FireEye Intel Center
FireEye, Inc. · Security. Reimagined.
1440 McCarthy Blvd · Milpitas, CA 95035

Governments Threat Trends (Q2 2015)

Date: July 1st, 2015 **Tags:** governments, germany, pii, india, japan, china, apt28

Governments Threat Trends (Q2 2015)

Threat Insight #1: German Government Reportedly Fends Off Another Hack of the Bundestag (Linked & Attached)

Threat Insight #2: We Know Who You Are—Nation State Actors Collect Personal Information on Citizens of Geopolitical Competitors (Linked & Attached)

Threat Horizon: Governments Risk Assessment for Apr-Jun 2015

State-sponsored threat actors will certainly continue to target foreign governments in search of strategic intelligence capable of providing their sponsoring government with a political, economic, or military advantage. We expect the following factors to influence threat actors' targeting in the government sector in the next quarter and beyond:

- Increasing regional tensions over China's island-building in the South China Sea will almost certainly drive states involved in the dispute to conduct cyber espionage activity against the other claimants. States will task threat actors with stealing data capable of informing decision makers as to the intents and capabilities of both foreign governments and organizations in the region. Decision-makers will probably use such intelligence to better defend their country's territorial claims in the diplomatic, military, or commercial domain.
- The chill between Moscow and the West will most likely lead to continued government-focused cyber espionage activity from both sides, as governments target information related to sanctions, military movements and exercises, energy, and other topics in search of a strategic advantage.
- As the U.S. and Iran continue to work towards a controversial nuclear deal, interested parties will probably employ cyber espionage to monitor the talks and provide decision makers with advance notice of any negotiating terms. States may also employ offensive cyber operations against an involved

government or its commercial assets to either protest the talks, attempt to influence the outcome, or in response to the talks' failure or what the actors perceive as their government's acceptance of unfair terms.
- Threat actors associated with various stakeholders in the ongoing conflicts in Syria, Iraq, Yemen, Saudi Arabia, Ukraine, and elsewhere, will almost certainly target adversary governments in search of valuable intelligence capable of supporting their cause through providing a strategic advantage.
- Hacktivists may deface or launch distributed denial of service attacks against government websites to promote a cause or respond to a perceived controversy. Potential drivers of such activity may include a country's military engagement in a foreign crisis or legislative approval for increased government surveillance.
- Due in part to the increasing digitalization of records, government agencies that hold mass amounts of financial account data or personally identifiable information will probably continue to face risks from cyber criminals seeking to steal and profit from such data through the unauthorized transfers, identify theft, or the sale of information on underground forums.

Governments Industry: Advanced Actor Targeting

FireEye believes that government agencies – both federal and local or regional – face cyber security threats from nation state threat actors, financially motivated cybercriminals, and hacktivists.

- Advanced Persistent Threat (APT) groups will almost certainly target foreign governments in pursuit of obtaining information that could provide their sponsoring government with political, economic, and military advantages. Such information might include classified reports, communications, and strategies. It may also include financial information, and data pertaining to defense technologies and programs.
- Nation states may also use threat actors to conduct offensive operations against an opposing government in the event of war. Such actors would likely use computer network attacks to obstruct government operations, impeding the government's ability to either respond to attack or provide critical services to its population.
- We also suggest that threat actors associated with a nation state may target local governments in an effort to perform reconnaissance on the targeted network, assess security provisions, and test their own capabilities.
- Financially motivated threat actors will likely target state-level financial institutions in search of citizens' tax data and personally identifiable information, which the threat actors can use for monetary gain. Although we consider that some threat actors may target similar federal institutions, we suggest that state-level institutions present the more likely target, given that such institutions have smaller budgets and resources to devote to security.
- Lastly, we suggest that hacktivists may also attempt to target both federal and state level governments to protest a particular policy and/or call attention to a cause. These threat actors may seek to embarrass the victim government and disrupt operations through distributed denial of service

attacks, defacing government webpages, or stealing and then leaking sensitive data.

For the January-March 2015 timeframe, based on FireEye® Dynamic Threat Intelligence™ (DTI) cloud data, FireEye has assigned a Cybercon™ level of 3 to Governments, which is considered Moderate.

Governments Q2 2015 Trend Intelligence (Attached)

- Daily Detection Levels, April - June 2015
- APT Malware Detections by Industry
- Top Non-APT Malware Detections
- APT Detections

Download the Full Q2 2015 Threat Trends Report: GOVERNMENTS