DOMAINTOOLS®

CYBERSECURITY OUTLOOK 2018

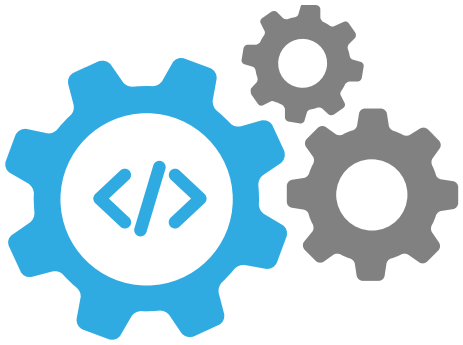
HOW TO STAY AHEAD OF SOPHISTICATED CYBER CRIMINALS IN 2018 AND BEYOND

In 2017, the WannaCry and NotPetya attacks made ransomware a household name, and it seemed no business or consumer data was safe. Beyond those global incidents, countless cyberattacks threatened consumer privacy, worldwide commerce and even infrastructure in some regions. Our research team uncovered fraudsters targeting UK banks such as NatWest, Barclays and HSBC with fake websites. Luxury retail brands including Chanel and Gucci learned of fraudulent websites spoofing their brands, tricking consumers into sharing sensitive personal data or purchasing imitation goods. In April, a successful cyberattack on U.S. critical infrastructure occurred when every outdoor emergency siren in Dallas was set off at the same time, sending some residents into a panic.

Since DomainTools launched Iris, our enterprise domain and DNS investigation platform, we have made it our mission to help our customers shift from a reactive to a proactive security strategy. In recent years, our analysts, researchers and executives have seen the sheer number and sophistication of security concerns facing organizations continue to mature and grow, irrespective of industry, region or company size.

After analyzing the activities of cyber threat actors this year, the DomainTools Research Team has identified four key cybersecurity concerns that security teams, executives, consumers and government officials can expect to encounter next year. From hacked drones with the potential to cause physical harm, to advancing activity from North Korea and Hidden Cobra, this paper connects the dots between the past, present and future to help organizations get ready for the security challenges of 2018.

RISE OF THE MACHINES



Rapid advances in technology are providing significant benefits in helping business automate processes and improve efficiencies. But it is difficult for security practices to keep up, which has proven to result in sometimes-disastrous effects on business continuity. Machine learning, a current hot topic in tech and business, provides one example. This technology enables a computer to learn over time how to conduct specific tasks without being explicitly programmed to do so. While the possibilities and opportunities for streamlining cumbersome business processes are endless, machine learning also reveals a unique opportunity for sophisticated hackers to intervene and influence unmonitored systems.

Similarly, the broad commercialization of drones, a new wave of IoT devices, exposes another vulnerability and threat vector for hackers. **DomainTools research found that 52 percent of security professionals feel the biggest threat in 2018 is the increasing number of connected devices and vulnerabilities surrounding them.** While IoT devices like smart TVs and home systems have been successfully hacked before, a hacked drone is the latest example of an IoT device that introduces a serious threat of bodily harm.

PREDICTIONS FROM THE EXPERTS:

"The example data that is used to teach computers how to make decisions is a very unique and dangerous threat vector. Any company that collects external data to feed into their machine learning systems are vulnerable to malicious actors injecting either noise or specific signals into these data feeds for the purpose of influencing the system's behavior. We saw a simple example of this with Microsoft's Tay chat bot last year, where people interacted with the bot for the specific purpose to turn it into a raging hate machine. This threat vector can be very hard to identify and as more and more companies bring machine learning systems online the danger will increase."

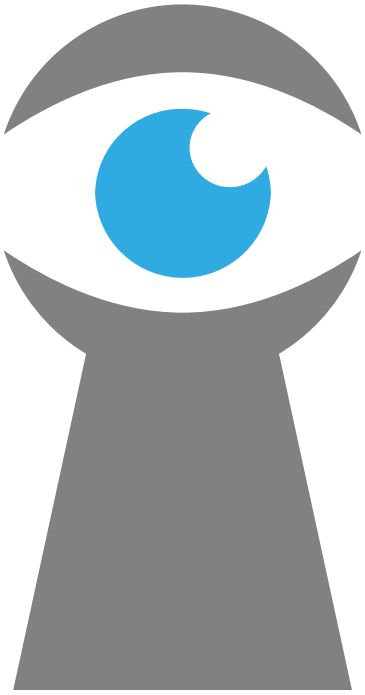
JOHN CONWELL, SENIOR DATA SCIENTIST

"Since 2015 we've seen a huge uptake in the development of commercial uses for drones including: construction surveying, mine surveying, delivery services, agricultural monitoring, and most recently, disaster and insurance assessment, etc. These devices range anywhere from a few pounds, up to 50+ pounds, and are guided either by a connected pilot or via an autonomous system; both of which are susceptible to influence or interruption by external actors. Drone manufacturers are in a race right now to create the "GoPro" of the drone industry, the product that defines the entire market, and in this race security most likely will be an afterthought. Early attacks will probably start out as amateur script kiddies trying to see if they can hack a flying drone, but could evolve into coordinated attacks by professional hackers."

JOHN CONWELL, SENIOR DATA SCIENTIST

THE BATTLE CONTINUES: INTERNET PRIVACY AND ACCESS

The battle between security intelligence sharing and privacy has reached a crisis point on the internet. In 2017, innovations such as the "world's most hack-proof" smartphone have been introduced into the market for privacy-conscious consumers who do not want to share personal data with their telecom service providers. But some worry that these anonymized solutions create new platforms that will make it easier for criminals to wreak havoc undetected. Further complicating the issue, the FBI has put pressure on tech giants like Apple and Facebook to provide them with back-door access into devices and accounts to conduct investigations.



Meanwhile, the net neutrality debate rages on, with some questioning the security and morality of a deregulated multi-tiered internet system, and what it means for businesses and individuals. One thing that can be agreed upon is the ever-present need to strike the right balance between national security and individual privacy.

PREDICTIONS FROM THE EXPERTS:

"In 2018, we'll see the internet become safer for the bad guys and less safe for the rest of us. The rise in anonymizing technologies continues without abatement, privacy interests override security interests. As a result, people will be increasingly discerning about what they choose to do and say and store online."

TIM CHEN, CEO

"Deregulation of internet service providers (ISPs) to allow preferential traffic will create a multi-tiered internet system: those who can afford to use VPNs/proxies to get the traffic they want at the speeds they want, and those who cannot. Deregulated data streams will be modified and augmented by ISPs to insert ads or other content – these augmented streams will be quickly compromised and malware will be sent to customers with no way to block it. Moreover, anti-malware software could be directly blocked by these hacked data streams. For reference, think of how the cheap android phones with built-in apps were hacked to steal data from the device without anyone knowing."

SEAN MCNEE, SENIOR DATA SCIENTIST

RANSOMWARE AND DDoS ON THE MOVE

The rise of cryptocurrencies has paved the way for an exponential rise in ransomware this past year. The perpetrators, who take over an organization's or individual's computer system and hold it ransom until a sum of money is paid, are protected by the anonymity of cryptocurrencies such as Bitcoin and Ethereum. According to a recent DomainTools survey of business and security executives, ransomware is the number one security concern keeping them up at night. The main reason a third of organizations are fearful of these attacks is the fact that hackers are becoming increasingly savvy. Concerns about impacts to brand reputation, financial damage and potential intellectual property loss also top of list of worries.

Another malicious threat to everyday systems, DDoS attacks, are expected to continue to compromise businesses without discrimination in the coming year. While these incidents typically target the systems of larger corporations such as Trump Hotels, our DomainTools Research experts expect growth in "down-markets" as well as an increase in strength and prevalence overall.

PREDICTIONS FROM THE EXPERTS:

"Cryptocurrency was a "killer app" and enabled and fueled the growth of ransomware and related ransom threats in 2017. This will continue to grow in 2018 to include holding identities for ransom. Users will receive emails or phone calls telling them that their SSNs and other information has been compromised (with evidence) and then instructed to pay via bitcoin to prevent the data from being leaked."

MICHAEL KLATT,
VP OF RESEARCH AND DEVELOPMENT

"As the large-scale ransomware attacks this year showed, many organizations are vulnerable. In 2018, there will be an increase in smaller players getting in on this action by attacking smaller institutions. Expect ransomware, DDOS, and phishing campaigns to target not critical infrastructure, but smaller banks, corporations, and universities. These should be easy to block, but volumes will grow dramatically and will over-burden SOCs."

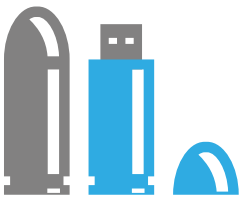
SEAN MCNEE,
SENIOR DATA SCIENTIST

"The strength and prevalence of DDoS attacks will increase in 2018. It's easier, faster, and requires virtually no knowledge to perform a DDoS nowadays, as attackers can leverage off the shelf 'stressors.' Due to the ease of performing such attacks, I would imagine we will see large geographical portions of nation states cut off from important services, like Amazon AWS or the like."

KYLE WILHOIT,
SENIOR SECURITY RESEARCHER

NATIONAL SECURITY & NORTH KOREA

In 2015, it was reported that China was a leading suspect in the hack of the U.S. Office of Personnel Management. Earlier this year, Russia's military admitted for the first time a significant effort to commit cyberwarfare against its perceived enemies. These are just two examples of many that show the growing impact state-sponsored cyber threat actors have on national security.



To get a pulse on the trend of cyberattacks being used by governments, against governments and the private sector, this year **DomainTools polled some of the nation's top cybersecurity experts to see if this was more than just a sensationalized concern. The response was telling – 39 percent of cybersecurity experts believe that cyberwarfare is simply the way wars are conducted these days.**

As we head into 2018, several DomainTools executives have specific ideas for what to expect on this front, paying particular attention to North Korea as political tensions with the U.S. continue to rise.

PREDICTIONS FROM THE EXPERTS:

"Next year, we will see a major disruption to a government agency's online operations. While there have been data breaches, denials of service, and temporary defacement of websites in the past, we predict a more comprehensive attack that cripples an agency's functions for an extended time period. We know that governments are targets and threat actors are relentless."

TIM HELMING, DIRECTOR OF PRODUCT MANAGEMENT

"In 2018, we will see an uptick in nation-state level actors involved in what is traditionally considered 'cybercrime.' Nation states, such as North Korea, which are under heavy sanctions will likely increase their 'cybercriminal' behavior as a method to supplement cash flow, such as ATM hacks, bank compromises, etc."

KYLE WILHOIT, SENIOR SECURITY RESEARCHER

"Tension with North Korea will escalate online, leading to a cybersecurity war. North Korea has defensive advantage because of the tight control of their network, therefore, China and Russia will have to play a large part in this war because of their close relationship to North Korea. We expect North Korea's attack pattern to follow Russia's example: targeted phishing campaigns and related "fake news" social media reports based on ideological boundaries, used to destabilize the internal social fabric of their adversaries and to gain technological advantage."

SEAN MCNEE, SENIOR DATA SCIENTIST

"Attacks into North Korea will rely on exploits buried in mass media (music, movies, etc.) pirated into the country. The real concern here is not the cyberwar with North Korea itself, but how it will act as a testbed for future cyberwars against far more sophisticated adversaries."

SEAN MCNEE, SENIOR DATA SCIENTIST

DOMAINTOOLS THOUGHT LEADERS

These DomainTools thought leaders are in the trenches every day, facing threat actors, ransomware chatbots, data breaches, denial of service attacks, spearphishing, business email compromises and more.

TIM CHEN, CEO
Tim joined as CEO of DomainTools in 2009 and has spent 8 years leading the transformation of the company from an advertising based consumer service to a profitable and growing Enterprise SaaS security firm with nearly 500 global customers.

JOHN CONWELL, SENIOR DATA SCIENTIST
John "Turbo" Conwell is a Senior Data Scientist at DomainTools. He brings 10 years experience in data science and machine learning to bear on cybersecurity. He is currently focusing on building models to identify domains created for malicious intent as soon as they are created.

TIM HELMING, DIRECTOR OF PRODUCT MANAGEMENT
Tim has over 15 years of experience in cybersecurity, from network to cloud to application attacks and defenses. Tim has spoken at security conferences, media events, and technology partner conferences worldwide.

MICHAEL KLATT, VP OF RESEARCH AND DEVELOPMENT
Michael joined DomainTools in 2005 and helped develop the back-end systems powering many of DomainTools' most popular products. He managed Engineering for 4 years before moving to his new role in R&D in 2012, where he focuses on exploring new technical opportunities & solutions. Michael is an expert in DNS and has deep experience with the collection and processing of Big Data.

SEAN MCNEE, SENIOR DATA SCIENTIST
Sean has a Ph.D. in Computer and Information Sciences from the University of Minnesota. His research and business efforts focus on the creation of actionable insights in support of critical decision-making through the use of new technologies and workflows over corporate & Internet networking data.

KYLE WILHOIT, SENIOR SECURITY RESEARCHER
Kyle is an internationally recognized security researcher with more than a decade of experience leading research teams to deliver timely and organized threat intelligence to internal and external customers. In his current role as senior security researcher at DomainTools, Kyle is leading efforts to do primary research on DNS-related exploits, investigate current cyber threats, and explore attack origins and threat actors.

ABOUT DOMAINTOOLS

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

Our goal is to stop security threats to your organization before they happen, using domain/DNS data, predictive analysis, and monitoring of trends on the Internet. We collect Open Source Intelligence (OSINT) data from many sources, along with historical records, in a central database. We index and analyze the data based on various connection algorithms to deliver actionable intelligence, including domain scoring and forensic mapping.

DomainTools has over 10 billion related DNS data points to build a map of 'who's doing what' on the Internet. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work.