FireEye
SECURITY REIMAGINED

FIREEYE
SECURITY
SUMMIT

FireEye Intelligence: Threat Landscape Overview

Manish Gupta, Senior Vice President of Products

SECURITY
REIMAGINED

Agenda

FIREEYE SECURITY SUMMIT

How FireEye Defines the Threat Landscape

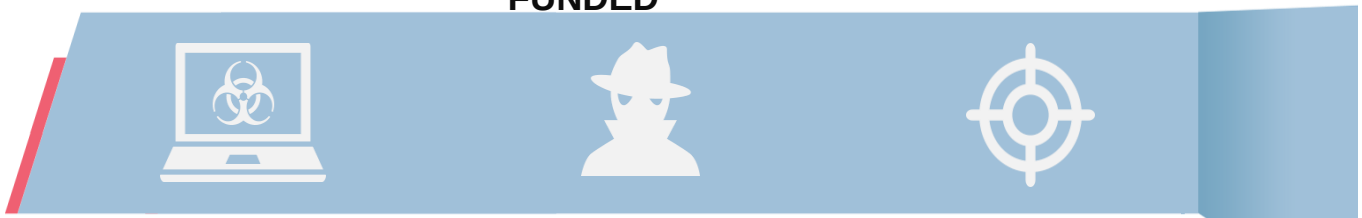
Intelligence Update for Europe

Threat Actor Categories

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Network Attack
Objective	 **Access & Propagation**	 **Economic, Political Advantage**	 **Financial Gain**	 **Defamation, Press & Policy**	 **Escalation, Destruction**
Example	Botnets & Spam	Advanced Persistent Threat	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
Targeted	☒	☑	☑	☑	☑
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven

APT Actors & Tactics

FIREEYE SECURITY SUMMIT



IT'S A "WHO," NOT A "WHAT"

- THERE'S A HUMAN AT THE KEYBOARD
- HIGHLY TAILORED AND CUSTOMIZED ATTACKS
- TARGETED SPECIFICALLY AT YOU

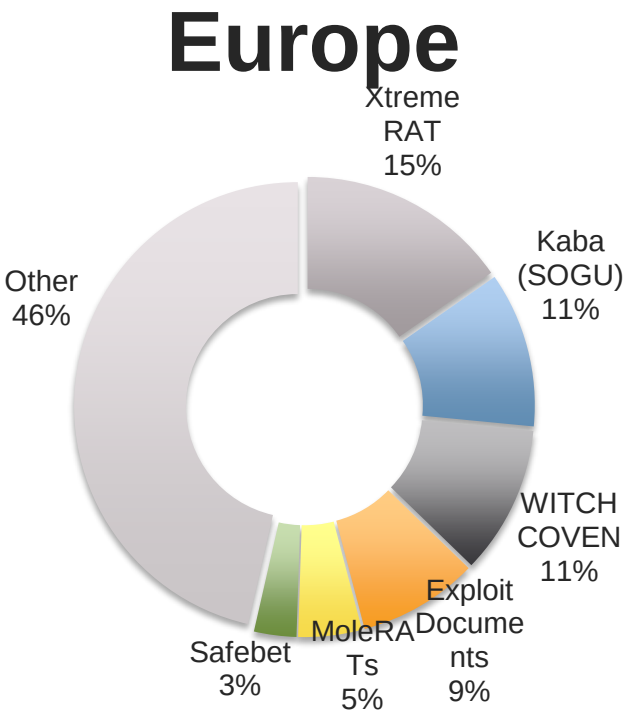
THEY ARE PROFESSIONAL, ORGANIZED AND WELL FUNDED

- NATION-STATE SPONSORED
- ESCALATE SOPHISTICATION OF TACTICS AS NEEDED
- RELENTLESSLY FOCUSED ON THEIR OBJECTIVE

IF YOU KICK THEM OUT THEY WILL RETURN

- THEY HAVE SPECIFIC OBJECTIVES
- THEIR GOAL IS LONG-TERM OCCUPATION
- PERSISTENCE TOOLS ENSURE ONGOING ACCESS

What APT Malware is Prevalent in Europe?



- Kaba/SOGU used by many different Chinese threat groups
- WITCHCOVEN is a profiling script used by APT groups
- MoleRATs used by Middle Eastern threat groups

FireEye Detections: January – June 2015

Europe in Context

FIREEYE SECURITY SUMMIT

Foreign Issues Are Domestic Concerns:

- Responding to Russian aggression
- Migrant Crisis
- Concerns over extremism
- Economic stability & energy security

Activity From a Range of Groups

– Intelligence Services - both allies and rivals

– Non-state actors engaging in their own operations

– Espionage, hacktivism, and the threat of computer network attack

The threat landscape in Europe reflects a mix of global actors and concerns

Russian Threat Activity

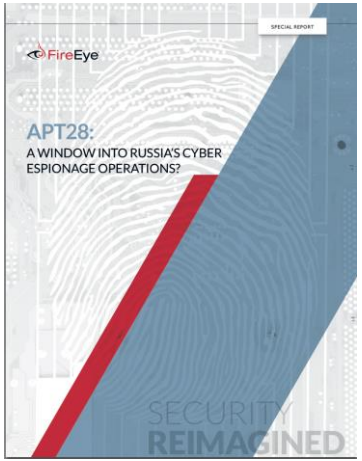
FIREEYE SECURITY SUMMIT

- **Long History of Information Warfare**
  - Broader meaning: cyber, electronic warfare, information operations
  - Established cyber program: uses in both peace and war
- **Involvement of Military and Intelligence Units**
  - Russian Ministry of Defense Cyber Command
- **Focus on secrecy and operational security**
  - Stealthy programs and doctrine
  - Possible use of criminal groups and hacktivists
- **Employment for…**
  - Espionage
  - Support military operations
  - Influence through media and other “information” means

Russian Cyber Operations

FIREEYE SECURITY SUMMIT

- **Espionage**
  - APT28 - Targeting think tanks, media, regime critics; iOS malware
  - APT29 - Targeting US, European govts & policymakers
- **Disruptive Activity Supporting Military Operations**
  - Estonia, Georgia, Ukraine
- **Reflections of Activity?**
  - Agent.BTZ / Snake / Turla / Uroburos
  - COZYCAR
  - Havex/Fertger
  - MiniDuke
  - BlackEnergy against ICS
- **Attribution Challenges**
  - RU Govt vs. RU Actor
  - Smoke and mirrors



Chinese Threat Activity

FIREEYE SECURITY SUMMIT

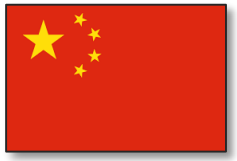
- **Cyber Activity Mirrors State Interests**
  - Protect Supremacy of Chinese Communist Party
  - Build economy, society, and military
  - 2050: Become a world-class power
- **Groups We Track**
  - Over two dozen groups
  - Some active for periods of 10 years or longer
  - Comprised of military and likely state security units
  - At least 3 groups are contractors
- **Targets**
  - Massive, worldwide scale
  - All sectors: Government, Industry, Non Profit

Current Five-Year Plan Priorities
Food and Beverage
Creative Industries
Specialized Manufacturing
Biotech/Health Sciences
Energy Industry
IT and Communications

New Trends Through 2014

FIREEYE SECURITY SUMMIT

- **Adapted Social Engineering**
  - Use of social media to interact with targets and develop trust before deploying a payload
- **Alternations to Malware**
  - UDP backdoor
  - Encryption and modularity
  - Memory only malware
  - C2 leverages DNS hijacking of legitimate domains
- **Data Theft via DropBox to Blend in with Legitimate Traffic**
- **Use of profiling scripts**
- **Healthcare Breaches, Office of Personnel Management, PII Theft**
- **Ties Between China-based APT Groups and DDoS Attacks?**



Other State Espionage Involving Europe

FIREEYE SECURITY SUMMIT

- **France**
  - Babar, Casper, Bunny
  - Greece, Spain, Syria
- **UK**
  - Regin
  - Telecommunications, researchers focusing on advanced mathematics and cryptology
  - Belgium, Germany, Algeria, Iran, Syria, Russia, Pakistan, others
- **US**
  - Equation Group
  - Financial institutions, Islamic scholars, and other victims
  - Germany, Switzerland, France, Belgium, the UK, and elsewhere

Hacktivists & the “CyberCaliphate”

FIREEYE SECURITY SUMMIT

- **Hacktivists allegedly target French websites post-Paris siege**
  - ~ 20,000 sites affected
  - Distributed denial of service attacks, defacements
  - French military official attributes to “well-known Islamist hackers”
- **“CyberCaliphate” targets TV5 Monde**
  - Apparent escalation in tactics
  - Disrupts programming on 11 channels
  - Defaces website and social media accounts
  - Claims to act in support of ISIS – no firm attribution or ties to ISIS

Threats to the European Energy Sector: ICS Malware

FIREEYE SECURITY SUMMIT

Havex

(aka Fertger / PEACEPIPE / “DragonFly” / “Energetic Bear”)

- Detected in Middle East networks in 2014
- Compromise via spear phish or SWC
- Targets are diverse: wide, multi-sector targeting
- Motivation somewhat unclear
  - » Espionage / intelligence collection
  - » Oil/gas: pricing data, negotiation positions?
  - » Business operations
  - » Possible disruptive ambitions?

BlackEnergy

ICS Variant

(aka “Quedagh Group” / “SandWorm”)

- Targets ICS Software
- Associated activity leveraged BlackEnergy to compromise NATO, Ukrainian targets

FIREEYE SECURITY SUMMIT

THANK YOU