police - an 18 year old suspect was arrested.

MODUS OPERANDI


Heat Map
Kadesh

PROFILE OF THE SUSPECT

Flooding the Darknet and Clearnet with fake identities

Active carder

Active on TOR network and Darknet

Using Bitcoin and virtual currencies, numerous entries to Blockchain etc.

Hiding identity and high anonymity while surfing the web via: VPN, SSH, TOR, Cloudflare, different WiFi networks

OUR "NEW" WORLD - THE CASE IN NUMBERS

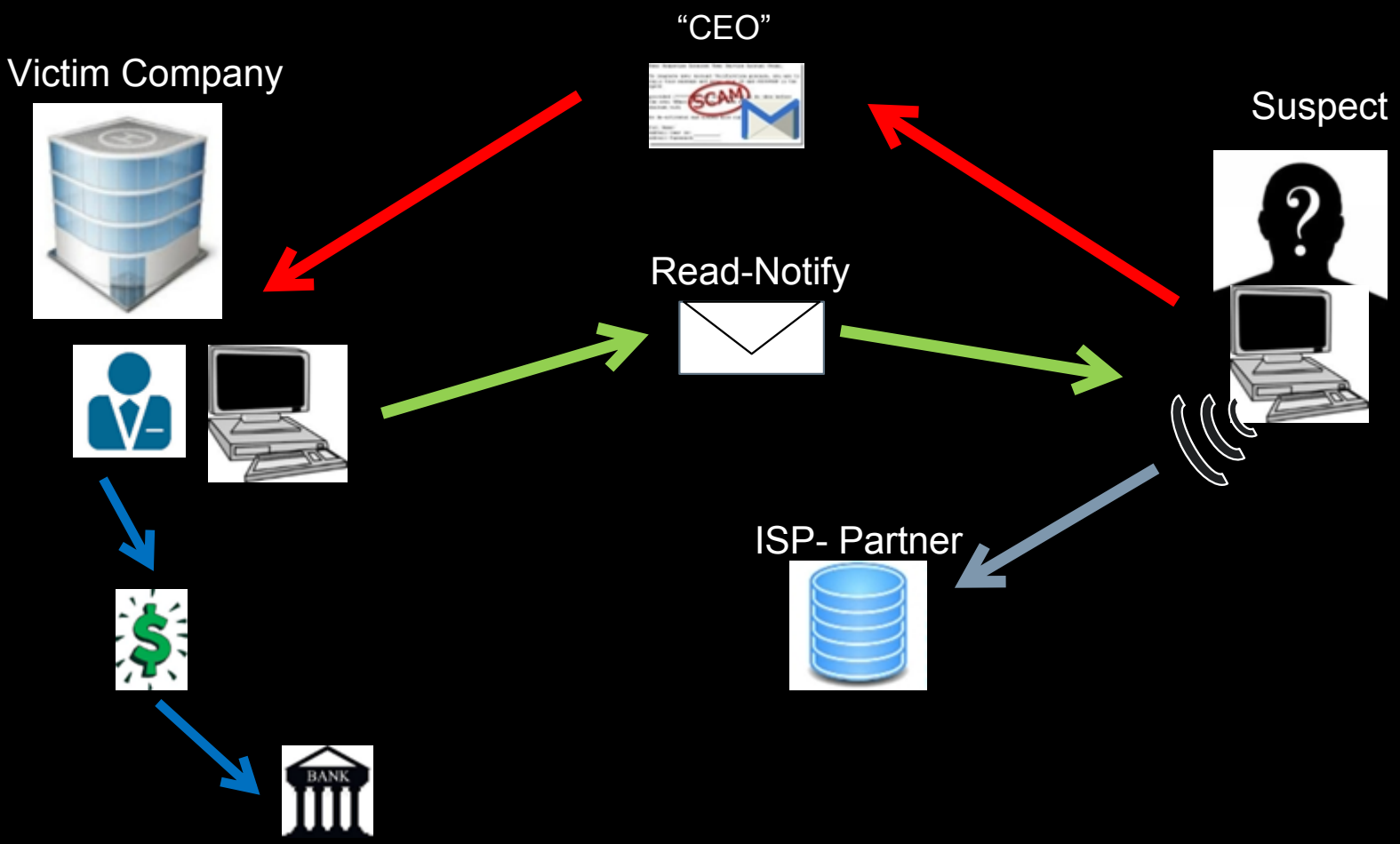
- Almost 2 Years
- 2438 events
- 16 countries
- 1 million $ at 4 bitcoins wallets
- Estimated damage of tens of millions $
- Most evidence at 128 Giga on 1 DOK!!

1 Suspect on 1 Laptop

CEO FRAUD

- Most of the incoming requests to Israel are regarding those Cases
- Major problem – Time & NAT
- One of the types of MITM attacks is the Man in the E-mail trend, where the suspect is “in between” the E-mail communication, convincing both sides that they are communicating with each other. Since the person in the “middle” is in control of the conversation.
- This phenomenon is also known as Business E-mail Compromise (BEC).

MODUS OPERANDI



BEC IN REAL TIME

- On 24.03.17 an urgent request for 24/7 assistance was received from the Austrian police. This case involved an Austrian company which was being scammed to transfer large sums of money (over 4 millions euro) to different bank accounts in the world.
- IP addresses which lead to the Israeli ISP, which were used for sending the impersonating emails. After real time action with both the victim company and the ISP, it was identified by the ISP that the suspect used a prepaid account and connected through a “net-stick”.
- The IP addresses received were NAT addresses (CGN) which are allocated to several users at once. Analytic manipulation was the ability which enabled the transfer of the NAT address - changing the suspect’s address in real-time to identify the user.

STRATEGY FOR SUCCESS

- National S.P.O.C Cyber Fusion Center with a broad definition of national & international responsibility in the cyber world
- Operational and technical support from a Cyber crime federal unit
- Data collaboration with application companies and Civil companies
- Direct 24/7 contact with countries, ISP's and application companies