Delivering Modern Cyber Defense

Kevin Mandia
CEO, FireEye
WHY ARE WE HERE?
There are **UNCERTAIN RULES OF ENGAGEMENT**
THERE IS AN **ESCALATING HUM**
OF CYBER CONFLICT
Today we are facing an **INVASION ON PRIVACY**
The security breach is growing more impactful.
A conflict on AUTHENTICITY AND DISINFORMATION
There will always be a security gap that can be exploited.
WE ARE IN THIS TOGETHER
WHAT ARE WE GOING TO DO ABOUT IT?
Intelligence Led
Technology Enabled
Outcome Based
INTELLIGENCE LED
~200 INTELLIGENCE ANALYSTS
32 LANGUAGES
18 COUNTRIES
700+ INVESTIGATIONS

200,000+ HOURS
380+ RED TEAM ENGAGEMENTS

60,000 HOURS
1 MILLION+
UNIQUE MALWARE SAMPLES PER DAY
MALWARE SAMPLES FROM INVESTIGATIONS

75,000+
MALWARE TRAFFIC DECRYPTION/DECODING SCRIPTS

150+

ATTACKER SESSIONS DECODED/MONTH IN SUPPORT OF INVESTIGATIONS

100+
There are FEW RISKS or REPERCUSSIONS for the attackers.
March: Islamic Revolutionary Guard Corps In an indictment, the U.S. Departments of Justice and Treasury accused Iran of stealing intellectual property from more than 300 universities, as well as government agencies and financial services companies.

July: Russian Intelligence Officers The U.S. Department of Justice announced the indictments of 12 Russian intelligence officers for carrying out large-scale cyber operations against the Democratic Party in advance of the 2016 Presidential election. The officers’ alleged crimes included the theft and subsequent leakage of emails from the Democratic National Committee and Hillary Clinton campaign, and the targeting of election infrastructure and local election officials in an attempt to interfere with the election.

August: FIN7 Cyber Crime Group Ukrainian nationals were indicted for participating in a prolific cyber crime group widely known as FIN7. They were accused of engaging in a highly sophisticated malware campaign that resulted in the theft of millions of customer credit and debit card numbers.

September: North Korea Sony Hack The U.S. Department of Justice announced the indictment of Park Jin Hyok, a North Korean hacker allegedly involved in the 2014 Sony hack, the 2016 theft of $81 million from a Bangladeshi bank, and the WannaCry ransomware attacks.

September: Financial Institutions Hack The U.S. Department of Justice announced the indictment and extradition of a Russian hacker accused of participating in the hack of JP Morgan Chase in 2014, leading to the theft of data from over 80 million customers, “the largest theft of customer data from a single U.S. financial institution in history.”
Attackers continue to 

EXPLOIT 

HUMAN TRUST
Cryptocurrencies are changing the game.
Cyber attackers reflect Geopolitical Conditions
DISCLOSURE is more probable and impact more severe
CEOs are wondering how good their cyber security needs to be.
RED TEAMING provides unvarnished truth of your defenses
PIONEERING MODERN CYBER DEFENSE

Intelligence Led

Technology Enabled

Outcome Based
OUR DIFFERENTIATION

Through our intelligence, technology and experts, we are positioned to learn, before anyone else, the tools and tactics attackers are using to circumvent security safeguards.
TECHNOLOGY ENABLED
PRODUCT VISION

Build the Best, Most Dynamic Layer of Defense

Be the Best at Security Validation

Deliver Expertise On Demand

Automate Security Operations

Know more about cyber attacks than anyone
OUTCOME BASED
MAKE LIFE HARDER FOR THE BAD GUYS
PROVIDE PEACE OF MIND FROM CYBER THREATS