CROWDSTRIKE

2015 CROWDSTRIKE GLOBAL THREAT REPORT

EXECUTIVE SUMMARY and FINDINGS for BUSINESS LEADERS and BOARD MEMBERS

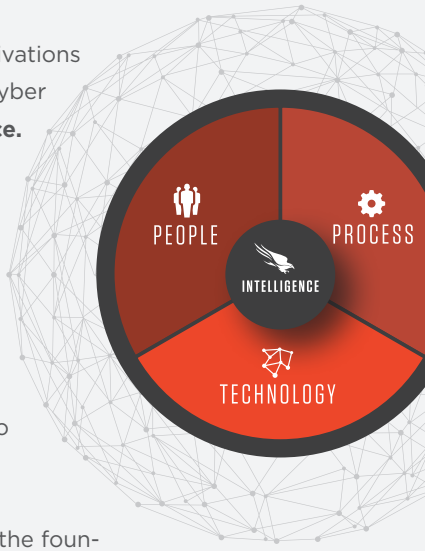
CROWDSTRIKE

LETTER FROM THE CEO

If there's one thing that businesses, boards of directors and C-level execs can take from **CrowdStrike's 2015 Threat Report,** it is that the paradigm has broadened beyond people, processes, and technology to now include integrated, crowdsourced, and enriched threat intelligence.

Our **Global Threat Report** highlights that today's threats, more than ever before, are driven by geopolitical and economic events around the world. The primary motivation behind global cyber activity has now shifted from disparate activities carried out by individuals, groups and criminal gangs pursuing short-term financial gain, to skilled adversaries driven by strategic global conflicts. The economic downturn and new Five Year Plan in China will continue to drive their state-sponsored cyber espionage activities. The situation in the Ukraine and falling oil prices will continue to fuel targeted intrusions from Russia. The conflict in the Middle East between Saudi Arabia and Iran over Yemen will continue to generate hacktivism from that region. CEOs and boards of directors who ignore or disregard the ramifications of global events such as these will pay for it in the loss of revenue, jobs, intellectual property, and shareholder value.

This shift underscores the importance for an effective intelligence program about the motivations of your adversary. The mantra "people, processes and technology" is no longer enough for cyber security. In today's threat environment, it takes **people, processes, technology** AND **intelligence.** Intelligence is no longer a "nice-to-have." It is a mandatory element of stopping breaches.



How can you expect to win if you do not have a solid understanding of how your adversary operates, what their tendencies are, what their goals are, and what motivates them? Recognize why they would want to come after you and your company. If you don't know the game plan of your adversary, you will fail to defend your corporation. It sounds like common sense, but it is something that is lost in the outdated discussion of people, processes and technology. Companies must have intelligence, either home-grown or provided by third-party sources who have the trained personnel to monitor, capture and analyze threat data effectively.

Emphasizing intelligence has been a cornerstone for CrowdStrike's approach to security since the foundation of the company five years ago: Providing cloud-based security powered by comprehensive, in-house threat intelligence. With our Falcon Platform and Threat Intelligence team, we have a unique bird's-eye view by having our endpoint sensors deployed in more than 170 different countries, handling more than ten billion events per day, as well as providing incident response services in response to some of the largest breaches. The "brains" behind our Falcon Platform is our Threat Graph engine, which constantly collects and analyzes billions of events, both in real time and retrospectively. As a result, on a weekly basis, we are identifying and mitigating hundreds of breaches for which traditional defenses silently fail.

The CrowdStrike team has put tremendous effort into capturing this real attack telemetry, analyzing it, distilling how adversaries operate, and more importantly, what motivates them. We hope our experiences and the lessons learned that are manifested in the 2015 Threat Report will provide companies a sampling of the intelligence they need to protect themselves in 2016 and beyond. Please click **here** to find out more about how CrowdStrike can prevent breaches with our groundbreaking endpoint technologies, intelligence products, and response services.

George Kurtz. President, CEO & Co-Founder

2015 CROWDSTRIKE GLOBAL THREAT REPORT

EXECUTIVE SUMMARY and FINDINGS for BUSINESS LEADERS and BOARD MEMBERS

The following summary of the exhaustive **CrowdStrike 2015 Global Threat Report** provides executives with high level, need-to-know information critical to making business decisions in the coming year. It recognizes that cyber security is a growing concern for their companies, and threats posed by malicious actors around the globe can have profound effects on their organizations, both in terms of current operations and long-term growth.

The behaviors of these malicious actors in 2015 are obvious when viewed through the lens of the events that influenced them. Whether it be the Russian Federation intrusions from Ukraine through Europe to the United States, or the hacktivist-on-hacktivist attacks following the terror attacks in Paris, or the massive uptick in cryptographic ransomware by eCrime actors following the success of Cryptolocker—the events that precipitated these actions were clear. By understanding the adversary, how they think, and what events impact their beliefs and motivations, it is possible to better prepare and react.

Adversary activity is generally not instantaneous after an event; they need to prepare, plan, and act. The instant an event that impacts the adversary occurs, the clock begins ticking as they process the event via a standard series of steps: Observe, orient, decide, and act (OODA). If you can go through these steps faster than the adversary, then you will have the advantage.

KEY FINDINGS: TARGETED INTRUSIONS:

CHINA:

China's cyber activity moving forward likely will be governed largely by the 13th Five Year Plan (FYP) introduced in 2015, which will carry through to 2020. Cyber activity will also be influenced by the reorganization of the military, the needs of an emerging middle class, and the continued efforts to reform the economy.

Chinese cyber activity may shift dynamics, but it is not expected to cease anytime soon. Given its remaining technological gaps and the strategic edge targeted intrusions can provide its economy, there is still plenty of incentive for China to engage in commercial cyber espionage when opportunities arise. As China looks to transform its standard of living and become less reliant on foreign technology, there most likely will be an increase in attacks targeting areas such as agriculture, healthcare, and alternative energy. All of these are areas that China deems crucial to promoting the wellbeing of its growing middle class, and where it has the most technological gaps. 2016 may see Chinese cyber operators targeting these sectors not just for intellectual property, but also for general know-how, such as building native supply chains and administrative expertise.

RUSSIA:

As the Russian economy faced the possibility of recession due to both the U.S. and EU sanctions stemming from the Ukraine conflict, and as the global price of oil fell, a noted increase in intrusion activity was observed. Perhaps in an effort to hedge against these challenges or to gain information to formulate monetary policy, Russia performed broad intelligence-collection campaigns, targeting numerous entities in government, defense, and non-governmental organizations (NGOs) in the U.S., Europe, Asia, South America and the Middle East. The expansion of reconnaissance may have been an effort on the part of the Russian government to seek understanding of changes in oil pricing in order to inform its national economic policies. Russia's precarious economic state will most likely continue to create an insatiable appetite for the intelligence needed by decision makers, particularly against targets operating in regional areas of interest and global energy companies.

IRAN:

The efforts of the Iranian leadership in 2015 clearly depict a regime struggling with the benefits and the threats of the impending Joint Comprehensive Plan of Action (JCPOA) and the outside influence that is attached to it. On the one hand is much-needed economic relief from the years of isolating sanctions; on the other hand, the influence of Western ideology threatens to come during crucial election cycles. On June 30, 2015, just before the finalization of the JCPOA, Supreme Leader Ayatollah Ali Khamenei revealed the outline of Iran's 6th Five-Year Plan, revealing Iran's intent to improve its infrastructure and cyber capabilities. Due to the intense concern of possible future degradation of Iran's Islamic values as businesses (primarily Western) renew trade with Iran, it is highly likely the Iranian government will react by increasing Internet monitoring and censorship on a national scale as quickly and as effectively as possible. With the regional tensions heading into 2016, there is increased likelihood Iran will use its cyber capabilities—which are also expected to strengthen and improve going forward—against its perceived enemies, particularly Saudi Arabia, regional governments, and their allies.

ECRIME

ECrime is an ecosystem where different organizations and individuals weave intricate relationships in order to exploit their victims, and they are constantly evolving and improving their tradecraft. Criminal activity continues to thrive in the shadow of legal impediments to law enforcement and the ability of the actors to hide in the relative anonymity of the Internet. CrowdStrike Intelligence observed a significant increase in extortive attacks carried out by organized criminal groups in 2015. The prevalence of social engineering schemes using inside knowledge of the target also flourished in 2015. Possibly as a consequence of the confluence of cybercriminal and espionage activities, tomorrow's malware may likely develop into a multi-purpose tool that provides a platform suitable for a wide variety of malicious operations. Such an open-ended architecture and the complexities involved in determining the actor's intent is likely to pose a research challenge to defenders in the near future. It is probable that in 2016, the introduction of new malware families with increased complexity and stealth will continue to expand. Ransomware also has been a growth market for criminals in 2015, and this trend shows no sign of abating.

HACKTIVISM

Hacktivist activity may occur in concert with geo-political issues and conducted in the guise of activism, nationalism, or simply mischief. Actors who participate in hacktivism can range from seasoned hacking veterans to angry neophytes who volunteer to join a participatory DDoS (distributed denial of service) attack. Regional conflicts will likely remain a primary driver of nationalistic hacktivist activity in 2016. Examples in 2015 include the controversial Canadian Anti-Terrorism Act (C-51), which resulted in widespread DDoS against Canadian government organizations. Hacktivism can also manifest itself in the form of social activism such as the DDoS attacks against targets in Baltimore, Maryland, following the funeral service for Freddie Gray, a man who died in police custody. Some cases of hacktivism are difficult to distinguish from nation-state offensive cyber activity. Groups like the Syrian Electronic Army (SEA), tracked by CrowdStrike as DEADEYE JACKAL, or the Yemeni Cyber Army can have strong overlap with regimes that want to use nationalistic hackers as a volunteer army to support the cause of a regime. Hacktivism such as that which followed the Charlie Hebdo events in Paris, or in wake of the increasing presence of Islamic extremism manifested by Da'esh (ISIS) and pro-ISIS groups, may take on an aggressive hacktivist-versus-hacktivist dynamic. Hacktivism can happen anywhere, at any time, for any reason, against any target, particularly government and financial sector organizations around the globe. Understanding the motivation and core ethos of hacktivist groups can help organizations be prepared to defend themselves against these aggressors.

SUMMARY

CEOs and boards of directors who ignore or disregard the ramifications of the global events which are the primary drivers behind today's cyber threats will pay for it in the loss of revenue, jobs, intellectual property, and shareholder value. This shift underscore's the importance of an effective intelligence program about the motivations of your adversary. The mantra "people, processes and technology" is no longer enough for cyber security. In today's threat environment, it takes people, processes, technology AND intelligence. Intelligence is no longer a "nice-to-have." It is a mandatory element of stopping breaches.

The CrowdStrike team has put tremendous effort into capturing this real attack telemetry, analyzing it, distilling how adversaries operate, and more importantly, what motivates them. We hope our experiences and the lessons learned that are manifested in the 2015 Threat Report will provide companies a sampling of the intelligence they need to protect themselves in 2016 and beyond.

FOR THE FULL REPORT CLICK HERE

CHINA

GLOBAL THREAT REPORT

This infographic depicts the impacts and targeting priorities for key business verticals of the Chinese 13th Five-Year Plan. Each vertical is split into the most likely components to be targeted. The number of Chinese based threat actors known to target that vertical are depicted in the black circles.

1 Energy

10 Chinese Adversaries

Nuclear Energy related businesses
IMPACT:
- Mergers and Acquisitions, multiparty bid information
- Research into safer nuclear energy usage
- Technology Supporting Nuclear Energy
- Nuclear Facilities operations and procedures

Clean Energy
IMPACT:
- Processes and Techniques for Clean Energy Production
- International climate policy and discussions
- International emission research and reporting
- Clean energy technology

Oil
IMPACT:
- Oil company pipeline construction projects
- Operations and surveys in South China Sea
- Bidding and contracting for resources
- Extraction, mapping, and safety technology

2 Transportation

12 Chinese Adversaries

High Speed Rail Projects
IMPACT:
- Railway project bidding
- Government Transportation Authorities
- High Speed Rail R&D

Electric/Hybrid Transportation
IMPACT:
- Electric car/bus production facilities
- Charging Station/Rechargeable Battery Technology
- Companies developing component technologies

Airlines
IMPACT:
- Passenger Name Records
- Mergers and Acquisitions Information
- Logistics/Operations/Processes information
- Route Information

3 Government

22 Chinese Adversaries

Think Tanks
IMPACT:
- Policy and analysis related to CN strategy
- Policy and analysis related to international political issues
- Logistics and operations to develop native think tanks

Foreign Government Targeting
IMPACT:
- Regional issues and diplomacy
- Disputes over international boundaries
- Cyber Sovereignty

Special Event Targeting
IMPACT:
- Olympics VIP intelligence
- US Candidates/Elections
- G20/G8

4 Defense/ Law Enforcement

28 Chinese Adversaries

Military Command Structure
IMPACT:
- Logistics and joint-command structure duplication
- Weapons Systems, Capabilities, and Technology
- Personnel Information

Navy/Air Forces
IMPACT:
- Aircraft/Carrier Operations and Technology Targeting
- Sea based weapon technology
- Unmanned Aerial Vehicle technologies
- PACOM logistics support and cleared contractors in SCS

Intelligence
IMPACT:
- Signal Intelligence/Cyber Integration
- Theft of Sensitive Personal Identifiable Information
- Organization Structures/Tradecraft knowledge

5 Technology

15 Chinese Adversaries

Popular Western apps & social services
IMPACT:
- Replication of top social/personal/ride sharing apps
- Mergers and Acquisitions Intelligence
- Theft of Research and Development information

Domestically sourced Semiconductors & computer chips
IMPACT:
- M&A with US chip manufacturers
- "Technology Transfer"
- National Security compliance used to acquire Western source code

COMPREHENSIVE VERTICALS

Academic
Educational institutions dedicated to instruction of students as well as research.

Aerospace
Research, design, manufacture, operate, or maintain aircraft and/or spacecraft.

Automotive
!Organizatiosn nvolved in the design, development, manufacturing, marketing, & selling of motor vehicles.

Casino
Facilities that house and accommodate gambling activities.

Chemical
Organizations that produce industrial chemicals.

Defense
Gov't & commercial organizations that research, develop, produce, military equipment, and facilities.

Dissident
Individuals & organizations who oppose gov't doctrine, policy, or institutions.

Energy
Organizations involved in the production, distribution, & sale of energy. Oil/gas not included.

Engineering
Organizations that design manufacture, & operate structures, machines, or devices.

Entertainment
Organizations that produce & distri- bute motion pictures & television programming.

Mining
Extraction of valuable minerals or other geological materials from the earth.

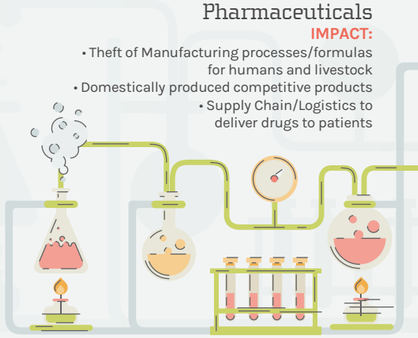
Financial
Provide financial services to commercial & retail customers.

Gaming
Organizations involved with the development, marketing &sales of video games.

6 Healthcare

9 Chinese Adversaries

Pharmaceuticals
IMPACT:
- Theft of Manufacturing processes/formulas for humans and livestock
- Domestically produced competitive products
- Supply Chain/Logistics to deliver drugs to patients



Health technology /biomedical
IMPACT:
- Mobile healthcare technology
- Healthcare/National ID technology
- Remote Medicine

Health Insurance systems
IMPACT:
- Healthcare insurance/delivery
- Multi-layered medical security network
- Theft of technology/software used by insurance industries

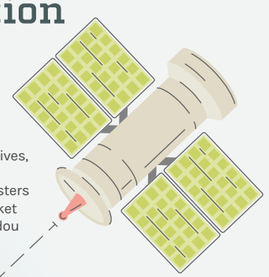
7 Telecommunication

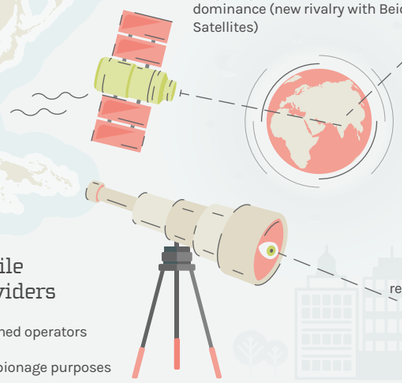
14 Chinese Adversaries

Diplomacy
IMPACT:
- Policy and analysis related to building/transportation projects with CN
- Silk Belt and Silk Road initiatives/agreements
- South China Sea development

Silk Belt
Silk Road

Space and Satellite Organizations
IMPACT:
- Theft of satellite technology
- Space programs, projects, initiatives, operation schedules
- Meeting/conference agendas, rosters
- Targeting of traditional GPS market dominance (new rivalry with Beidou Satellites)

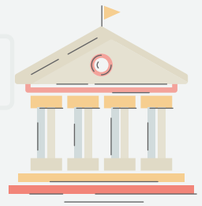




Internet Service Providers/Internet Services
IMPACT:
- Theft of research and development information
- Logistic and operation information pertaining to foreign infrastructure and services
- Alternative solutions to reliance on Western technology
- Censorship policy and implementation

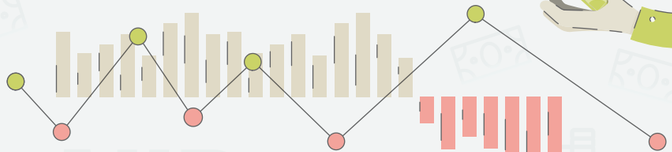
Private cellular mobile communication providers
IMPACT:
- Relationship with CN state-owned operators
- Merger information
- Infrastructure targeting for espionage purposes

8 Financial

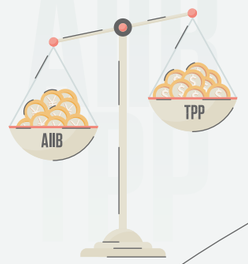


International Financial Organizations
IMPACT:
- Policy related to financial trade agreements
- Analysis and reporting on economic forecasts
- Annual meeting agendas, rosters
- Changes in financial market regulations

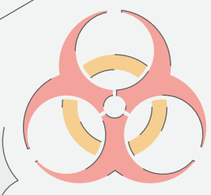
11 Chinese Adversaries



Think Tanks
IMPACT:
- Policy and analysis related to CN financial issues
- Policy and analysis related to global economic forecasts
- Policy and analysis of Taiwan/SCS issues

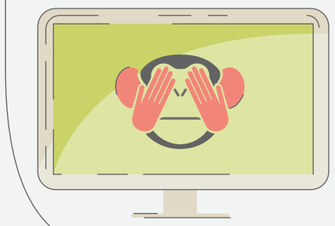


9 Chinese Adversaries



9 Media

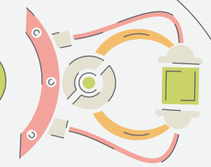
International Multimedia Companies
IMPACT:
- Coverage and analysis of CN issues and events
- Social media and networking services
- Censorship enforcement/Cyber Sovereignty
- Content Delivery Network (CDN) providers



Domestic/Near Region Multimedia Companies
IMPACT:
- CN buyouts of near-region media groups
- Direct publisher targeting/pressure for pro-Beijing stance
- Continued targeting of Taiwanese and Hong Kong media

9 Chinese Adversaries

10 Manufacturing



Engineering and Construction Industries
IMPACT:
- Private-sector targeting as CN SOEs replaced
- Project management know-how for shift of military projects to civilian companies
- Logistics and operations
- Manufacturing best practices and analysis

11 Agriculture

Crop/Animal Production
IMPACT:
- R&D on synthetic growth of crops and animal meat
- Near-region buyouts of cattle producers
- Organic/non-toxic pesticide chemical formulas

3 Chinese Adversaries

Government
Institutions dedicated to providing various gov't services at the national, state, or local level.

Healthcare
Provide goods and services meant to treat patients with curative preventive, rehabilitative, & palliative care.

Internet Services
Provide goods and services that operate & provide access to the Internet.

Manufacturing
Mechanical, physical, or chemical transformation of materials, or components into new products.

Media
Organizations whose primary purpose is to provide news coverage to the public.

Oil/Gas
Involved in the exploration, extraction, refining, transportation, & marketing of petroleum products.

Pharmaceutical
Organizations that develop, produce, & market drugs & pharmaceuticals.

Political
Entities responsible for the advocacy of specific political ideals.

Professional Services
Work that involves specialized education, knowledge, labor, judgment, & skill.

Retail
Organizations involved in the selling of goods via physical or electronic storefronts.

Shipping
Organizations engaged in the transportation of goods by means of high-capacity, ocean-going ships.

Telecommunication
Organizations that design, develop, & manufacture communications equipment.

Think Tank/NGO
Provide advice & ideas or advocate on behalf of specific issues such as politics, economics, or int'l relations.