A View From the Front Lines

David GROUT
CTO EMEA

FIREEYE™

700+
Threat Researchers, Platform Engineers, Malware Analysts, Intelligence Analysts, And Investigators

4
Cyber Threat Operations Centers Worldwide

30+
Languages Across 26 Countries

700+
Breach Investigations In 2018

24,000
Intelligence Reports Published In 2018

70+
Dedicated Researchers

David GROUT
15+ years
Prior SE leader
Think Tanks
Lots of breach experience

Industries Served
- Retail
- Healthcare
- Power & Utilities
- Oil & Gas
- Governments
- Telecommunications

WHY ARE WE HERE?

Evolution of Cyber Security Landscape

What Happened during the last 18 months

Dwell Times Continue to Decline

GLOBAL MEDIAN DWELL TIME

COMPROMISE NOTIFICATION	2011	2012	2013	2014	2015	2016	2017	2018
ALL	416	243	229	205	146	99	101	78
EXTERNAL					320	107	186	104
INTERNAL					56	80	57.5	50.5

MEDIAN DWELL TIME

416
DAYS IN 2011

78
DAYS IN 2018

GLOBAL DWELL TIME DISTRIBUTION

Newly Named APT Groups


APT37 – North Korea
Confirmed Targets
APT37
Targets – Defense,
Aerospace, Petrochemical,
Western Companies
TTPS– Compromise Web,
Spear-phishing
Destructive Capabilities


APT38 – North Korea
Confirmed Targets
APT38
Targets – Financial
Institutions, InterBank
financial systems
TTPS– Compromise Web,
Spear-phishing
Destructive Capabilities


APT39 Iran Nexus Group
Confirmed Targets
APT39
Targets – Transportation,
Aviation,
Telecommunication
TTPS– Compromise Web,
Spear-phishing
RDP, Mimikatz


APT40 – China
Belt & Road Initiative
APT40
Targets – Aerospace, Military, High-Tech, Transportation, Chemical, University …
TTPS– Variety of malware, Exploit CVEs, WebShells, Windows Command Lines


Russia: Sponsoring Increasingly Destructive Attacks & Influence
Targets – OT Systems, Elections
TTPS– Focus on Safety System, Built a framework Influence campaign, destabilization focus

Current landscape

May 2019: Real-time kinetic response to a cyber threat

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Thursday, December 20, 2018

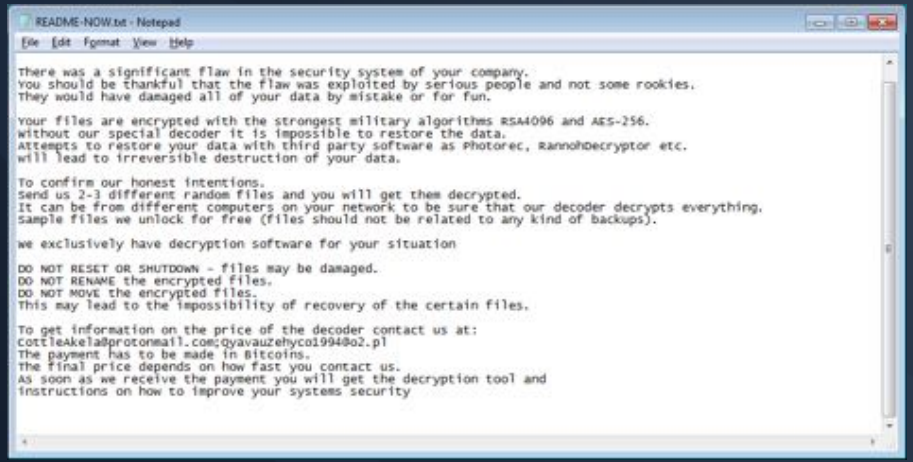
Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information

Defendants Were Members of the APT 10 Hacking Group Who Acted in Association with the Tianjin State Security Bureau and Engaged in Global Computer Intrusions for More Than a Decade, Continuing into 2018, Including Thefts from Managed Service Providers and

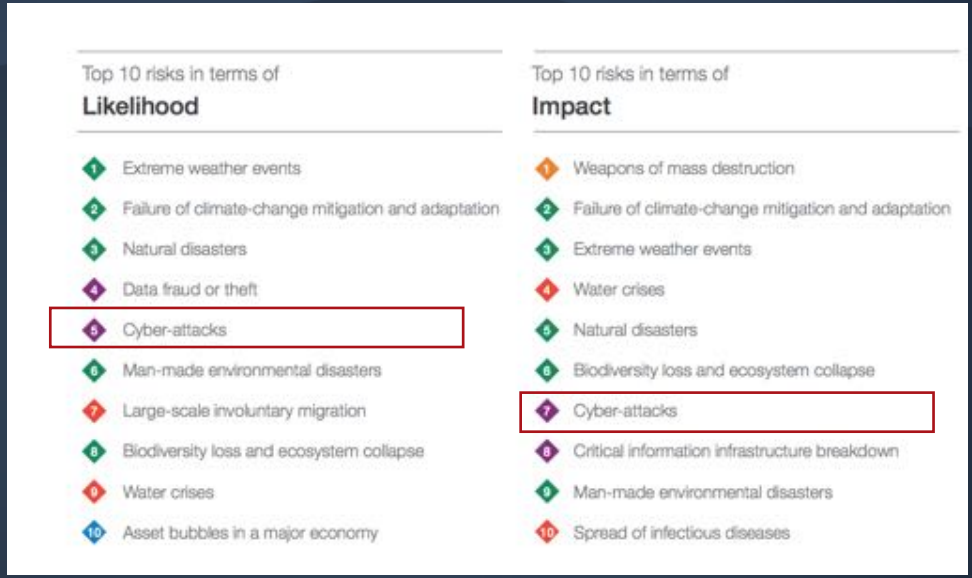
December 2018 : Ministry of Justice APT10 Indictment

May 2019 : Baltimore city under ransom

Current landscape



March 2019: FIN6 using LockerGoga



December 2018: Davos classified Cyber as a Top WW risks

ITALY – state of play

Cyber Espionage

- MODERATE RISK
- The amount of cyber espionage activity targeting Italy is roughly comparable to that targeting other advanced regional powers not currently involved in kinetic conflicts or major territorial disputes.

Cyber Crime

- HIGH RISK
- Frequently observed types of activity include fraud, personal or corporate data theft, and ransomware use. Due to Italians' heavy reliance on mobile internet access, mobile malware continues to be a particularly effective method of compromise.

Hacktivism

- MODERATE RISK
- Numerous hacktivist groups operate in Italy, and membership in these collectives likely overlaps considerably.

FIREEYE™

What do we need to do ?

Our strategy

INTELLIGENCE
Knowing the threats, the attackers to strengthen protection and reaction

TOOLS - PLATFORM
Delivering tools to increase detection, investigation, automation and remediation

RESPONSE
Ability to answer and investigate breaches

REMOVE ASSUMPTIONS
PROVE SECURITY

END-TO-END
VALIDATION

VERODIN SECURITY INSTRUMENTATION

Verodin is a security instrumentation platform that **continuously measures, tests, and improves cyber security effectiveness.**

1 CONTROLS EFFECTIVENESS

2 OPTIMIZE & RATIONALIZE

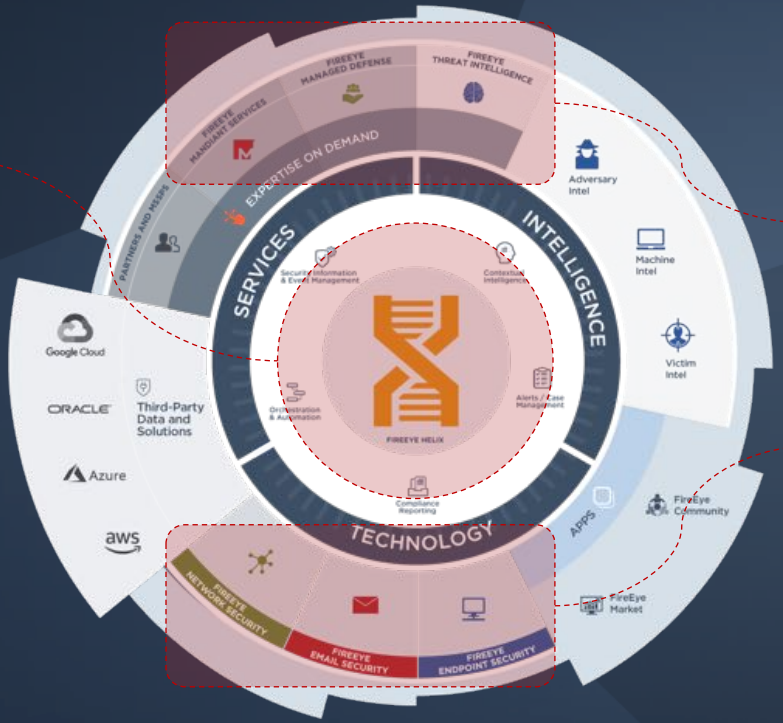
3 ENVIRONMENTAL DRIFT DETECTION

4 UNDERSTANDING CYBER RISK

SECURITY INSTRUMENTATION PLATFORM

VERODIN INTEGRATION WITH FIREEYE

Integrating with Helix to automate and orchestrate observed outcomes for a continuous self-healing security operation



Applying our understanding of the attacker derived on the front lines to continuously monitor and improve security posture

Monitoring and measuring proper deployment, configuration, and integration to deliver maximum ROI

FireEye Take Aways

Cyber security depends on the intersection of diplomacy, technology, and people.

- Products, services, intel alone won't cut it
- We need to be thinking of integrated platforms
- We can reduce human effort through orchestration
- Continuous evaluation is key for success

PROTECT. DEFEND. INNOVATE.