2015 GLOBAL THREAT REPORT

INSIDE:

- Targeted Intrusions
- Criminal and Hacktivist Activity
- 2016 Predictions

CROWDSTRIKE

PROVIDED BY
THE CROWDSTRIKE
INTELLIGENCE TEAM

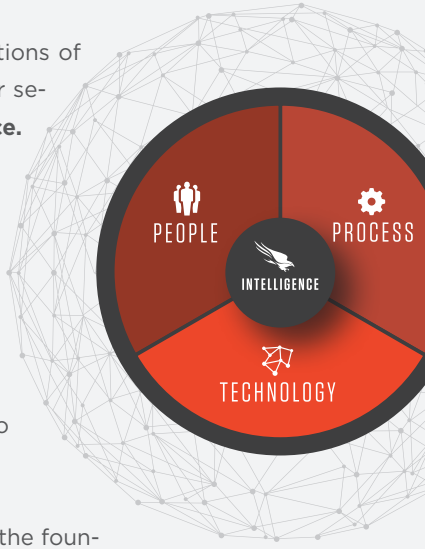
CROWDSTRIKE

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 It sounds like common sense, but it is something that is lost in the outdated discussion of people, processes and technology.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.

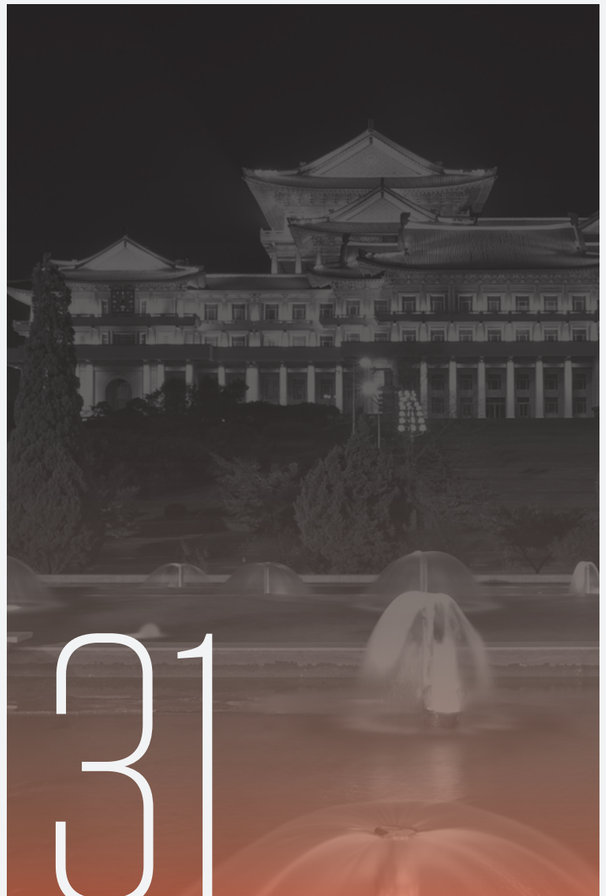
Emphasizing intelligence has been a cornerstone for CrowdStrike's approach to security since the foundation of the company five years ago: Providing cloud-based security powered by comprehensive, in-house threat intelligence. With our Falcon Platform and Threat Intelligence team, we have a unique bird's-eye 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.

George Kurtz. President, CEO & Co-Founder

CON-TENTS

2015 GLOBAL THREAT REPORT



INTRODUCTION

At **CrowdStrike**, a fundamental belief is that **intelligence powers everything we do.** It drives our **next-generation endpoint protection,** it fuels our **incident response** teams so they can resolve incidents faster, and it is consumed by our customers and their enterprise tools, allowing them to **detect** and stop attacks.

A well-known proverb captures the essence of intelligence: *In the land of the blind, the one-eyed man is king.* One who is better informed than his adversaries will have the advantage. Intelligence helps remove uncertainty from decision making; businesses around the world use various types of intelligence to ascertain what markets they should focus on, and how they should enter those markets. Intelligence about what personnel, which business units, or what products are being targeted by malicious threat actors can similarly aid in the decision-making process for the business. This transcends the security operations center and incident response measures. This information can help the business make more informed decisions, from the IT team, the C-suite, and even the board of directors.

Increasingly, organizations around the globe are using threat intelligence to make their enterprises smarter and more resilient. These organizations use threat intelligence to stay ahead of the adversary. As more and more organizations begin to utilize threat intelligence, the value in understanding what these threats mean to the business becomes evident. Intelligence powers everything we do, and it can power everything you do as well.

This year's CrowdStrike Intelligence Global Threat Report contains a wealth of intelligence regarding adversary behavior, capabilities, and intentions. More importantly, it ties it back to the events that influenced those activities. By understanding the events that shape the beliefs and motivations of threat actors—regardless if they are criminal, nation-state, or hacktivist—it is possible to comprehend what drove the adversaries to behave as they did, and perhaps to understand what this will mean for the future. The hope is that this report will provide a lens by which the reader can begin to view the world through the eyes of the attacker and use that information to stay ahead of the adversary—or as some might say, "to the left of boom".

CrowdStrike buckets more than 70 designated adversaries into three different motivations. These motivations—Targeted Intrusion, eCrime, and Hacktivism—can be influenced by a wide range of external factors. Targeted intrusion is most frequently executed by nation-states seeking to collect intelligence to facilitate public and private decision making. These nations have collected intelligence from private enterprises, non-governmental organizations, military and defense related businesses, foreign governments, and individuals deemed to be dangerous to the aggressor. Electronic crime (eCrime) is financially motivated activity by threat actors targeting any number of victims ranging from individuals to corporations. Targeted eCrime is an issue that is emergent and covered in the report as well. Hacktivism can pop up at any time, for any reason, anywhere; hacktivist actors may be nationalists, social activists, terrorist supporters, or pranksters.

This report is organized differently from our previous Global Threat Reports. In years past, the reports contained a review of notable activity followed by adversary-specific information, and they culminated in a looking forward section. These reports were contiguous and meant to be read from start to finish. This report is designed to flow more like a magazine; there are feature reports on various topics, smaller pieces meant to augment those topics, and profiles of select adversaries. The basic structure covers the three adversary motivations tracked by CrowdStrike: Targeted Intrusion, eCrime, and Hacktivism. This is followed by a review of predictions from last year's report to track how those predictions panned out, and what to expect for 2016.

Throughout the year, the **CrowdStrike Intelligence** team provides numerous intelligence summaries to customers with varying periodicity. These intelligence summaries are meant to memorialize what occurred in a specified period of time. It is our hope that by reviewing previous activity, we can begin to peer around the corner to predict what may occur in the future.

Adversaries are human; they have patterns, preferences, and short- and long-term plans. If we pay close attention, these patterns can lead to a better understanding of the mindset of the adversary, and ultimately allow us to know their next move. The ***Looking Forward*** section is a sample of the CrowdStrike Intelligence analysts, peering around the corner to see what the coming year may hold.

REVIEW OF 2014 PREDICTIONS

The 2014 Global Threat Report had many predictions based on analytic judgements about what might happen in 2015. We believe that when we make such assessments, it is a good exercise to review them each year so we can continue to improve our tradecraft.

LOOKING FORWARD

Adversary Operational Security
In the 2014 report, CrowdStrike assessed that the launch of the free SSL certificate service Let's Encrypt might have an impact on increased usage of secure communication protocols by adversary tools. Let's Encrypt did not launch as expected, and it only entered public beta in the final weeks of 2015. Even with the late 2015 launch, public reporting indicates that certificates from Let's Encrypt were misused in an Angler campaign within weeks of the public beta.

CrowdStrike also advised that it was possible that adversaries would deploy more sophisticated encryption schemes in 2015. CrowdStrike did observe a number of adversaries increasingly implementing Virtual Private Networks (VPNs), novel encryption schemes, and Point-to-Point encryption solutions in 2015. This dynamic by multiple actors was observed across all adversary motivations.

Increased Targeting of Embedded Devices
CrowdStrike assessed that we would see increased targeting of embedded devices by various actors. This is well highlighted by the actions of GEKKO JACKAL, who deployed a massive botnet using a weakness introduced by the Shellshock vulnerability on embedded routers, cameras, and other network-attached devices. Targeted intrusion actors were observed compromising Cisco routers and switches in victim environments, and an unknown actor has been tracked compromising embedded devices across the globe.

China Will Continue Conducting Espionage
CrowdStrike did not need a crystal ball for this one; we assessed that China would continue conducting espionage that supported objectives laid out in the 12th Five-Year Plan, supported their agenda in the South China Sea, and worked against an increasingly defiant Taiwan. We further assessed that China would continue to conduct attacks in support of "soft power" initiatives, from which efforts such as the Shanghai Cooperation Organization (SCO) and the Silk Road Initiative would benefit. All of these activities were observed throughout the course of 2015, with Chinese intrusion activity expanding in all directions to include increased targeting in support of anti-corruption measures implemented by the government under President XI.

Joint Plan of Action as a Catalyst
The CrowdStrike Intelligence team's 2014 predictions around Iranian intrusion activity vis-a-vis the success or failure of the JPOA were thankfully not tested. The prediction pertained to the likelihood that Iran would conduct retaliatory cyber attacks if the JPOA was perceived by Iran as taking a disadvantageous turn, or outright failing. Fortunately, neither of those scenarios came to fruition, even though the JPOA negotiation process took longer than expected and was arduous.

Furthermore, increased escalation of activity in Yemen by Houthi fighters and the military action of other nations diverted much of Iran's attention to that region. Further escalation in the Syrian civil war further distracted Iranian actors whose attention appears to have been focused on Gulf Cooperation Council (GCC) members, specifically Saudi Arabia.

Cyber Spillover from Regional Conflict
Ukraine, the South China Sea, Syria, and global energy prices were all identified in the 2014 report as being potential flash points for cyber activity. This was all very much the case in 2015. Ukraine was a hotbed of activity by a variety of Russian Federation-based adversaries who conducted extensive intelligence-collection operations and possibly even kinetic attacks using cyber means. The South China Sea continued to be an issue between various nations in that region as China continued to develop airstrips and naval stations in the contested atolls.

Chinese intrusion activity against Vietnam, the Philippines, and Taiwan occurred routinely as the Chinese sought to collect critical intelligence on potential repercussions of their aggressive posture. ISIS activity in Syria and abroad spawned numerous groups on both sides of Da'esh, who sniped at each other with compromises, data leaks, and disruptive attacks. The impact of economic sanctions and global energy prices surely had an impact on Russian intrusion activity, as it conducted operations against countries from the Commonwealth of Independent States (CIS), across Europe, and into the United States.

Point-of-Sale Attacks in the Wake of EMV
CrowdStrike assessed that the instances of point-of-sale (PoS) malware would sharply decline as EMV became the predominant technology in the United States. In October 2015, many payment processors implemented a fraud liability shift for vendors not supporting EMV technology. This technology does make commodity PoS malware as it existed ineffective—an unforeseen occurrence, despite increased usage of PoS malware at the end of 2015. As criminals realized that the PoS tools they had developed would be rendered useless, they rapidly deployed their malware in a last-ditch effort to collect as much data as possible.

Destructive and Disruptive Attacks
CrowdStrike, as expected, observed an increase in disruptive and destructive attacks. The lion's share of these attacks was conducted by hacktivist actors conducting DDoS attacks for a variety of motivations. Attacks by extortionist actors such as PIZZO SPIDER, MIMIC SPIDER, and other copycat groups became an almost-daily occurrence, moving from Bitcoin businesses to large-scale financial and technology companies. Ransomware also increased substantially in distribution and variety over the course of 2015, a constant threat with the potential to devastate anyone from an individual, small/medium business up through massive enterprises. Destructive attacks by nation-state actors continued through 2015, with activity by VOODOO BEAR dominating the headlines toward the end of 2015.

R&D

A key component of understanding the threat landscape and where it is going is to observe the direction of security research. Tomorrow's exploitable vulnerability or security bypass is likely being explored by researchers today. Time and time again the security community's research has been picked up by savvy attackers and forged into a weapon used by adversaries to achieve their goals.

In 2015, issues with encryption dominated the headlines of attacks, as well as being relentlessly tested by security researchers seeking to find flaws in these systems that protect our personal data and business secrets. Secure boot processes are a key component of trusted computing; if the boot process has been compromised, then it's game over.

Over the years, an arms race has been raging between system designers and researchers driving down to the silicon chips that support the boot process, exposing previously unknown flaws in software that we rely on every day. This leads to enhanced protections, and in some cases, wily attackers can use the flaws to compromise systems at a very low level.

Virtual Machine computing is another area of intense research. In the last year, it became apparent here, too, that low-level drivers and code to support antiquated devices could diminish the security of the overall system. With these research stories slowly percolating into the mainstream media, it is important to keep an eye on novel research that may lead to critical exposures in the future.

x86 System and Firmware Security

After seeing adversaries deploy Basic Input Output System (BIOS) implants for some time, the topic of system and firmware security seems to have finally arrived in mainstream security discussions. The Hacking Team leak revealed them to be developing a BIOS persistence implant deployed via physical access; other government-backed actors such as ENERGETIC BEAR have also been observed by CrowdStrike Intelligence to scout BIOS dumps after remote system compromise, potentially enabling BIOS implantation. Besides deploying BIOS implants after remote compromise, ensuring the integrity of a system after physical access due to border inspections or supply chain interdiction is a growing concern for many medium- and high-ranking business officials.

> “TOMORROW'S EXPLOITABLE VULNERABILITY OR SECURITY BYPASS IS LIKELY BEING EXPLORED BY RESEARCHERS TODAY.”

Modern flash chips that store BIOS images, colloquially known as Read Only Memory (ROMs), should be write-protected after system boot to protect against simple firmware reflashing attacks, which can occur after privileges have been escalated in the running operating system. Even with such protection, vulnerabilities in the boot process (or sometimes after the boot process) can be exploited to circumvent this simple write-protection. Pedro Vilaça uncovered a vulnerability in how Apple OS X manages flash chip write-protection: Upon resume after suspend-to-RAM, the boot code failed to ensure write-protection, effectively leaving the flash chip unprotected following the first suspend-resume iteration. Since a suspend can generally also be triggered by malicious software running on the system, this effectively enables BIOS implant deployment after remote compromise.

Polish security researcher Joanna Rutkowska covered the state of establishing a trustworthy boot chain on the x86 architecture in a much broader analysis in her excellent paper “Intel x86 considered harmful”. While her analysis paints a rather grim picture of the current state of affairs, it is an accurate picture of analysis from a paranoid perspective.

The Purism company attempted to create a “fully liberated” laptop that did not depend on any binary or closed-source firmware for any of its components. However, to date they have not managed to “liberate” the different firmware packages required for running modern Intel processors (see also Rutkowska’s analysis of Intel ME and associated binary blobs). Google Chromebooks rely on the open-source Coreboot firmware for initializing the system and can be seen as fully open-source boot chain implementation. Yet even they have to rely on binary blobs supplied by Intel to support chipset and processor initialization and memory training. Multiple researchers are actively working on reverse engineering Intel ME firmware binary blobs, and CrowdStrike expects more publications on this in 2016.

It appears impossible to create a fully user-controlled boot chain on x86 going forward, and it is expected that there will be further research into the closed binary blobs and uncovering of associated vulnerabilities.

A new extension to the Intel processors called Software Guard Extensions (SGX) has been gaining attention by security researchers. SGX was designed to bootstrap a trusted enclave in an untrusted ecosystem (such as cloud computing), but it may also be abused for Digital Rights Management (DRM) or rootkit purposes according to multiple researchers’ assessments. As the first processors implementing SGX become available in 2016, CrowdStrike expects offensive and defensive research leveraging this technology to follow suit promptly.

State of the TLS Ecosystem

Transport Layer Security (TLS) is the centerpiece of modern connected systems providing a secure communication protocol. As such, it was not surprising that 2015 saw a wealth of attacks on the TLS protocol. During the same time, standards bodies were actively improving the protocol and phasing out old and insecure aspects of it in order to help mitigate possible attack surface.

ATTACKS AND INCIDENTS

Throughout 2015 numerous notable events took place that demonstrated potential misuse of TLS and possible implications of such misuse.

- In February 2015, it was revealed that computer maker Lenovo had been pre-installing the Superfish Visual Search software on its computers running Windows. This software installed a static TLS root certificate authority (CA) and corresponding private key into the system, thereby placing every user at risk of being attacked via a Man-In-The-Middle attack on the TLS protocol. Lenovo published an apology to its users and released a removal tool as open-source software. Later in 2015, it was discovered that Dell had also been pre-installing a root CA and key on its Windows machines, resulting in the same security risks for users.
- In March of 2015, the Chinese root CA CNNIC was removed from some major browsers after a security incident was revealed by the Google Chrome team. CNNIC had issued a full root CA certificate to a third party that had used it for testing in network equipment designed to do transparent TLS interception.
- March 2015 also saw the first large-scale attack of the so-called Great Cannon of China. In this incident, unsuspecting international visitors of the Baidu search engine had malicious JavaScript injected into their connection. As CrowdStrike pointed out at BlackHat USA 2015, this attack would have been impossible with HTTPS in place, a lesson that many large Chinese companies have not yet taken to heart.
- In December, the government of Kazakhstan announced that it would require Internet users to install a custom root CA certificate, thereby making it possible for the government to intercept all of the HTTPS connections of its citizens.

One alarming trend is for security software, such as anti-virus programs, to do TLS interception and inspection by installing their own certificate into the browser root CA store. While these tools generate a certificate for each installation, they sometimes introduce other weaknesses.

During a survey, it was discovered that commonly used AV software such as Avast, Kaspersky, and ESET would degrade the security of TLS by being susceptible to the FREAK and CRIME attacks. This is facilitated by not implementing HTTP Public Key Pinning (HPKP) or Online Certificate Status Protocol (OCSP), stapling, and in general supporting older, less-secure ciphers. Due to the difficulty of implementing TLS correctly, it is perhaps not surprising that running additional software to do TLS interception increases the attack surface of a system.

New Developments
On 3 December, the first free and automated TLS Root Certificate Authority launched to the general public. Called Let's Encrypt, it offers free certificates for manual and automated consumption. Contrary to existing CAs, it does not require any manual interaction to get or refresh a TLS certificate for a website, which is why certificates issued by Let's Encrypt will only be valid for three months.

The HTTP/2 specification was finalized by the Internet Engineering Task Force (IETF) in May 2015 (RFC 7540). It is a major overhaul of the venerable HTTP protocol that will greatly increase the performance of resource-heavy interactive websites and speed up browsing for mobile users. While the IETF working group refrained from making TLS/HTTPS (and thus encryption) mandatory for HTTP/2, a number of browser vendors have already announced that they will only support HTTP/2 with HTTPS. Support for HTTP/2 already exists in major browsers and web servers, but it remains to be seen whether the added functionality will result in new vulnerabilities. HTTP/2 will require less performance trickery by application developers, and it makes dedicated external Content Delivery Networks (CDNs) for JavaScript less attractive.

In April 2015, the Public Key Pinning Extension for HTTP (HPKP, RFC 7469) was published by the IETF. This is an HTTP header which tells browser to "pin" a public key certificate for the current website, only accepting this particular certificate for a specific time range. Used correctly, this extension will make intermittent TLS Man-In-The-Middle practically impossible.

In January, the Certificate Transparency project by Google started to be made mandatory for Extended Validation (EV) certificates in the Chrome browser. This project, which is basically a verifiable log of issued certificates, will make it impossible for a CA to issue a certificate without the rightful domain owner becoming aware of it.

Other software on the web landscape is also creating a noticeable incentive for the adoption of TLS/HTTPS. The HTML5 ServiceWorker spec will enable fast, near-native online and offline applications, but it will only work on HTTPS websites. The Chrome browser will now display mixed-content warnings (HTTP and HTTPS content) like plain unencrypted websites. W3C initiatives like Subresource Integrity (SRI) and the Content Security Policy 2.0 (CSP), both actively developed during 2015, greatly increase the security and robustness of web applications. Furthermore, these measures can mitigate some of the inherent risk emanating from insecure websites. In 2015, multiple (free) services appeared that aid users in checking for insecure web-server and header settings and offer ready-made configuration snippets to achieve A-grade TLS security without much effort.

Changes to the Protocol
The IETF is currently in the process of developing version 1.3 of the TLS protocol. While TLS v1.3 is still in draft state, a number of promising improvements have already emerged. TLS v1.3 will no longer support any type of handshake that does not offer perfect forward secrecy (PFS). A number of cryptographically weak ciphers and options will be removed in v1.3. In terms of performance, TLS v1.3 will also enable faster handshakes that use fewer round trips between client and server. This will greatly increase performance, thus further driving TLS adoption.

Looking Ahead
While an automated and free CA will hopefully drive the adoption of TLS, it can also be used for malicious purposes. The end of 2015 already saw Let's Encrypt being employed for malicious ads. Our prediction for 2016 is that we will encounter more incidents where actors leverage the ease and anonymity of creating TLS certificates to enable attacks and hide their tracks. With a valid TLS certificate, malicious content can be referenced across domains without triggering mixed content warnings. If an attacker can host content on a subdomain of a legitimate business, he will be able to create a TLS certificate for that domain that will look authentic to a user. Traffic protected by TLS can bypass systems like an IDS more easily, as it is encrypted. As the "green lock" of TLS-protected websites become more prevalent on the Internet, users will have to be educated that it does not imply trustworthiness of the site. In the face of these challenges to network-based security solutions, next-generation endpoint protection will become even more critical to enterprise security.

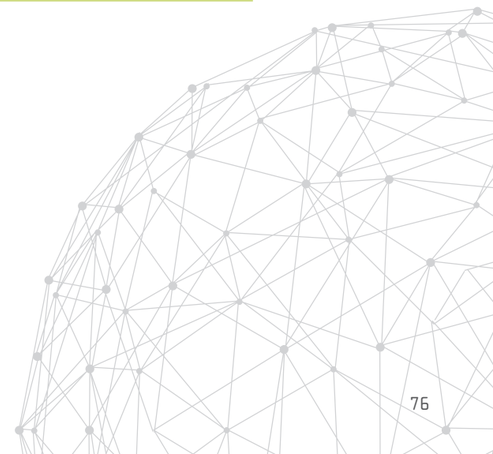
CONTAINER AND VIRTUALIZATION SECURITY

In 2015, virtualization was still the go-to technology to achieve multi-tenancy for a number of applications. Dozens of companies have emerged that either offer such infrastructure as a service or provide solutions for monitoring and managing the ever-growing fleet of virtual machines. It is not surprising that the demand for secure deployment guidelines has surged.

Containers
Another emerging trend in terms of multi-tenancy is the containerization of applications. Containers are not as heavyweight as VMs, and thus are easier to set up and significantly more resource effective than VMs on shared hardware. For many users, the only reason to employ VMs is the perceived lack of isolation that popular container software offers at this time. Providing a secure isolation layer will be paramount for driving the future adoption of containers.

Docker is a container solution built on recently added features of the Linux kernel, and it is arguably the most prominent and widely used

"IN THE FACE OF THESE CHALLENGES TO NETWORK-BASED SECURITY SOLUTIONS, NEXT-GENERATION ENDPOINT PROTECTION WILL BECOME EVEN MORE CRITICAL TO ENTERPRISE SECURITY."



container software today. There has been some confusion as to the purpose of Docker containers and the level of isolation these can offer. Since applications can easily escape Docker containers under certain circumstances, even proponents of containers have gone so far as to point to VMs for isolation of possibly malicious code.

From the attacks on the Docker ecosystem and the ensuing discussions in the community, it is apparent that users are frequently not educated about the implications of running containers with potentially malicious code. Currently, the lack of support for user name-spaces in Docker means that it is easy to inadvertently run an application inside a Docker container as root. In 2015, Docker also added signature verification for images, a feature that enterprise customers had been waiting for.

The Docker container ecosystem offers a way for users to share the containers they created via the so-called Docker Hub. This repository holds a large number of pre-installed Docker container images, both from official software vendors as well as regular users. Users can typically expect to find an existing Docker image for the software they want to run inside a container.

In May, there was an automated survey of the official Docker images, i.e., those from the actual software vendors. It found that about 40 percent of the images suffered from severe vulnerabilities that were discovered and fixed in the course of the previous year (e.g., Shellshock, POODLE, Heartbleed).

Docker itself saw a number of Common Vulnerability and Exposures (CVEs) assigned in 2015, most of them relating to ways the container could either disable or circumvent Linux security models and affect the host system. The Docker Engine is the actual software behind Docker that is responsible for creating and managing containers on a host system. Because of the power that the Docker Engine wields with regard to the host system, tools instrumenting it will be a prime target for attackers.

Virtual Machines

There have been a number of critical advisories related to virtualization technology such as Xen and KVM. For Xen, there were 10 advisories in 2015 that described a way for the guest OS to escape its confinement, potentially compromising the host system. Another 15 advisories described various ways for guests to perform a Denial of Service (DoS) of the host system.

In May, CrowdStrike discovered a vulnerability in Xen that allowed x86 HVM guests to escape to the host system through the QEMU floppy disk controller. The vulnerability was patched as part of XSA-133. Like other privilege-escalation vulnerabilities, this one affected more than one virtualization solution since it originated in the QEMU emulator, which is used by multiple projects such as Xen, KVM, and VirtualBox. Other companies came forward with similar bugs, showing the vested interest that a wide range of industries has in keeping the security model of VMs robust and intact.

BlackHat USA 2015 and DefCon featured talks on cross-VM covert channel communication using the CPU. These kinds of attacks are certainly quite complex and may be hard to execute, yet they show the multitude of potential pitfalls for providers offering VMs to users.

Looking Ahead

CrowdStrike expects a number of new challenges to arise as a result of an increased adoption of containerization technology. The most obvious one will be the fact that more developers and users will use containers for external reasons. Efficiency and the continuous march toward virtual appliances and cross-platform deployment will drive increased adoption of these technologies.

Currently, the user base of containers can probably be described as “educated early adopters”, while future generations of users might not be so savvy. As a result, there will likely be cases where insecure software inside of containers is not updated because users lack the knowledge to do so or because they don’t understand the security implications. Current operating systems frequently offer automatic updates for software installed through system facilities, such as shared libraries or servers. Containers, on the other hand, require a different approach to dealing with the update process. Even if the need to update is evident to the user, it remains to be seen whether container and software deployment processes can keep up with the pace of security issues.

TARGETED INTRUSION: CHINA

2016 looks to be a pivotal year for China-based, state-sponsored cyber adversaries as China enters a transformational period in terms of its economy, its global status, and the cyber methods it uses to achieve its strategic goals. This is most easily discussed by separating out Chinese intentions in cyberspace, the changing dynamics of Chinese cyber operators, and China’s new Five-Year Plan (FYP).

Chinese Intentions in Cyberspace

For China, cyber operations have previously been a relatively inexpensive means to some of these strategic ends: It has conducted cyber reconnaissance on its neighbors to make calculated territorial maneuvers; used extensive cyber monitoring capabilities to simultaneously suppress dissidents and manage a growing population of domestic Internet users; and conducted cyber espionage in order to steal intellectual property, fill technological gaps, and maintain its impressive economic growth.

Efforts by the private sector and the U.S. government to expose Chinese cyber operations over the past several years has raised the cost of these operations both from a financial as well as an economic perspective for Beijing, and in 2015 it came to a boiling point. The threat of U.S. economic sanctions and potential diplomatic fallout appears to have finally forced meaningful dialogue between governments.

If observed campaigns in late 2015 were any indication, it is unlikely China will completely cease its cyber operations, and 2016 will show the new direction it is headed. Although China and the U.S. signed a cyber agreement and restarted cyber dialogue between the two nations following President XI’s September 2015 visit to Washington, the wording was described by most analysts as extremely vague and largely open to interpretation. A short time later, China sought to sign identical agreements with the UK and Germany, and even sought to normalize a similar agreement at U.N. proceedings not long after.

Beneath the surface, however, China has not appeared to change its intentions where cyber is concerned. This is best illustrated by how Beijing treats its allies as opposed to its rivals. Whereas the agreements that China has been attempting to normalize specify not hacking for economic espionage purposes, China signed a May 2015 pact with Russia, a known ally, with both sides abolishing malicious hacking of any type against one another. Yet CrowdStrike actually observed an increase in activity against Russian targets from HAMMER PANDA directly following the agreement. The Russian targeting continued over several months after the friendly agreement had been signed, suggesting that Chinese intentions are far removed from the agreements they sign, even with allies.

China was also observed targeting the website of the Permanent Court of Arbitration in the Hague during a week-long hearing on its SCS dispute with the Philippines. The tribunal was intended to be a neutral ground to resolve international disputes, but Beijing refused to acknowledge the

case as valid, instead infecting the website and potentially any victims interested in the landmark case. This further shows Chinese intentions to continue to use cyber as a means to gain the upper hand in any international disputes, even when the victim is an impartial judge designed to equalize opponents and prevent bullying.

Observed activity has shown that China may change tactics and reduce its cyber activity when under close inspection. Examples of these reductions are apparent in the drop-off of COMMENT PANDA activity after the May 2014 PLA indictments, or the cessation of PUTTER PANDA following the public release of CrowdStrike's analysis of their activity in June 2014. China has demonstrated that their operators will resume normal activities when scrutiny has diminished. The cyber agreements appear to be an attempt to appease the U.S., avoid economic sanctions, and offer a chance for China to seize upon a global initiative to "normalize" sanctioned cyber activity. China has promised new cyber tact, however the reality of its intentions is far divorced from what it has promised. Given its remaining technological gaps and the strategic edge cyber can provide its economy, there is still plenty of incentive for China to engage in commercial cyber espionage when opportunities arise.

The Shifting Dynamics of China's Cyber Operators

A reduction in activity by China-based adversaries in 2016 is possible; such a reduction would be indicative of a shift in the way China goes about cyber espionage. The cyber agreements come at a time when President XI has been preparing a massive military overhaul that would see a bloated PLA trimmed and more resources distributed to the PLAAF and PLAN. President XI has said that a joint-command structure similar to the U.S. military is necessary to provide China with a modern, nimble fighting force capable of defending China's territory. This carries obvious implications for enforcing China's interests as well as defending them from a physical standpoint, and will likely make the SCS a continued flash point as the reorganization will likely allow Chinese military forces more mobility and faster response times to potential conflict.

The reorganization may also split China's military cyber forces into their own division and likely serves the dual purpose of revamping China's cyber forces at a time when more oversight is needed while giving the impression of a reduction in U.S. targeting. CrowdStrike has frequently observed duplicated collection efforts by multiple groups, indicating relatively little oversight or coordination between units. At present, preventing an outright violation of the cyber agreement with the U.S. is a high priority for China, as economic sanctions would place a severe strain on its already-troubled economy. The potential embarrassment of soldiers moonlighting as contractors and carrying out operations on behalf of Chinese companies has likely prompted a significant drop in normal activity by Chinese military operators as they undergo a fundamental shift in how they carry out operations.

This reorganization will not happen overnight. It is slated for completion by 2020; however, cyber will likely be a priority due to China's emphasis on winning informatized wars, meaning that the shift may be observed soonest in that arena. Potential signals that the reorganization has made China's cyber forces more efficient would include improved tradecraft, better sharing of tools between groups, and coordination on targets.

As China's military cyber forces undergo changes, China will likely increase its reliance on its civilian intelligence agencies and associated contractors, all of which generally employ better tradecraft. This includes the Ministry of Public Security (MPS), which has already seen some monumental changes to its mission in 2015 such as increased overseas operations, as well as the Ministry of State Security (MSS), which has typically employed top-tier contractors. To illustrate this point, DEEP PANDA, which CrowdStrike associates as being one of the non-military cyber organizations China regularly uses, has engaged in activity across a wide variety of sectors since the cyber agreement with the U.S., and it is expected to continue to do so.

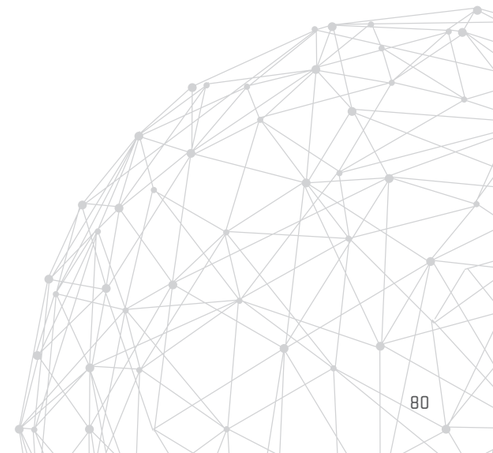
Overall, Chinese cyber activity may shift dynamics, but it is not expected to cease anytime soon. Beijing views winning informatized wars as integral to its rejuvenation as a "great nation", and despite the promotion of domestically sourced innovation and technologies, China still has numerous intelligence gaps that cyber espionage can assist in filling to accomplish its long-term strategic goals. A cessation of intrusions associated with China is unlikely.

China's 13th Five-Year Plan

Notably, China's economy has reached a tipping point as it looks to maintain medium/high growth trajectory and to better satisfy its exponentially growing middle class with better access to quality food, affordable healthcare, and job opportunities. President XI and senior officials have frequently alluded to economic reforms multiple times in the past two years, highlighting that the CCP recognizes a troubled economy constitutes one of the largest threats to party rule. China will look to transform its global status as an exporter of cheap goods (i.e., "Made in China") to that of a domestic powerhouse and innovator.

China also suffered two serious embarrassments on a global scale: the Chinese stock market crashes in mid-2015 and its issuing a pollution red alert for Beijing during the Paris climate talks. Both of these events showed significant weaknesses where China has been looking to brand itself as a global leader, and it is likely that China will seek to avoid any further incidents that reflect negatively on China in the financial and energy sectors.

"CHINA SIGNED A MAY 2015 PACT WITH RUSSIA, A KNOWN ALLY, WITH BOTH SIDES ABOLISHING MALICIOUS HACKING OF ANY TYPE AGAINST ONE ANOTHER.YET CROWDSTRIKE ACTUALLY OBSERVED AN INCREASE IN ACTIVITY AGAINST RUSSIAN TARGETS FROM HAMMER PANDA DIRECTLY FOLLOWING THE AGREEMENT."



These factor heavily into the first draft of China's 13th Five-Year Plan, which was released in November 2015 and will be finalized in early 2016. These plans typically provide a roadmap for what China will target using cyber means. Alternative energy and domestic technological innovations will have a renewed focus as China looks to transform its standard of living and become less reliant on foreign technology. This will likely resonate with Chinese citizens as increased opportunity, both in terms of everyday prospects and entrepreneurship, which the CCP is promoting heavily along with private sector/military cooperation as a way to stimulate growth and innovation.

The combination of China becoming increasingly untrusting of western information technology and a desire to promote its own sectors of industrial manufacturing and retail may lead to a gradual tapering off of targeting against these sectors. However, it will also likely mean increased cyber targeting in areas like agriculture, healthcare, and alternative energy 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 know-how such as building native supply chains and administrative expertise. The targeting of U.S. healthcare institutions in 2015 was suspected to be for espionage purposes, though it may have had the dual purpose of providing western models for supplying affordable healthcare to citizens as China looks to modify its current healthcare system.

It is no coincidence that a plethora of key state projects have completion goals of 2020. 2021 will mark the 100th anniversary of the founding of the CCP, and the party intends to have myriad successes to present to the Chinese people in order to reinforce its political legitimacy. These projects and targets are wide ranging, with some very specific goals (e.g., achieve a 60 percent urbanization rate, complete the Chinese space station, reveal a domestically produced aircraft carrier, double 2010 levels of growth) and some extremely vague goals (e.g., become an "Internet Power" and become a "moderately well-off society"). However, there are several stated goals that have strategic and economic implications for several sectors.

The included infographic gives a further breakdown of potential targets across sectors based on China's 13th FYP and its strategic projects that are slated for completion by 2020.

RUSSIA

The Russian National Security Strategy, released on 31 December 2015, both establishes the plans the leadership aims to implement throughout 2016 and reflects the desire for the nation to realign its interests, focus domestically, and improve its influence and standing. A realignment of interests orients Russia eastward toward China and India and places a greater focus on regional partnerships, such as the Collective Security Treaty Organization (CSTO), as it distances itself from NATO. This shift portends further military joint training engagements and may also be either complicated or reinforced by attempts at intelligence collection associated with nations in Russia's sphere of interest.

The domestic focus alluded to in the strategy is multifaceted, but in terms of technology the nation is poised to increase investments in the technology sector. Some of these investments were announced or had already begun in 2015 as reports of intent to develop mobile operating systems and nationally developed hardware proliferated. Supplementing the growth in the national technological sector will be the increasing internalization of data resources and application of control over content. In 2015 Roskomnadzor, Russia's communication, information technology, and mass media service, had enforced legislation governing how private data of Russian citizens' information is handled. The service cracked down on foreign companies who operate in Russia and do not comply. Per legal guidance, companies that possess data belonging to Russian citizens must provide the government access to the data or house their servers within Russian territory. In terms of content control, Russia has surreptitiously employed teams of online bloggers, commentators, and "trolls" to disseminate false information, drown out the voices of legitimate users, and direct discussion in a manner chosen by the government. Operating under the broad moniker "Internet Research Agency," these operators have employed their techniques following high-profile events such as the assassination of political activist Boris Nemtsov in late February, and they are expected to continue their operations throughout 2016.

Additionally expected in 2016 are domestic deployments of systems that may allow expanded government control of online resources. GosSOPKA is a government system reportedly designed to detect and eliminate computer attacks. First imagined in 2013, GosSOPKA is intended for development and management by the FSB. It potentially supplements existing forms of online overwatch such as SORM, but it also adds an aspect of real-time defense.

GosSOPKA began its initial implementations in 2015 on Ministry of Economic Development network resources. Wider plans for distribution in 2016 and beyond include government agencies as well as Russia's diplomatic offices and consular bureaus located overseas.

In an effort to improve status and influence, Russia is still expected to project military power in the form of bomber training flights and joint military exercises, but these will likely be seen less frequently than in 2015 due to economic challenges faced domestically. Improvement of the economy was a major talking point within the strategy and a large portion of Russia's focus on domestic issues. The improvements will most likely come in concrete forms such as sales of natural resources, but also in terms of changes to financial policy and development of partnerships for domestic investment. These shifts will most likely necessitate information for decision making, and therefore they portend increased intelligence collection by Russia-based adversaries particularly against regional targets and global energy companies.

IRAN

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.

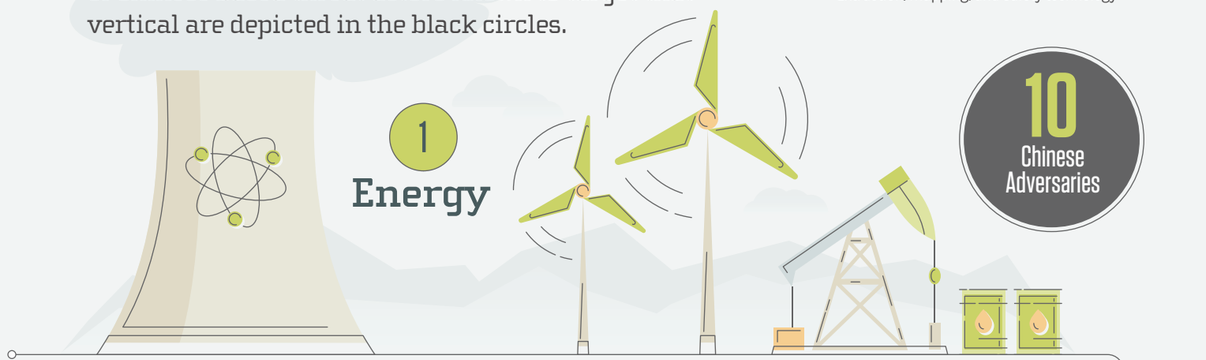
It is likely, too, that Iran will also conduct increasing domestic cyber espionage operations to be vigilant of any influence of western ideals on Iran, threatening its Islamic culture. Subsequently, it is also likely that arrests of Iranians for content offensive to Islam or threatening to the Iranian government (both statements that are broad in application to activities) will increase as more technical apparatus is put in place to monitor and censor network traffic.

Furthermore, the Iranian government will almost certainly be concerned about the contents of any reports from investigative regulatory bodies on Iran's continued compliance with the nuclear agreement. The relief of sanctions from the JCPOA is of vital importance to Iran and its economy. During the JPOA negotiations through 2014 and into 2015, Iranian adversary

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

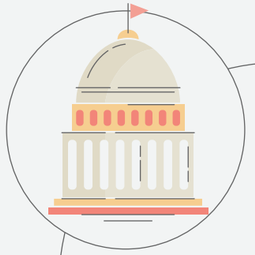
2 Transportation

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

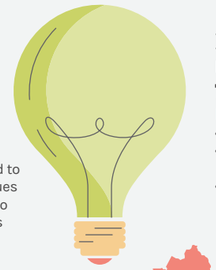
Airlines
IMPACT:
- Passenger Name Records
- Mergers and Acquisitions Information
- Logistics/Operations/Processes information
- Route Information



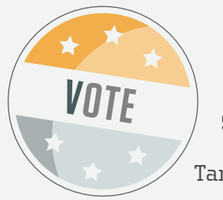
3 Government

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

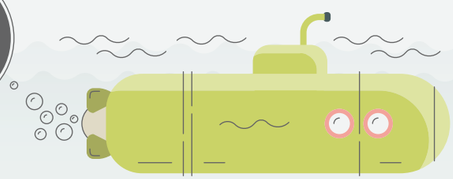


Special Event Targeting
IMPACT:
- Olympics VIP intelligence
- US Candidates/Elections
- G20/G8

4 Defense/ Law Enforcement

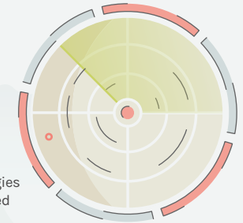
28 Chinese Adversaries

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

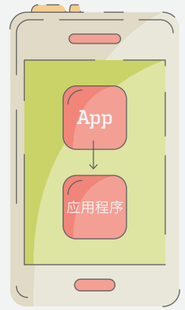
Intelligence
IMPACT:
- Signal Intelligence/Cyber Integration
- Theft of Sensitive Personal Identifiable Information
- Organization Structures/Tradecraft knowledge

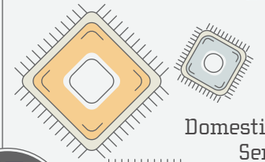


5 Technology

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.

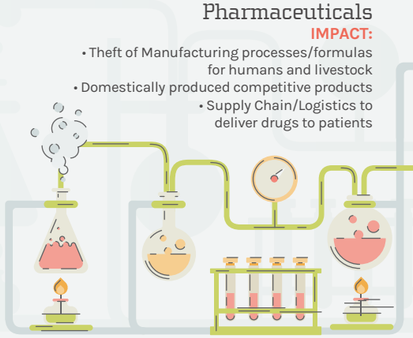
Gaming
Organizations involved with the development, marketing &sales of video games.

9 Chinese Adversaries

Pharmaceuticals

IMPACT:

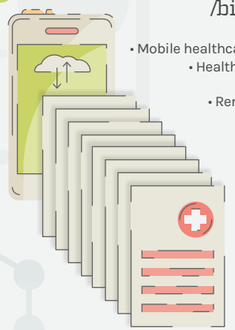
- Theft of Manufacturing processes/formulas for humans and livestock
- Domestically produced competitive products
- Supply Chain/Logistics to deliver drugs to patients



Health technology /biomedical

IMPACT:

- Mobile healthcare technology
- Healthcare/National ID technology
- Remote Medicine



6 Healthcare

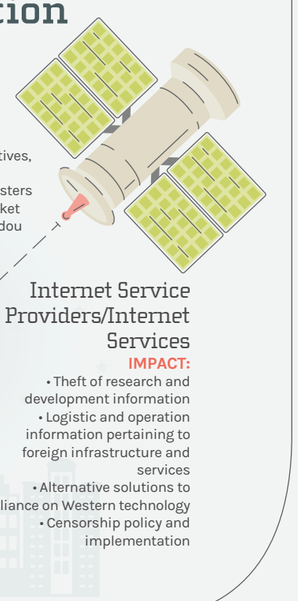
Health Insurance systems

IMPACT:

- Healthcare insurance/delivery
- Multi-layered medical security network
- Theft of technology/software used by insurance industries

14 Chinese Adversaries

7 Telecommunication



Diplomacy

IMPACT:

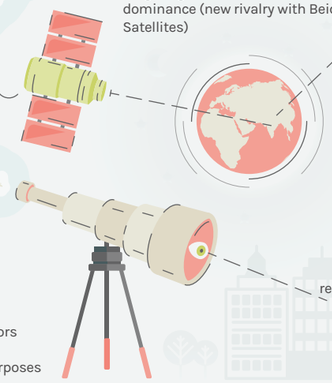
- Policy and analysis related to building/transportation projects with CN
- Silk Belt and Silk Road initiatives/agreements
- South China Sea development

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:

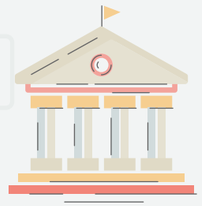
- Theft of research and development information
- Logistic and operation information pertaining to foreign infrastructure and services
- Alternative solutions to reliance on Western technology
- Censorship policy and implementation

Private cellular mobile communication providers

IMPACT:

- Relationship with CN state-owned operators
- Merger information
- Infrastructure targeting for espionage purposes

8 Financial

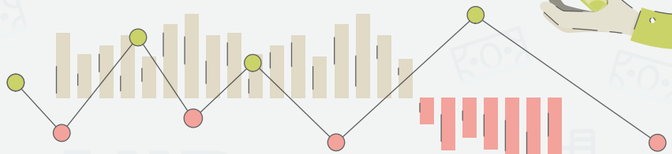


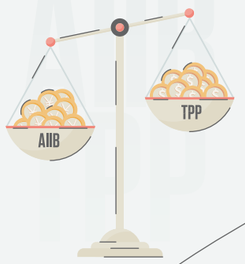
International Financial Organizations

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



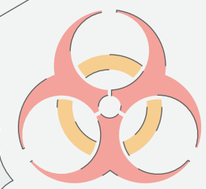


Think Tanks

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

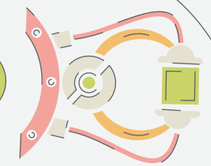
Domestic/Near Region Multimedia Companies

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:

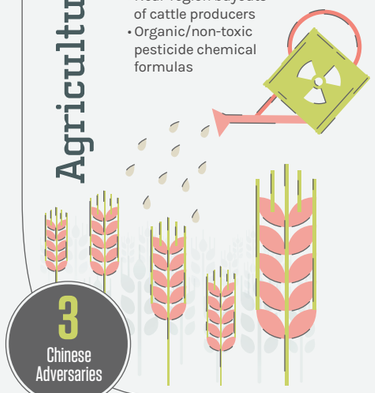
- Private-sector targeting as CN SOEs replaced
- Project management know-how for shift of military projects to civilian companies
- Logistics and operations
- Manufacturing best practices and analysis

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.

ROCKET KITTEN was observed continuing to target European and regional targets in cyber espionage campaigns with the likely intent (at least in part) of obtaining an advantage in the negotiating process. Thus, reporting associations, receiving parties, and third parties such as host governments for meetings should expect it is likely they would be included in targeting by Iranian cyber espionage operations for knowledge gathering. The threat is increased if Iran violates, or is accused of violating, the JCPOA and risks the re-establishment of economic sanctions.

Lastly, as assessed once evaluating the U.S. Government report in June 2015, Iran separates its nuclear policy (and the JCPOA agreement with the P5+1 countries) from its foreign policy in the Middle East. Through 2014, regardless of ongoing nuclear negotiations, Iran continued to support Lebanese Hezbollah, a number of Iraqi Shia militant groups, Hamas, Palestine Islamic Jihad, and the regime of Syrian President Bashar al-Assad. Although the report was from 2014, U.S. officials claim the activities continued into 2015. Additionally, Iran is also strongly suspected of providing various means of logistical and financial support for the Zaidi Shiite insurgent group known as the Houthis throughout 2014 and 2015.

There are no indications that the Iranian government will shift from its current foreign policy supporting the aforementioned groups. Specifically, there are increasing tensions between the two regional powers of Iran and the Kingdom of Saudi Arabia (KSA) that increase the likelihood that Iran would use its proven cyber capabilities in 2016, targeting Saudi Arabia and regional governments that are becoming involved in the two countries' dispute by choosing to align with Saudi Arabia.

One escalating tension is the Yemen conflict, in which Iran has supported the Houthi rebels against a Saudi-backed Yemeni government in exile. The Saudi-led coalition announced on 2 January 2016 that the 15 December 2015 cease-fire agreement, which had been violated multiple times by both sides, would end on that day at 1100 GMT, meaning the conflict is far from over. A Saudi Arabian air strike on 8 January 2016 resulted in the near-bombing of Iran's embassy in Sanaa, Yemen. Erroneously, Iran media first reported that the embassy had been hit during the air strike.

On the same day as the end of the Yemeni cease-fire on 2 January 2016, Saudi Arabia executed Shiite cleric Nimr Al-Nimr. Sheikh Al-Nimr had been charged with instigating unrest while he participated in protests against the Saudi government during the Arab Spring in 2011. Al-Nimr was convicted in October 2012, sentenced to death, and had been scheduled for execution with 46 other prisoners at an undetermined date.

Following the executions, Iranian protestors—motivated by the execution of a prominent Shiite cleric and seeing the action as an offense against Shiite Muslims by the Sunni-ruled Saudi Arabia—attacked the Saudi Arabian embassy in Tehran. Saudi Arabia was forced to remove its diplomatic personnel from the embassy. Adding to the tensions, the governments of Bahrain, Sudan, Qatar, Kuwait, and the United Arab Emirates (UAE) also severed or downgraded diplomatic ties in support of their alliance with Saudi Arabia.

With the regional tensions heading into 2016, there is increased likelihood Iran would 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. This would likely occur for a few primary reasons: to conduct network reconnaissance activities to prepare for any future offensive or retaliatory cyber operations; to conduct retaliatory cyber operations damaging or destroying networks; or to obtain information to answer any current intelligence gaps of its enemy's political strategies, military objectives, and mission details. The lifting of sanctions will likely improve economic conditions in Iran and make infrastructure and technology purchases significantly easier. This potentially foreshadows an increase in both augmented capabilities and the ability to operate more globally for Iranian threat actors.

NORTH KOREA

While the Democratic People's Republic of Korea (DPRK) has been involved in offensive cyber operations since at least 2009, the activity identified in 2015 suggests a growing confidence to leverage such operations for espionage purposes during periods of heightened tension.

China has been historically inconsistent in directing North Korean behavior, recently publicly condemning nuclear tests but privately providing more aid, while fearing any escalation that could lead to a spillover of North Korean refugees into Chinese territory. China has been the DPRK's number one source of aid and trade in recent years, and potentially a gateway for North Korean cyber operations; however, its increasing responsibility in the global community consistently puts it at odds with protecting the rogue state. The DPRK has been observed increasing its ties with the Russian Federation, potentially reducing the influence Beijing has over the rogue nation.

A major shift in Chinese support may cause the DPRK to seek more a more aggressive cyber posture, on the high end as a preparation for military readiness and on the low end as a means to reiterate its demands on the international stage by provoking western powers. It also cannot be dismissed that DPRK cyber operations may further branch out into criminal activity as a way to increase the regime's financial position.

Monetization of cyber intrusion is consistent with the responsibilities of the so called "3rd floor" bureaus, which have participated in illegal drugs, counterfeiting, and other illicit activity. The cyber agreement between the U.S. and South Korea is only likely to exacerbate the DPRK's justification for continuing to target the the two countries. CrowdStrike anticipates continued intelligence collection activity and incremental improvements in the technological capabilities of the DPRK in 2016.

CRIMINAL

Targeted Criminal Intrusion

During 2015, cases of targeted intrusion were observed by groups dubbed Carbanak, Butterfly (a.k.a. Wild Newtron), and FIN4. These groups have all used customized malware to target large organizations for high-value financial gain. CrowdStrike assesses it is likely that targeted criminal activity will continue to increase in the coming year. Groups operating globally but often originating out of Lagos, Nigeria used opportunistic targeting in 2015 to gain a foothold in organizations using readily available remote access tools. These groups used this foothold to collect intelligence about lexicon, organizational charts, and business processes to conduct highly targeted social engineering. Similar groups focused research on publicly available information to collect their intelligence. Such activity is likely to continue into 2016, as the potential financial reward is high and the prosecution of such activity is difficult.

Commodity Malware

Markets used to obtain banking Trojans and ransomware will both increase and diversify with more malware family authors attempting to gain increased market share. Criminal actors often obtain malware, exploits, and binders (packers) from underground markets and forums; competition in these forums has been observed and continues to increase. Authors are constantly looking to grow their user base through novel features and increased stealth from anti-virus technology;

this drives the complexity of such malware up, providing criminal elements who intend to use the malware with increased revenue-generating opportunities. It is probable that in 2016, the introduction of new malware families with increased complexity and stealth will continue to expand. Ransomware has been a growth market for criminals in 2015, and this trend shows no sign of abating.

EXTORTION

Extortion actors in 2015 were extremely prevalent; groups such as PIZZO SPIDER, MIMIC SPIDER, and other copycats targeted all manner of businesses. This activity may continue, however due to increased awareness and lack of paying victims, it is unlikely that these groups will see high return on investment and may disband. Due to the high visibility of these attacks, coordinated investigation and disruption is likely by international law enforcement.

Analysis of transactions to Bitcoin addresses observed in various extortion schemes indicates a very low number of paying victims. Businesses that are extorted for Bitcoin often have no idea how to find the necessary funds, and the delivery of ransom notes to email addresses that may not be monitored or to users who have no idea what the note is referring to result in slow response times. During those slow response times, the actors often move on to another target.

HACKTIVISM

Motivation

Regional conflicts will likely remain a primary driver of nationalistic hacktivist activity in 2016. Gulf Cooperation Council (GCC) military involvement in Yemen, for example, has been cited by hacktivist actors operating on both sides of the conflict. These hacktivist campaigns often occur in near-real time to the real-world events that inspire them, and as such they can often be difficult to anticipate.

While some nationalist groups are well established and maintain a public web presence, such as DEADEYE JACKAL, others often materialize—seemingly instantaneously—to carry out a sensational attack in retaliation to a real-world event. Examples of the latter include the previously discussed Yemen Cyber Army and, more recently, the January 2016 compromise of Saudi-owned broadcaster Al Arabiya's website by the Defenders of the Hijaz group. 2016 will almost certainly see a continuation of hacktivist activity mirroring regional conflict events.

In addition to politically motivated actors, hacktivists seeking public recognition will also likely continue to be prominent in 2016. GEKKO JACKAL provides an example trajectory of how such groups can increase in skill level and thus ultimately begin to move toward a financially motivated criminal operation. Copycat groups, such as Phantom Squad, are currently involved primarily in DDoS attacks against gaming-sector targets; however, it should be expected that these attacks, as seen in the case of GEKKO JACKAL, will broaden to include additional verticals. International events such as the 2016 Olympic Games in Brazil will almost certainly attract hacktivist actors seeking to capitalize on the global visibility of the event.

DDoS

2015 saw a notable increase—both in frequency and effects—in DDoS attacks carried out by hacktivist actors. DDoS-based hacktivist activity throughout the year varied in motivation and included more traditional protest-style campaigns as well as those carried out by actors driven solely by a desire for media attention. One common trend identified as being in part responsible for this increase in DDoS activity is the widespread availability of paid network stress testing, or stresser services. CrowdStrike assesses that the increasing adoption of paid stresser services for use in hacktivist operations will likely continue throughout 2016.

These DDoS-for-hire services allow low or unskilled actors to carry out disruptive attacks leveraging amplification TTPs. Such functionality represents a marked improvement over that offered by traditionally popular, freely available DDoS tools such as LOIC, Torshammer, or PyLoris. Additionally, the use of third-party web-based DDoS services reduces the risk of attribution to the attacker, since disruptive traffic is not generated from the attacker's own network as it is with the aforementioned freely available tools.

In addition to their ease of use and relatively low cost, stresser services have proven to be a powerful tool in the hands of low-sophistication hacktivist actors, enabling them to disrupt the operations of victim organizations. Attacks carried out in early 2015 by actor Bitcoin Baron, for example, underscore the disruptive and dangerous capability provided by such services. In March 2015, Bitcoin Baron launched a series of attacks against state and local government agencies in Wisconsin in protest of an alleged incident of police brutality. The ensuing DDoS attack disrupted not only the public websites of the city of Madison and local banks, but also affected internal networks used for emergency communication by the department of public safety. Specifically, police officer mobile data terminals (MDT) as well as payment-processing systems were reportedly impacted.

Additionally, due to the low barrier to entry, relatively low risk of attribution, and ease of use associated with stresser services, hacktivist campaigns leveraging them are increasingly employing little vetting of target lists to ensure victim organizations are in line with the operation's stated aims. This is best evidenced, as previously discussed, in Anonymous-led DDoS attacks opposing ISIS, which often mistakenly target unrelated websites. CrowdStrike assesses that the risk of organizations being affected as collateral damage in hacktivist campaigns will remain prevalent throughout 2016.

> "CROWDSTRIKE ASSESSES IT IS LIKELY THAT TARGETED CRIMINAL ACTIVITY WILL CONTINUE TO INCREASE IN THE COMING YEAR."

This report previously discussed GEKKO JACKAL's development of a botnet-based DDoS-for-hire service using a lightaidra malware variant called bashlite. The source code for GEKKO JACKAL's bashlite implant was publicly leaked in January 2015. CrowdStrike has subsequently observed a proliferation of this malware across multiple hacktivist communities and therefore assesses that its prevalence will likely increase during 2016. Similarly, the presence of bashlite infrastructure in identified attacks will likely no longer be intrinsically indicative of GEKKO JACKAL involvement.

In addition to GEKKO JACKAL, CrowdStrike has observed similar copycat hacktivist activity during 2015. Like GEKKO JACKAL, these groups originate largely from online gaming communities, which is often reflected in their targeting of entertainment sector organizations. A recent example of such activity was the DDoS attacks against Xbox Live, PlayStation, and other gaming networks during the 2015 Christmas holiday by groups including Phantom Squad and OurMine Team. These groups are motivated primarily by public recognition, and their activity will likely remain prominent in 2016.