Accenture Security

2017 CYBER THREATSCAPE REPORT

MIDYEAR CYBERSECURITY RISK REVIEW: FORECAST AND REMEDIATIONS
EXECUTIVE SUMMARY

iDefense

Part of Accenture Security

EXECUTIVE SUMMARY

The 2017 Cyber Threatscape Report examines cyber-threat trends during the first half of 2017 and offers an overview of how those trends might unfold in the latter half of the year. This report should serve as a reference and strategic complement to Accenture Security iDefense's daily intelligence reporting to provide IT security and business operations with actionable and relevant decision support. By informing IT security teams, business operations teams, and organization leadership about emerging trends and threats, the report helps those groups anticipate key cybersecurity developments for the coming year, and provides, where appropriate, solutions to help reduce organizations' risk related to cybersecurity. The report relies on iDefense intelligence collection, research, and analysis as well as research using primary and secondary open-source material.

Four key findings result from the iDefense research during the first half of 2017 in the areas of cyber-espionage, financially motivated cyber-crime, and hacktivism.

DESTRUCTIVE CYBER-THREAT ACTIVITY IS BECOMING MORE COMMON AND ATTRIBUTION IS GETTING HARDER

The WannaCry and Petya malware outbreaks wreaked havoc against worldwide businesses, governments, and non-profit institutions in mid-2017, using Windows exploits leaked to the public by the hacking group SHADOW BROKERS, widely reported as stolen from government entities. These leaks, which exposed numerous zero-day vulnerabilities, created multiple worst-case network defense scenarios. Although governments are trying hard to avoid future leaks, Accenture Security iDefense anticipates that more exploit arsenals will be exposed in the coming years. While software vendors (such as Web browser providers) are attempting to harden their products, eliminate entire classes of vulnerabilities, and reduce windows of opportunity for threat actors, new exploit releases will undoubtedly result in the broad compromise of those organizations, which lack sufficient controls.

WannaCry (linked to North Korea by defense agencies in the United States and United Kingdom) and Petya (with reported links to sources in Russia) are examples of a new strain of high-profile, global-scale, debilitating attacks, that appear to be government-sponsored and aimed at creating chaos and achieving strategic geopolitical goals. Meanwhile, governments struggle to find an acceptable and proportionate response and deterrence actions, as more of what appear to be state-sponsored hackers use tools and techniques traditionally used by financially motivated cyber-criminals, complicating attribution and assessments of motive.

Accenture Security iDefense has also observed increasing cyber-criminal use of deception tactics, including anti-analysis code, steganography, and expendable command-and-control (C2) servers used for concealment. Greater public reporting on cyber-threat activity and attribution may accelerate this denial and deception trend, increasing the complexity, cost of cyber defense efforts and resource allocation.

Phishing campaigns continue to use familiar lures—subject lines mentioning invoices, shipments, resumes, wire transfers, missed payments, and more—but ransomware has displaced banking Trojans as one of the most common malware types delivered via phishing techniques. Increased user awareness and campaign publicity is driving greater sophistication of the spear phishes observed. Users are still a company's greatest weakness and greatest asset for network defense.

Bitcoin continues to be the currency of choice among cyber-criminals; however, with monetization being the end goal of conducting financially motivated cyber-crime, iDefense has observed threat actors are taking additional measures to conceal bitcoin transactions. This manifests itself in cyber-criminals either developing and leveraging bitcoin-laundering techniques or adopting alternative crypto-currencies.

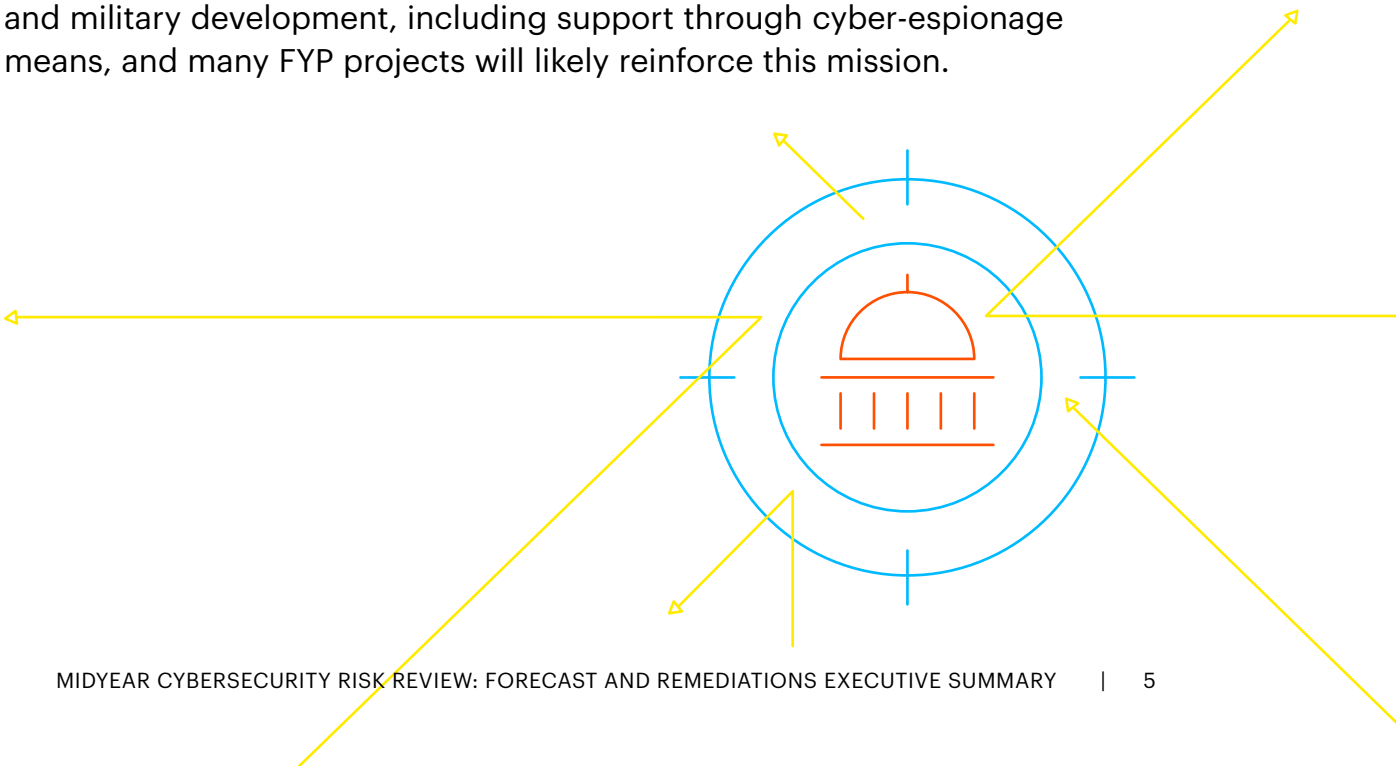
CRIMINAL MARKETPLACES ARE PROFITABLE AND TOOLS ARE MORE ACCESSIBLE TO ALL

An increasingly lucrative criminal marketplace is driving differentiated criminal offerings, emboldening and enabling more actors with better capabilities. The continued evolution of ransomware during 2016 and the first half of 2017 produced variants that were more customizable and richer in features than before. For the remainder of 2017, iDefense expects to see ransomware variants targeting non-Windows platforms, such as Linux and OSX, as well as mobile platforms, such as iOS and Android. Low-end booter and stresser distributed denial of service (DDoS)-for-hire services have given way to a thriving DDoS-for-hire botnet ecosystem primarily employing domain name system (DNS) amplification. The rapid adoption of Internet of Things (IoT) devices has created a rise of IoT botnets, which will continue to grow as more diverse devices join the global network.

GOVERNMENTS
ARE STRENGTHENING CAPABILITIES TO MEET STRATEGIC GOALS

Between October 2016 and June 2017, North Korea is reported to have unleashed several large-scale and noisy operations aimed at exfiltrating foreign intellectual property, stealing money from foreign governments, and probing vulnerabilities within United States and European key critical infrastructure. Iran, meanwhile, has focused cyber-espionage and disruption efforts on critical infrastructure verticals such as: financial, energy, aviation, and government. North Korea and Iran continue to improve their national level cyber-threat capabilities, and iDefense expects to see a growth in cyber-espionage and disruption activity from both countries in the next few months, not only in response to geopolitical triggers, such as economic sanctions and military exercises, but also in continuing service to national strategic goals.

After observing a downturn of activity in China, iDefense expects China's cyber-espionage activities aimed at technology transfer to regain historic levels. China's 13th Five-Year Plan (FYP), which is now underway, may prompt the targeting of companies active in the areas of cyber-security, cloud computing and big data, new energy automobiles, high-performance computing, biomedical materials, repair and replacement of tissues and organs, deep sea key technology and equipment, and smart grid technology and equipment. Historically, Chinese cyber-espionage operations have heavily targeted foreign technologies that overlap with FYP goals. Newly created after a military-wide restructuring, the Strategic Support Force of the People's Liberation Army (PLA) is also tasked with supporting innovation and military development, including support through cyber-espionage means, and many FYP projects will likely reinforce this mission.



Russian hybrid operations and active measures reached a feverish pitch in the first half of 2017 as election seasons swept over Western Europe. These efforts integrate cyber-attacks with psychological operations to exploit media, social media, and influence groups in a bid to exacerbate existing social rifts and solidify pro-Russia policies in targeted countries. Although unsuccessful in bringing victory to Russia's favored candidates in the Netherlands and France, Russia will likely continue its attempts as German and United States legislative elections approach in late 2017 and 2018.

LAW ENFORCEMENT IS BECOMING OVERWHELMED

Due to a wide range of factors, underground cyber-criminal communities are culturally varied. In Brazil, where law enforcement is overburdened and as a result criminal conviction low, knowledge and tools (with a heavy emphasis on carding) are openly disseminated in “clearnet" (non darknet) hacking forums to maximize visibility to the market, whereas direct transactions occur largely in mobile messaging platforms. The increasing entanglement of financially motivated cyber-crime with organized criminal groups has prompted a growth in malware sophistication, although in cases like Brazil’s “off-the-shelf” malware, versions are modified for local environments prior to deployment. Familiarity with local cyber-threat environment is essential to the security of an organization’s full-scope network and operations.

THE FRONT LINE OF DEFENSE

The destructiveness of increasing ransomware and DDoS attacks; the aggressive use of information operations by nation-states; growth in the numbers and diversity of cyber-threat actors; and the greater availability of exploits, tools, encryption, and anonymous payment systems in 2017 pave the way for a rapid growth of cybersecurity challenges across all industry verticals in the coming year. Industry will have to meet these challenges with equally aggressive defense strategies, including user education and the integration of threat intelligence and risk assessment into business operations across the enterprise.

CONTACTS

Rick Hemsley
Managing Director, Accenture Security
rick.hemsley@accenture.com

Uwe Kissmann
Managing Director, Accenture Security
uwe.kissmann@accenture.com

Josh Ray
Managing Director, Accenture Security
joshua.a.ray@accenture.com

Gareth Russell
Managing Director, Accenture Security
gareth.russell@accenture.com

Justin Harvey
Managing Director, Accenture Security
Incident Response & Threat Hunting
justin.harvey@accenture.com

For more detail on the scope and purpose of this review, please see the full version of the report.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.