Report

McAfee Labs
2016 Threats Predictions

intel Security

McAfee Labs offers a five-year cybersecurity forecast and predicts the leading threats of the coming year.

About McAfee Labs

McAfee Labs is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

McAfee is now part of Intel Security.

www.mcafee.com/us/mcafee-labs.aspx

Follow McAfee Labs

Introduction

Welcome to the McAfee Labs 2016 Threats Predictions report!

This year, we developed two distinct views of the future.

In the *McAfee Labs Threats Report: August 2015*, we looked back on the on the last five years since Intel announced the acquisition of McAfee. We compared what we thought would happen in the cyber threat landscape with what actually happened.

In the first section of this predictions report, we turn around and look forward five years. We interviewed 21 key people who shared unique insights into the expected cyber threat landscape and the security industry's likely response. They were asked to look over the horizon and predict how the types of threat actors will change, how attackers' behaviors and targets will change, and how the industry will respond between now and 2020.

In the second section, we drill down and make specific predictions about expected threat activity in 2016. Predictions for next year run the gamut from ransomware to attacks on automobiles, and from critical infrastructure attacks to the warehousing and sale of stolen data. Among other things, we:

- Discuss a subtle yet equally impactful form of attack—integrity attacks—that will become more prominent in 2016.
- Explain why better security in the enterprise will lead to more attacks on employees as they work from home.
- Describe changes in the way we pay for things, and their implications.
- Outline why wearables, integrated with smartphones, are an attractive attack vector.
- Highlight positive changes in the sharing of threat intelligence within the private sector and between the private sector and governments.

We hope that these two views of the future will provide valuable insight as you develop both near-term plans and long-range strategies.

Happy holidays to you and your loved ones.

—Vincent Weafer, Senior Vice President, McAfee Labs

Contents

Intel Security: A Five-Year Look Ahead 6

McAfee Labs 2016 Threats Predictions 22

- Hardware 23
- Ransomware 24
- Vulnerabilities 25
- Payment systems 27
- Attacks through employee systems 28
- Cloud services 29
- Wearables 30
- Automobiles 31
- Warehouses of stolen data 33
- Integrity 34
- Cyber espionage 35
- Hacktivism 36
- Critical infrastructure 37
- Sharing threat intelligence 38

McAfee Labs 2016 Threats Predictions

These thought leaders collaborated to produce a five-year look ahead at how the cybersecurity marketplace and actors are likely to evolve:

Brad Antoniewicz
Christiaan Beek
Torry Campbell
Gary Davis
Carric Dooley
Steven Grobman
Simon Hunt
Rees Johnson
Brett Kelsey
Tyson Macaulay
Raja Patel
Tom Quillin
Matthew Rosenquist
Raj Samani
Craig Schmugar
Michael Sentonas
Rick Simon
Bruce Snell
Jim Walter
Vincent Weafer
Candace Worley

The 2016 Threats Predictions were researched and written by:

Christiaan Beek
Carlos Castillo
Cedric Cochin
Alex Hinchliffe
Jeannette Jarvis
Haifei Li
Qiang Liu
Debasish Mandal
Matthew Rosenquist
Raj Samani
Ryan Sherstobitoff
Rick Simon
Bruce Snell
Dan Sommer
Bing Sun
Jim Walter
Chong Xu
Stanley Zhu

Intel Security: A Five-Year Look Ahead

Intel Security: A five-year look ahead

Twenty-one thought leaders from Intel Security collaborated to produce this look ahead at how the cybersecurity marketplace and actors are likely to evolve.

Our lineup:

Brad Antoniewicz
Christiaan Beek
Torry Campbell
Gary Davis
Carric Dooley
Steven Grobman
Simon Hunt
Rees Johnson
Brett Kelsey
Tyson Macaulay
Raja Patel
Tom Quillin
Matthew Rosenquist
Raj Samani
Craig Schmugar
Michael Sentonas
Rick Simon
Bruce Snell
Jim Walter
Vincent Weafer
Candace Worley

Computing is becoming increasingly pervasive and enhancing nearly all aspects of personal life and business, creating more and more opportunity for innovation, but also more and more threats. Sight, sound, and touch technologies allow people to experience the world differently and to interact with it and with each other in new and remarkable ways. Everyday objects are becoming smarter and more connected, driving the next wave of computing. Businesses are building deeper real-time connections with their suppliers, partners, governments, and customers, collecting and selectively sharing vast amounts of data. The value of stored and in-transit information is rising rapidly, fueling new markets, creating a need for securely connecting devices, delivering trusted data to the cloud, and deriving value through analytics.

Like anything of value, information is also attracting the attention of adversaries looking for new ways to steal it, leverage it, and benefit from it. Although people often think of organized crime and other criminals, potential adversaries also include hacktivists, nation-states, and others not necessarily seeking direct financial gain. As we look ahead to the personalization and consumerization of cyberattacks, adversaries may also include a competitor, political opponent, spouse, neighbor, or other personal nemesis, as well as the rising activity of chaotic actors who just want to see things burn.

As our computing becomes an extension of the individual, making our environment smarter, contextually aware, and better connected, everything will begin to change. Passwords will finally be replaced by a more sophisticated system of managing and authenticating credentials, and trust will be cultivated into a vital part of our online and electronic activities. Value, transparency, and consent will become important concepts in our digital vocabulary. And personal data will rise in value not only to us, but also to our adversaries.

What we saw then, what we see now

In the *McAfee Labs Threats Report: August 2015*, we looked back to the acquisition of McAfee by Intel in 2010 and examined our expectations at that time compared to what actually happened across the threat landscape during the last five years. Building on that retrospective, 21 thought leaders from Intel Security collaborated to produce this look ahead at what we expect to see in the cybersecurity industry during the next five years. What new security functionality will be added to our hardware to help strengthen security and more effectively counter increasingly sophisticated threats? How will security tools be leveraged to protect privacy and security across your personal network and beyond? Was the perfect storm that we anticipated just the leading edge of something far larger, more innovative, but potentially more destructive? What changes will we see in the cyber threat landscape, due to changes in the technology and economics of information?

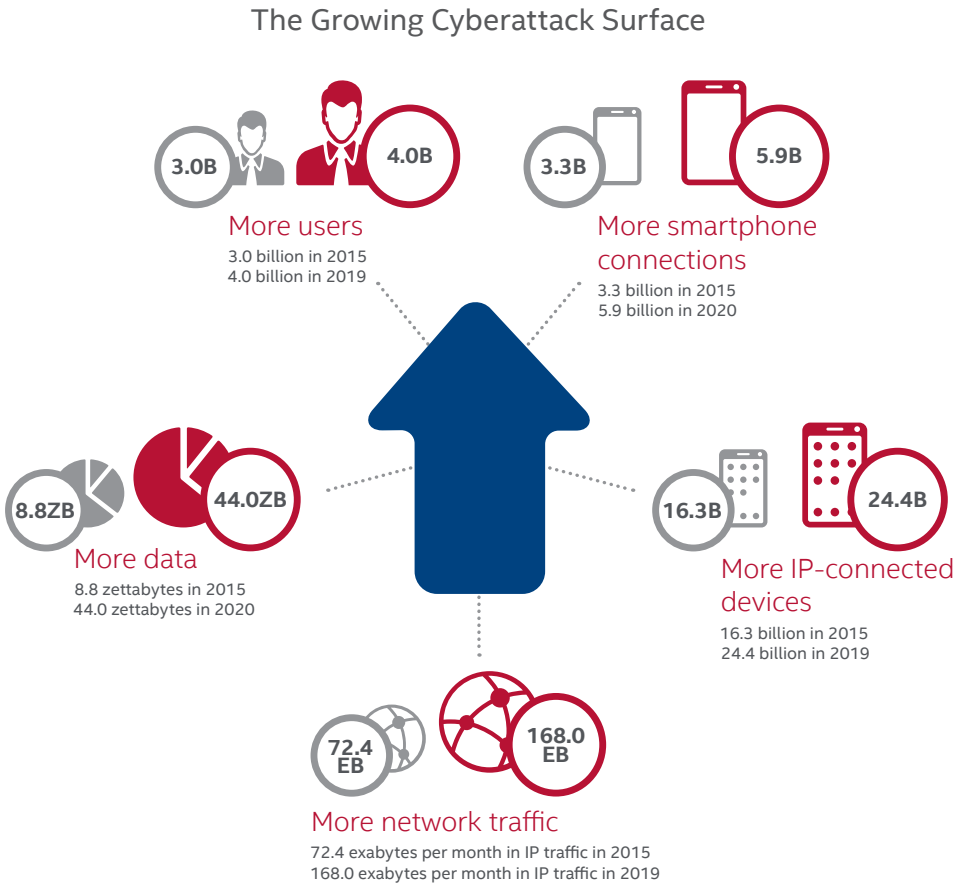
The cyberattack surface

Five years ago, we thought that more users, more data, more devices, and more clouds were creating a perfect security storm of threats and vulnerabilities. Many of those predictions came true, but they were only the leading indicators of a much bigger storm, the acceleration of "more."

On the work side, a dynamic workplace environment, highly mobile workforce, and rapidly changing workers' expectations have blurred the concept of a network perimeter. Workers no longer stay within the confines of a trusted network, or the restrictions of a specific device, making them more productive, but security more difficult. Over time, what we call perimeter inversion or outside-in happens: Applications and devices that were once directed primarily to the corporate network and data center are now directed primarily to the Internet and cloud, with the data center hosting limited processing and storage only for core intellectual property. The release and adoption of Microsoft Office 365 may be the tipping point that reorients the majority of us from PC-centric to cloud-centric storage. Security vendors will have to develop better protections for the growing variety of endpoint devices, the cloud storage and processing environments, and the communication channels that connect them all.

Everywhere we go and in everything we do, we are leaving a trail of "digital exhaust."

On the consumer side, the explosion of devices and the proliferation of exciting "free" services—whether phones, tablets, wearables, smart TVs, or home automation—is fueling an exponential growth in personal data. Everywhere we go and in everything we do, we are leaving a trail of "digital exhaust." At the same time, a strange combination of privacy expectations while intentionally or unknowingly sharing too much will drive the debate over privacy control and regulation. Because privacy considerations vary considerably by country and culture, we do not expect a global consensus on privacy, which will make it challenging for multinational organizations to offer consistent products and services across borders. This combination of trends will also pose compliance challenges for multinational companies whose employees use the same tools to access both personal and corporate resources.



Source: McAfee Labs, 2015.

Devices will continue to grow in volume and variety, and the forecast for connected devices by 2020 is now 200 billion and climbing. Combine this massive increase in the number of devices that need to be secured with a well-documented shortage of security talent, and it is easy to understand why the security industry must simplify and automate defenses and their configurations, and improve efficiency with machine learning and networked collaboration. Even with those improvements, security settings will remain well outside the realm of the average person, fueling the growth in security services that will provide education, guidance, setup, and update assistance to consumers and small businesses. People who install home and small business networks will be required to get much better about providing secure systems to their customers, because no one is going to be the security administrator on these networks.

Security on silicon

As applications and operating systems are hardened further and expand their walled-garden restrictions, attackers will continue to look lower in the stack for vulnerabilities to exploit. We have seen attacks on disk drive firmware and graphics processing units. Recent demonstrations of exploits that leverage BIOS or other firmware vulnerabilities show that the lower you go, the more control you have. Instead of being stuck in a single application or virtual machine, successful firmware attacks can access the entire physical machine without triggering any alarms; all of the virtual machines, all of memory, and all of the drivers can remain persistent even after a reboot or reinstallation.

These attacks will also be effective across a wider range of devices, independent of the operating system. So there is a race to the bottom of the stack, because whoever gets there first has a strategic advantage, whether for defense or attack.

"As new or different criminal actors and nation-states start to exercise their cyber threats, we may see more hardware-based attacks as a means to create chaos or deny service to an organization."

—Steven Grobman, Chief Technology Officer, Intel Security

We currently see only miniscule amounts of malware that target hardware or firmware vulnerabilities, but that is going to change during the next five years. We expect to see many groups leveraging newly discovered techniques, sharing what they know as they try to build effective attacks. Much of this will trickle down, from advanced nation-state intelligence and defense agencies, through big organized crime syndicates, and into broader use.

Hardware and firmware protections such as secure boot, trusted execution environments, tamper protection, cryptographic acceleration, active memory protection, and immutable device identity make it more difficult for these attacks to gain a foothold, as well as easier to detect and correct them.

At the same time, we need to accept that we will never eliminate all risk, that nothing is permanently safe. And even if we could, it would be far too expensive. So we need a mechanism to keep devices, gadgets, and sensors healthy. An essential part of hardware and firmware defenses will be over-the-air updates, or other nonphysical means of updating code. While introducing any type of external connection increases the attack surface, the benefits of being able to quickly update code to address a newly discovered vulnerability outweigh the risks of leaving thousands or millions of devices vulnerable until they can be physically modified.

Linked to remote and automated updating for devices will be identity and access controls for devices that scale up well past conventional identity and access systems into many millions, while also scaling down in size and complexity to support very small, constrained devices.

Intel's famous Moore's Law will accelerate mathematical operations to the point where the cost of hardware-based data encryption will approach zero.

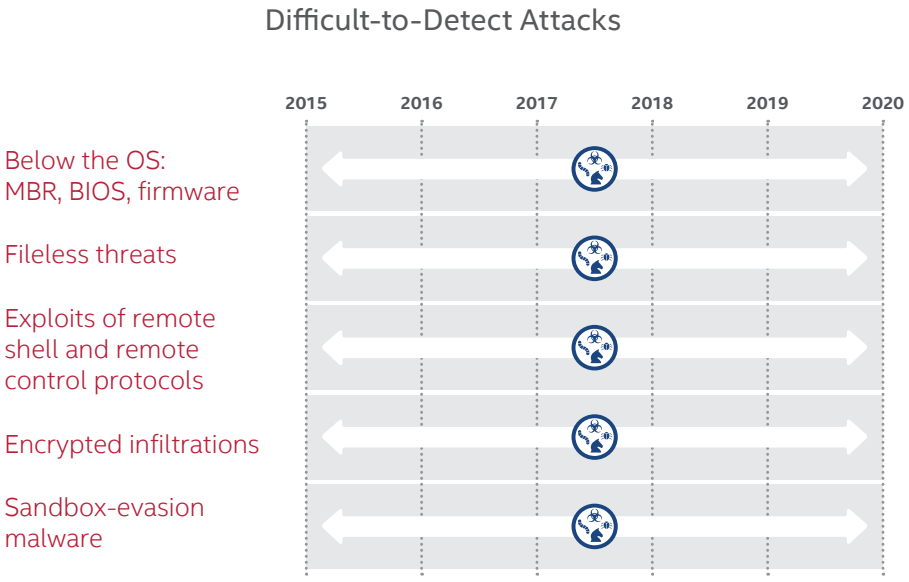
Intel's famous Moore's law will accelerate mathematical operations to the point where the cost of hardware-based data encryption will approach zero, greatly improving our prospects for protecting data at rest, in use, and in motion. Encryption protects data, communications, and code updates from tampering and spoofing. Hardware encryption encourages developers to use it more, by offloading and speeding up the process between five and 20 times, depending on the type of encryption. Because we continue to discover a few vulnerabilities every year in common encryption methods, we need to investigate and embrace stronger or better encryption models, provided they continue to be efficient and transparent to the user.

The growing linkage between hardware and security software will also be seen in the ability to do certain types of TCP/IP packet processing in hardware, allowing for more security processing on smaller processing platforms. The cost per security-computing unit will drop even as security technologies themselves get better.

Difficult-to-detect attacks

The increasing ability of attacks to avoid traditional security systems and remain undetectable was a prediction we got right five years ago, but we have seen only the early stages of this phenomenon. Malware is still very popular and growing, but the past year has marked the beginnings of a significant shift toward new threats that are more difficult to detect, including fileless attacks, exploits of remote shell and remote control protocols, encrypted infiltrations, and credential theft.

As endpoint, perimeter, and gateway security systems got better at inspecting and convicting malicious executables, attackers moved to other file types. Now they are experimenting with infections that do not use a file. Leveraging vulnerabilities in BIOS, drivers, and other firmware, they are evading defenses by injecting commands straight into memory, or manipulating functions in memory to install an infection or exfiltrate data. These attacks are not easy to execute and are not as interchangeable as some of the most popular malware, so the number of known attacks is currently quite small. However, like other techniques, they will get simpler and commoditized over time, broadening their accessibility and fueling their growth. The security industry is developing active memory protection and scanning technology that detects memory not linked to a specific file, but we expect to see an escalation in this type of attack until these defenses are commonly deployed.



Another type of fileless attack that we predict will increase during the next five years is the hijacking of various remote shell or remote control protocols, such as VNC, RDP, WMI, and PowerShell. These give attackers direct control over systems and enable them to install malicious code without tripping endpoint alarms. In other cases, attackers will work to steal user credentials so that they can legitimately use these protocols, which is even harder to catch. In fact, we expect credential acquisition to become a primary target, as credentials are often an easier target than data and frequently provide direct access to a host of valuable resources, from the devices themselves to owners' applications and cloud services. Once an attacker has the credentials, most security defenses will consider further actions legitimate, allowing attackers to move freely within the environment.

Behavioral analysis can detect some attacks like these. Unfortunately, the security industry is playing catch-up in this area and it may take most of the next five years before solid behavioral analysis technologies gain the upper hand. Between now and then, two-factor authentication and biometrics will grow to supplant passwords, and other technologies will be the essential determinants of legitimacy.

We will also see attacks with more patience, "sleepers" that are willing to wait months before activating to evade sandbox environments, or infections that quietly gather data without interfering at all with the user. Or infiltrations hidden in commonly encrypted protocols, such as HTTPS. Another sneaky technique we will continue to see borrows from the stage magician's playbook of misdirection: a visible and active malware or botnet attack that draws the attention and resources of the security team while the real attack slips in quietly somewhere else and moves around unobserved and unconstrained.

Virtualization

Virtualization, like any technology, provides security benefits and weaknesses. Although it isolates and protects virtual servers and applications, it can also make lateral movement harder to detect. Before virtualization, we could potentially catch lateral movement through anomalous network traffic. Now, that traffic is wholly contained within the physical machine in software-based switching and routing. The top-down view of the whole machine that we once relied on is complicated by all of the virtual machines and barriers between operating system functions. There is also the question of who is responsible for security at the various layers when hardware and basic functions are provided by one company or administrative function, cloud and virtualization services by another, and application services by a third. And how do you accurately track and attribute an attack, with all of the obfuscation possible with clouds and virtualization?

Virtualization, in its many forms, presents significant technical and operational security challenges.

Something else is happening to virtualization: It is moving from the data center into the network. This is a rapidly evolving technology called network function virtualization (NFV) and it will take telecom networks by storm during the next five years.

Although virtualized networking has existed in data center clouds for several years, it is new inside the networks that join users and endpoint devices to clouds—such as the Internet. NFV uses standard computing platforms for specialized network tasks that used to demand specialized appliances: routers, switches, telecom-specific IT, firewalls, IPS, DNS, DHCP, etc.

NFV is another big question mark when it comes to security for a variety of reasons. NFV makes networking vastly more flexible and efficient, but also more complex. NFV is most frequently based on open-source technologies, whose flaws are generally disclosed without ado—there are no vendor-specific grace periods between discovery and disclosure. NFV creates efficiencies by allowing multiple network elements to be virtualized onto a single platform—creating a single point of failure in the event of a successful attack or other failure.

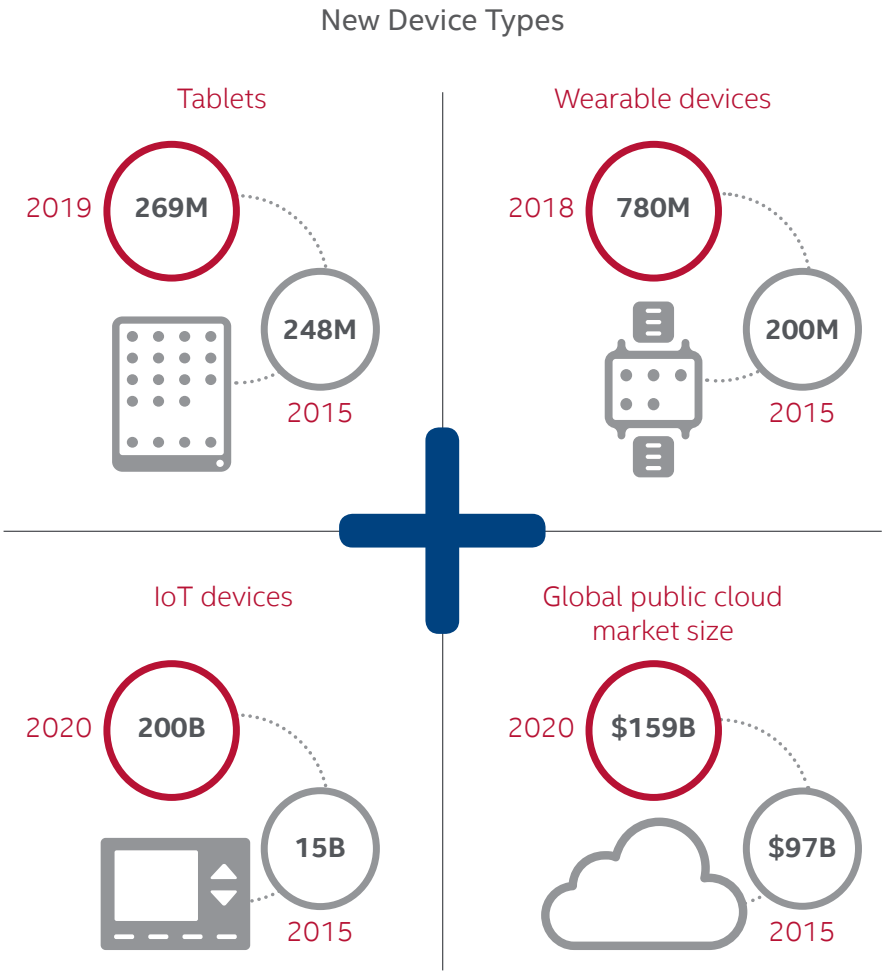
Further, we have “containers” and “containerization”—a new form of virtualization that looks like it will become the new, better, faster, lighter virtual machines. Containers replace “images” in the data center and cloud, by essentially sharing not only hardware resources (as a hypervisor allows) but also operating system resources such as libraries. Containerization is a technology already widely employed by leading cloud service providers; it will come to a data center near you in the next five years. Like NFV, containers can create new forms of complexity and risk. They are mostly based on open-source software, and create new attack surfaces through the sharing of more resources across all containers.

Finally, in the next five years software-defined network (SDN) will go mainstream in networking, not just data center and cloud environments. SDN will be used in combination with NFV to create amazing new forms of value-added services available on demand, in highly scalable forms, and fully automated. Yet like NFV, SDN comes with a security price: yet more complexity, open-source software, expanded attack surfaces, and single points of failure.

New device types

Our earlier predictions on the growth in volume and types of devices was wrong only by being too conservative, and what we have experienced in the last five years is just a small part of what the next five will bring. The ease and cost of developing connected things is dropping fast, leading to an explosion of new products, business models, and usage models. Prototypes are quickly becoming products, and early-adopted gadgets are maturing and rapidly growing their installed bases in consumer, industrial, and business applications. Some of these leading-edge Internet of Things (IoT) devices have enough installed base to warrant attacks, with many others following closely behind.

The majority of these companies and their gadgets are driven by time to market, usability, and thin cost structures, meaning they have limited time and resources to invest in IoT device security. Not only do these devices often expose themselves to attackers but they also expose the systems they connect, and the personal information they manage, to those same attackers. Further, many of these devices will be designed to remain in operation for many years, exposing themselves and the systems they connect with to threats that would otherwise be eliminated by upgrades or short refresh cycles.



Source: McAfee Labs, 2015.

In the home, smartphones or tablets have become the nexus of this IoT ecosystem. Phones or tablets are the collection points for most wearables. They are used to configure and control smart TVs; operate lights, locks, and appliances; link to the car; and coordinate many digital health tools, all connected to a cloud backend. This nexus is an excellent intelligence-gathering point for the bad guys. We know that phones have vulnerabilities that have not been targeted because attackers do not yet have the right financial motivation. With the increasing use of smartphones and tablets as collection points, we expect them to be aggressively targeted during the next five years for the data they store or the data that passes through them.

Similarly, as companies compete to own the connected home, we expect to see home hubs and their cloud services targeted by patient and low-profile intelligence-gathering malware. Many of these devices are always on, always listening, and always communicating, raising concerns about transparency and privacy. With homeowners unprepared and ill-equipped to detect and remediate most security threats, some highly successful attacks will collect

personal info on an ongoing basis, enable denial-of-service actions, and turn Internet-connected home devices into zombies. During the next five years, connected home networks could become the simplest way to hack into people's lives or into their employer's resources. Because of that, there will be a high demand for installation technicians with cybersecurity skills, a need for more effective default home network configurations, and new security services from broadband and application providers to complement those connected home devices.

Smarter, security-capable home gateways will also break onto the scene in the next five years. Today, home gateways are mostly dumb. They pass packets to and from the Internet with limited to no oversight, and they pass packets (switching) around the home without policy or oversight. Gateways will need to improve to support the IoT, with its cyber-physical interconnections and safety-critical applications. One compromised device (or user) in the home cannot be allowed to attack another IoT device in the home without some form of detection or, better yet, protection. Home gateways will become the last line of defense, but also enable many new and valuable safety-critical services in the face of consumer fears and regulatory doubts.

The new range of devices implies more than just a shift to phones and tablets. It also heralds a change to a world in which on-the-move users can employ any device with a keyboard and monitor to access information in the cloud. The attacker's target has always been the data, and now the access devices are less controlled and potentially less protected gateways to a lot more data. If we keep our stuff in the cloud and access it from a phone, tablet, kiosk, automobile, or watch (all of which run different operating systems and different applications), we have substantially broadened the attack surface. Because these access devices will inevitably be less secure, cloud vendors will be compelled to significantly improve security on the connections and on the data itself. We think successful cloud providers will respond to this challenge during the next five years, enabled by technologies from leading security vendors.

In parallel, new types of business devices and sensors now feed into industrial systems, critical infrastructure control systems, and core business processes, creating new attack surfaces. In addition to direct threats, we have seen how these new device types make it possible to cross over from industrial to business systems, a trend that will only compound as more and more are interconnected. Some of these devices will stand at critical points in trusted networks, making them attractive beachheads for additional attacks if they can be compromised. We must also be careful not to make this into a numbers game. Although a successful attack on industrial IoT devices with an installed base of hundreds of millions would likely cause havoc, one device at a key point in a critical infrastructure control system could be far more devastating.

Cyber threat evolution

As long as there are digital valuables there will be criminals, so cybercrime will continue to thrive during the next five years. Like any business, most cybercriminal operations follow the money, looking for the easiest way to steal something of value. The growing value of personal data will play a big part, as it is already more valuable than payment card information and will continue to climb. Increased use of cryptocurrencies such as Bitcoin will make virtual currency an attractive target for theft, not just the preferred payment method of criminals.

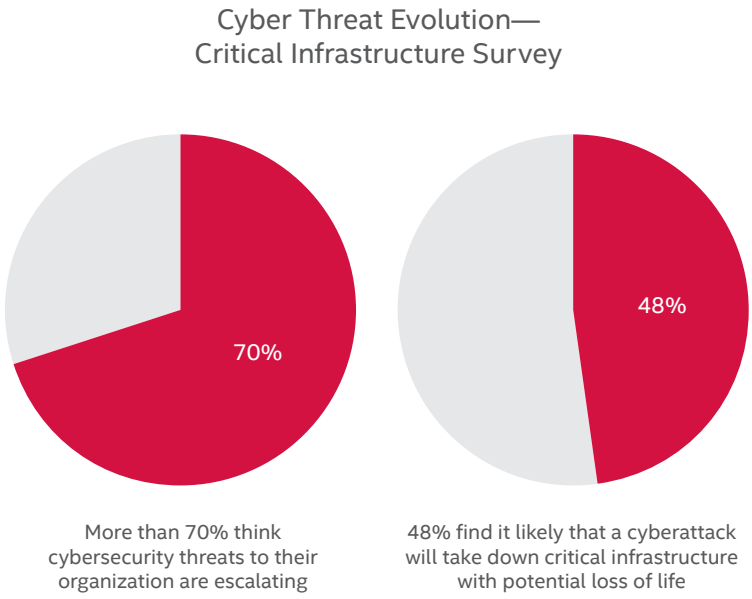
The offering of cyberattacks as packaged goods will continue to expand accessibility to less-skilled people, enabling or boosting more personal attack objectives, such as embarrassment, integrity, harassment, vandalism, or just pure chaos.

The growth in cloud computing will create new vulnerabilities and threats. Traditional network and system infrastructures offered the potential to define clearly a perimeter to secure, whereas clouds and their breadth of organizational boundaries and distributed control points make that task more difficult. Attackers will increasingly target the cloud to take advantage of these frequently ill-defined boundaries. They will also target the public cloud because it offers a chance that they can move laterally and breach other virtual networks in the same public cloud.

Cloud computing will also provide tremendous resources to criminals in the form of computing and storage capacity, plus the ability to appear and disappear at the click of a mouse. Law enforcement organizations will find it challenging to shut down an entire cloud service provider for the behavior of its criminal clients, so it will be necessary to go after other criminal resources, such as their Bitcoin wallets, to put them out of business.

We noted the evolution toward more nation-state attacks in our five-year retrospective. Nation-states will continue to strengthen their defensive and offensive cyber skills. They will improve their intelligence-gathering capabilities, they will grow their ability to surreptitiously manipulate markets, and they will continue to expand the definition of and rules of engagement for cyberwarfare.

Nation-state cyberwarfare will become an equalizer, shifting the balance of power in many international relationships just as nuclear weapons did starting in the 1950s. Small countries will be able to build or buy a good cyber team to take on a larger country. In fact, cyberwarfare skills have already become part of the international political toolkit, with both offensive and defensive capabilities.



Source: http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf

Offensive cyberwarfare may also target not only databases and digital infrastructure but also weapons and physical infrastructure. Nation-state attackers could attempt to turn off the power or water instead of the Internet, or take control of drones, weapons, and targeting systems. Digital espionage is also part of cyberwarfare: Digital intelligence agents co-opt surveillance systems, track government employees, and exfiltrate documents for strategic advantage. We have already seen that with the far-reaching U.S. Office of Personnel Management breach and will likely see more of this behavior during the next five years.

IoT security standards

We discussed emerging IoT devices in the preceding section on new device types. We did not, however, discuss expected new IoT standards—in particular, IoT standards related to security. The establishment of sound IoT security standards is vitally important because so many IoT devices collect very personal or business-critical data. In the wrong hands, that data could destroy a business or be personally fatal.

When it comes to standards of any sort, the IoT is a kaleidoscope. There are literally hundreds of standards that potentially touch IoT and precious few that directly accommodate IoT. Standards on networking security (from many bodies), data center security (from many bodies), identity management, interoperability, wireless standards, privacy standards, and more affect IoT.

Yet even in this swirl of overlapping and competing standards, there are gaps—especially related to security standards. For example, how to securely design and manage an NFV- or SDN-based network is not addressed by the major bodies such as ISO, EIC, or ITU. Similarly, the new and differing requirements for identity and access control related to IoT, or the clear application of privacy standards to IoT big data, need much more work.

The good news is that efforts are under way that should yield significantly better guidance, at the international standards level, related to IoT security. These efforts will further enable these markets and provide reassurance in the face of the certain high-profile tragedies that will be related to "the early days" of IoT.

Personal data, security, and privacy

Personal data, its value, and privacy demands will dramatically change security and cybercrime, from targets to attacks to defenses. Within the next five years, the volume and types of personal information gathered and stored will grow from a person's name, address, phone number, email address, and some purchasing history to include frequently visited locations, "normal" behaviors, what we eat, watch, and listen to, our weight, blood pressure, prescriptions, sleeping habits, daily schedule, and exercise routine. Sensors will feed information to all sorts of organizations, returning ads, recommendations, and offers with real value. This combined information represents the digital exhaust that will become a mainstay and unavoidable by-product of modern life.

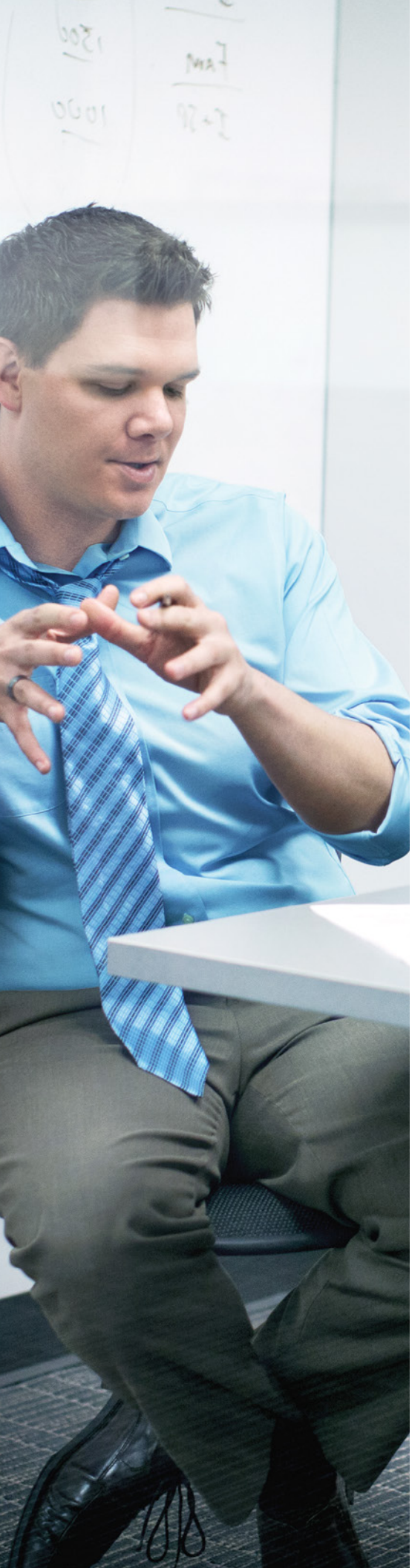
The growing value of personal data will attract cyber thieves and lead to sophisticated markets for stolen data. It will also lead to more security and privacy legislation.

Digital exhaust that we knowingly or unknowingly give away today will have huge economic value in the future, enabling us to sell and trade it for cash, discounts, products, or services that are increasingly personalized and customized. Because that information will have greater value, we will want to protect and control it. Some will continue taking our data "legitimately," by burying the terms in a service agreement for an otherwise innocuous app or service. Others will try to lift it from the cloud, through our devices, or as it crosses the many networks we traverse every day. Others, of course, will want to steal it.

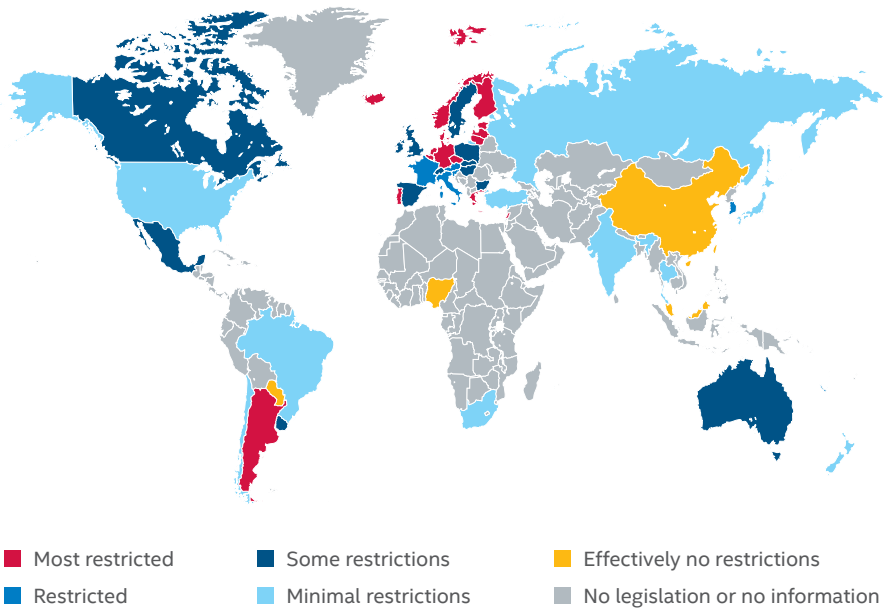
The growing value of personal data is creating a new type of criminal, one that combines, warehouses, and sells stolen information for specific purposes. Leveraging analytic techniques used in the world of big data, these criminals will look for links and correlations throughout their trove of stolen information, reverse engineering personal identities and selling that intelligence to the highest bidder.

This technique will enable thieves to circumvent commonly used techniques to verify identity—social security numbers, birthdates, last four digits of credit cards, or answers to typical security questions—and essentially sell legitimate credentials and make it more difficult for security defenses to identify suspicious behavior. Cybercriminals may even be able to use behavioral analytics to figure out what purchases can be made with stolen payment card info that will not trigger an alert.

Digital privacy and security guidelines and regulations are not new. There have long been discussions and activities in many industries and countries about what is acceptable, appropriate compliance requirements, and penalties for malfeasance. As more and more personal data is captured and stored, attempts to codify policies and penalties will continue. Consumers will demand not only more privacy, but also better ways of giving consent to be tracked, more transparency about what is kept, and the right to view, edit, and even delete their information. Businesses will move pre-emptively toward self-regulation, possibly delivering products with default configurations geared more to consumer privacy than information gathering: moving to opt-in instead of opt-out models of data collection. This will be a fine line to navigate, and industries that do not adapt enough will find themselves in the legislative crosshairs.



2014 Data Privacy Heat Map



Sources: US Department of Commerce and country-specific legislation; Forrester Research, Inc.

Over-regulation is also a danger, full of unintended consequences, potentially hampering innovation, and posing a significant threat to industries. It took more than a century for the regulation of cars and phones to evolve. During the next five years, we will see the impact, if any, of the U.S. Federal Communications Commission's recently issued net neutrality rule, which imposes regulations on the Internet. Expect to see bold forays and failures related to IoT regulation, starting in the next five years.

There will be significant pressure to share personal data with governments, forcing multinational companies to struggle with conflicting regulations and legal liabilities when sharing data across national boundaries. As we already see today, organizations may demand protection from liabilities, or decline to cooperate with disclosure regulations in certain countries that are contrary to their values or the regulations of their headquarters location, setting up interesting conflicts.

The security industry fights back

Behavioral analytics will improve the ability to detect advanced attacks.

Behavioral analytics is the next big weapon in the security defense toolkit. Building baselines for normal behavior and continuously monitoring activity, these tools will learn the regular movements and activities of legitimate people and send alerts or take action when it detects something irregular. Is this application typically used during the course of a person's work? Is this activity being performed during normal working hours, in typical locations, and using verified devices? Behavioral analytics technologies are still in the early stages and it remains challenging to extract meaningful information from massive data sets, but they will mature quickly during the next five years as skills in machine learning, big data, and analytics address the problem.

Better collaboration and shared threat intelligence will lead to faster identification of attackers' tactics and techniques.

In an effort to deliver faster and better protection, there will be pressure on businesses, governments, and security vendors to share threat intelligence. We already see the early stages of this today, as some ecosystem participants conclude that the benefits of sharing outweigh the disadvantages. These threat exchanges will likely grow up and down the supply chain and across industries, as organizations decide whom they can trust and how they can use threat intelligence in their own businesses. Threat intelligence products and services will continue to proliferate, but security vendors will struggle with the conflicts between the marketing and revenue value of intelligence subscriptions services versus the clear need for shared intelligence and better collaboration. Government agencies will also struggle with jurisdictional cooperation and conflicts and with companies concerned about the liability of sharing threat intelligence with law enforcement.

The volume of threat intelligence generated will require progress in machine learning and analytics to efficiently translate it to appropriate actions and human notifications in a timely manner. Threat exchanges will need scoring systems for trust and quality, audit capabilities, and sophisticated methods for quick corroboration and attestation to reduce false positives and prevent gaming the system.

Boosting security efficiency and effectiveness will also be a key imperative during the next five years. The number of devices to protect will exceed 200 billion by 2020. At the same time the number and required skill level of security professionals is increasing while the availability of those people and skills is way below market demand. Out of necessity, this will lead to deeper and richer automation of security functions.

Businesses will also demand predictable levels of security investment and risk management, prompting the continued development of security as a service, security insurance products, and hedging plans against catastrophic security events. Threat intelligence will play its part in this, providing the data needed to build actuarial models for the insurance industry. These may come from interesting partnerships among the insurance industry and security vendors, cloud providers, or threat intelligence consortiums.

Security industry to-do list

- Behavioral analytics: to detect irregular activities.
- Shared threat intelligence: to deliver faster and better protection.
- Cloud-integrated security: to improve visibility and control.
- Automated detection and correction: to protect more devices with fewer security professionals.

Conclusion

Five years ago, we felt that three forces were responsible for the challenges facing cybersecurity: the expanding attack surface, the industrialization of hacking, and the complexity and fragmentation of the IT security market. Looking ahead, we think the main forces will be the continuing expansion of the attack surface, increased attacker sophistication, the rising cost of breaches, the lack of integrated security technologies, and a shortage of skilled security talent to fight back.

Wearables, gadgets, sensors, and other things on the Internet are creating new connections and exposing new vulnerabilities. Every new product that connects to the Internet faces the full force of today's threats, and we have a long way to go to keep up with the speed and complexity of attacks. Building security into the hardware and software layers is essential for new products to succeed at convincing users to trust them. On the positive side, new security tools are coming to market and business awareness about the importance of good cybersecurity has become more common in companies of all sizes.

The personal data economy is going to be a boon for consumers as they capture more and more value from their activities and information. We face tremendous threats to personal privacy as this data and the value it represents attracts thieves. We also face threats to innovation and civil liberties as this data attracts regulatory activity. Organizations of all types will lobby for their point of view, and for limited liability in the face of a breach. Security operations will shift further from a capital expenditures model to an ongoing and predictable model of outsourcing and operating expenditures, coupled with insurance and risk management.

Finally, the cyberwarfare capabilities of nation-states will continue to grow in scope and sophistication. Cold and hot offensive cyberattacks will affect political relationships and power structures around the world, and their tools will trickle down to organized crime and other groups with malicious, economic, or chaotic motivations.

There are hopeful signs: The security industry and many government agencies are finding it easier to collaborate with each other, improving our success rate in catching and stopping cyberthreats. Vulnerability and security research continues to grow, identifying exploits sooner. Large technology companies, including Intel, have built highly skilled security research and development teams that will continue to enhance the effectiveness of tools to detect, protect, and correct attacks.

McAfee Labs 2016 Threats Predictions

- Hardware
- Ransomware
- Vulnerabilities
- Payment systems
- Attacks through employee systems
- Cloud services
- Wearables
- Automobiles
- Warehouses of stolen data
- Integrity
- Cyber espionage
- Hacktivism
- Critical infrastructure
- Sharing threat intelligence

Hardware

For the purposes of this prediction, "hardware" includes firmware, BIOS, and UEFI (below the operating system) attacks that affect or directly exploit system hardware components.

In 2015 we saw a sea change within the domain of hardware and hardware-centric attacks. Many new academic and proof-of-concept reports concerning hardware attacks were published, and the security industry and organizations discovered multiple, in-the-wild hardware-based attacks.

In the case of the Equation Group attacks uncovered earlier this year, the malware artifacts involved were actually several years old at the time of discovery. This is yet another example of threat researchers discovering ultra-low-level and highly sophisticated malware that is (at the same time) "old" by the standards of malware authors and attackers. We have previously seen the use of old malware in threats such as Flame, Duqu, and others in that class.

Specifically, the Equation Group's malware was capable of reprogramming hard disk and solid state drive firmware and remaining persistent despite efforts at higher levels (operating system reinstalls, drive reformats) to remove it. This attack is a stunning example of leveraging intimate knowledge of firmware and reference code from specific manufacturers and using those details to aggressively maintain the malware's persistence. Not only will this trend continue in 2016, but it is also highly likely that threat researchers will continue to uncover ongoing attacks of this nature as we continually peel back layers of current threats.

UEFI (Unified Extensible Firmware Interface) is a standards-based firmware interface for PCs, designed to replace BIOS. This standard was created by more than 140 technology companies who are part of the UEFI Forum.

Hardware attacks are amplified by the emergence of commercial attack tools. In 2015, we discovered the first commercial UEFI rootkit, including source code. The rootkit's authors, Hacking Team, offer a platform called Remote Control System, which includes this rootkit module. Portions of the tool have already been adjusted for attacks observed in the wild. Providing source code has made it very easy for attackers to customize and retrofit the threat for their purposes. Copycat code and similar tools will likely follow in 2016.

We can also see similar examples (and research) via efforts like the NSA Playset. Again, these tools are not new, but attackers can and will continue to adapt the tools for their nefarious purposes. Being able to persist below the operating system, where most typical security controls have their strongest effects, is very attractive to threat actors of all skill levels, whether they are common cyber thieves or nation-states.

System firmware-based attacks pose a critical risk when coupled with the cloud or with cloud service providers. In 2015, the Intel ATR team demonstrated how to gain access to adjacent virtual machines through multiple vectors, including firmware rootkits or simple misconfigurations. Threats similar to the S3 Boot Script attack can be adapted for in-the-wild attacks. In many cases, it is just a matter of exploiting simple misconfigurations in UEFI or BIOS.

Going forward, we must be hyperaware of the system components below the operation system and how those components can be exploited or leveraged for attack. Available controls for under the operating system attacks include tools like CHIPSEC, and technologies like Intel's Kernel Guard Technology (iKGT) and Intel BIOS Guard.

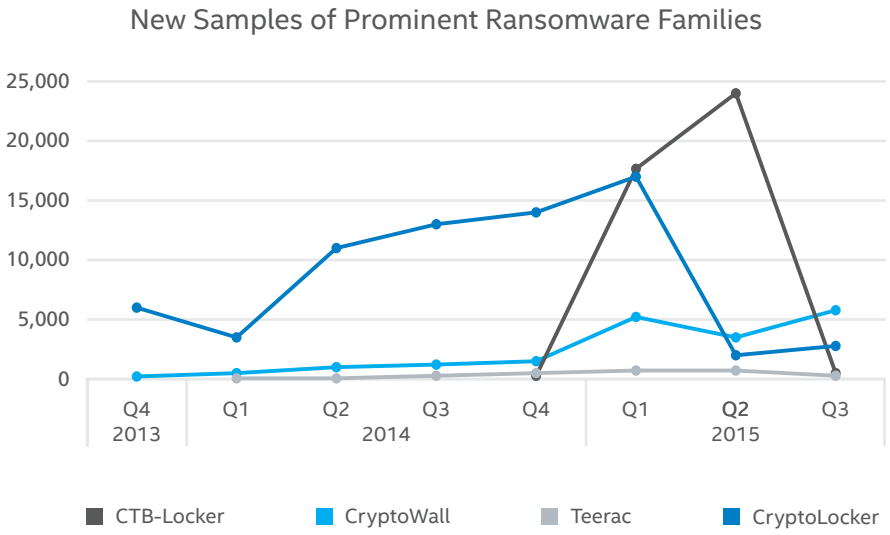
—Jim Walter

Ransomware

Ransomware will remain a major and rapidly growing threat in 2016. With upcoming new variants and the success of the "ransomware-as-a-service" business model, we predict that the rise of ransomware that started in the third quarter of 2014 will continue in 2016.

In 2015 we saw ransomware-as-a-service hosted on the Tor network and using virtual currencies for payments. We expect to see more of this in 2016, as inexperienced cybercriminals will gain access to this service while staying relatively anonymous.

Although a few families—including CryptoWall 3, CTB-Locker, and CryptoLocker—dominate the current ransomware landscape, we predict that new variants of these families and new families will surface with new stealth functionalities. For example, new variants may start to silently encrypt data. These encrypted files will be backed up and eventually the attacker will pull the key, resulting in encrypted files both on the system and in the backup. Other new variants might use kernel components to hook the file system and encrypt files on the fly, as the user accesses them.



Source: McAfee Labs, 2015.

The groups behind most current ransomware campaigns are going for "fast cash," by using spam campaigns and exploit kits such as Angler, and targeting wealthy countries in which people can afford to pay the ransom. While we expect this to continue in 2016, we also foresee a new focus on industry sectors including financials and local government, which will quickly pay ransoms to restore their critical operations. In fact, we have already have seen criminals be quite effective in attacking these sectors. Usually only Microsoft Office, Adobe PDF, and graphics files are targeted; in 2016 we predict that other file extensions typically found in business environments will also become targets. Attacks will continue on Microsoft Windows. We also expect ransomware to start targeting Mac OSX in 2016 due to its growing popularity.

In our 2015 report we made predictions around ransomware targeting cloud and mobile devices, yet we have seen few attempts in those areas. Although people store personal files on mobile phones, it's pretty easy to restore encrypted or damaged files from the application provider's cloud service or from a local backup.

—*Christiaan Beek*

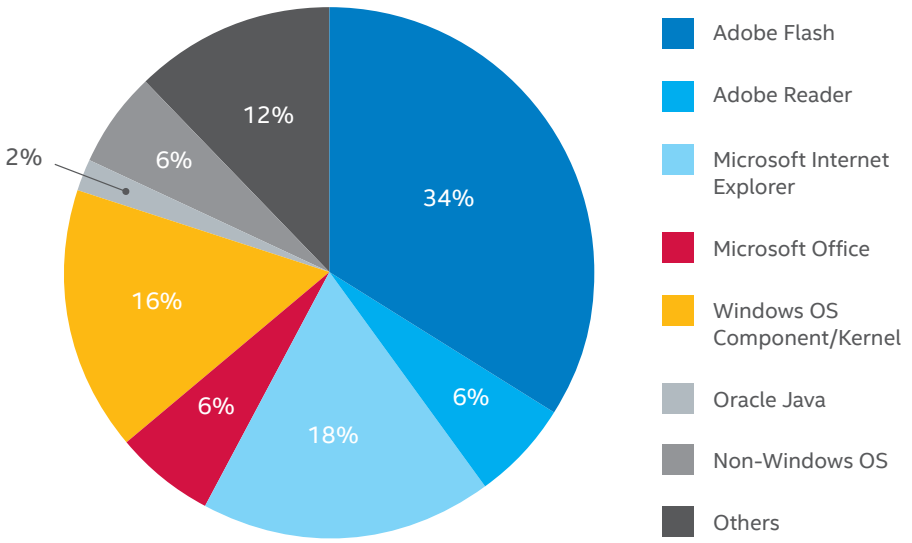
Vulnerabilities

Application vulnerabilities are an ongoing problem for software developers and their customers. Adobe Flash is perhaps the most frequently attacked product: Flash vulnerabilities, including CVE-2015-0311 and CVE-2015-0313, accounted for almost one-third of all zero-day attacks discovered by security companies in 2014 and 2015. In spite of Flash's notoriety, Adobe rapidly fixes its flaws. Further, we predict the popularity of this attack vector (especially attacks instigated by exploit kits) will cool down in the next year due to new mitigation features introduced in a recent Flash Player patch.

These mitigation features nullify the popular "vector spray" exploitation method, increasing Flash's security and raising the bar to exploitation. But no prevention or mitigation is perfect. Because the code quality and complexity of Flash has not changed, there will still be many Flash vulnerabilities. We expect to see some working proofs of concept of mitigation bypasses disclosed in the next year.

Some developers have called for HTML5 to replace Flash, and Google Chrome will soon handicap Flash. But any transition away from Flash will be slow. The Internet is full of legacy Flash content, at least for desktops (though not for mobile devices). We don't expect to see this change soon.

2014–2015 Zero-Day Attacks by Vulnerable Application



Source: McAfee Labs, 2015.

Vulnerabilities in Internet Explorer are less common today than a few years ago, though we can still occasionally see in-the-wild exploits such as CVE-2015-2425 and CVE-2014-1815. This decline is mostly due to recent mitigations that increase the cost of exploitation, and we don't expect to see a big change in 2016. On the other hand, although Microsoft keeps adding new defenses (enhanced protected mode, virtual table guard, control flow guard, isolated heap, memory protection, etc.) to IE, attackers often find ways to get around them. Tricks for bypassing these features are constantly leaked. Consequently, it's just a matter of time before we will see advanced zero-day attacks bypassing IE's latest protections.

What about Microsoft's new browser, Edge, shipping with Windows 10? With its expanded attack surface (because of support for new web standards) and new and enhanced mitigations (such as Memory Garbage Collector), we predict some interesting competition in this new battlefield. Will Edge be as vulnerable as IE was? We expect vulnerabilities will still be found in Edge, but they will become more difficult to exploit.

Java, PDF, and Office exploits have declined significantly in recent years. We have seen only one Java zero day (CVE-2015-2590) in the wild during the past two years. We primarily attribute this paucity to security enhancements in the latest versions of the Java Runtime Environment.

The number of critical Office-based zero-day attacks over the past few years is not high; however, this kind of attack is very dangerous in enterprise computing environments. At Black Hat USA 2015, we presented our research on the security of Object Linking and Embedding (OLE)—an important feature used by Office documents. We disclosed that OLE has a very big attack surface, and we expect attackers to continue targeting OLE. Current detection and protection methods for Office-based vulnerabilities attacks are still not effective enough (for example, encrypted Office documents can be used to evade detection). As a result, we predict we'll see more Office-based attacks in the next year.

We especially expect to see exploits of newly discovered vulnerabilities in areas beyond Windows. Increasingly, embedded systems, the Internet of Things, and infrastructure software will become the targets for advanced threats and zero-day attacks. These include variants of Unix, popular smartphone platforms, IoT specific systems (such as Tizen and Project Brillo), and underlying foundation components and libraries (Glibc, OpenSSL, etc.). In particular, widely used foundation libraries and components, especially open-source framework tools, are not as secure as they should be. Looking at critical zero-day attacks over the past two years, we see that many of them are related to vulnerabilities in open-source software such as CVE-2015-0235 (GHOST) and OpenSSL issues (CVE-2015-1793, CVE-2014-3566, and CVE-2014-0160). We predict these non-Windows targets will be very active in 2016.

—Bing Sun and Haifei Li

Payment systems

Shopping used to be so simple. To buy something, all you needed was enough cash in your pocket. Today, however, the number of alternate payment methods is rather dizzying, from Bitcoins, ApplePay, credit cards, and debit cards, to online payment services. In the 2013 report *Digital Laundry: An analysis of online currencies, and their uses in cybercrime*, we discussed the main electronic and virtual money platforms available at the time. According to Wikipedia, there are now more than 740 cryptocurrencies! Wikipedia also tallies more than 60 online payment services.

We place a significant security focus on vulnerabilities associated with credit and debit card transactions. That makes sense because most digital transactions use these forms of payment. However, with the growth in alternate payment methods, the number attack surfaces have multiplied, giving cyber thieves many, many targets from which to choose.

We see little innovation in attack methods associated with debit and credit cards. Most attacks approach payment card theft in the same way they have for the past 10 years, by attacking payment mechanisms or the databases containing card data. Once they have obtained the card data, they sell it as quickly as possible and pocket the profit.

Now, however, the game is changing. Given the plethora of payment methods, most of which still require usernames and passwords, credentials have become very valuable. To steal credentials, the cybercriminals are targeting the consumers directly because they are both the source of the credentials and the weakest link in the payment process.

We predict that in 2016, payment system cybercriminals will increasingly focus on attacks that lead to the theft and sale of credentials. We think that they will leverage traditional, time-proven mechanisms including phishing attacks and keystroke loggers, but new methods will emerge too. We also predict that the number of payment system thefts will continue its relentless growth.

—Raj Samani

Attacks through employee systems

High-profile attacks continue to increase in frequency. This year we have seen major attacks against large enterprises, governmental agencies, and even dating sites (Ashley Madison). And we're no longer talking just about defaced homepages. Personal information including credit cards, social security numbers, and addresses for millions of individuals has been stolen this year alone. Unfortunately, we expect this trend to continue.

The hacks of the past few years have made security a common boardroom topic—not one that can be brushed under the carpet. We now see more spending on security. Unfortunately, a lot of this money may not be spent in the most effective manner, but we will see the overall security investment rise for most businesses. Smart organizations will spend their money not just on technology, but also on more training, awareness, and personnel.

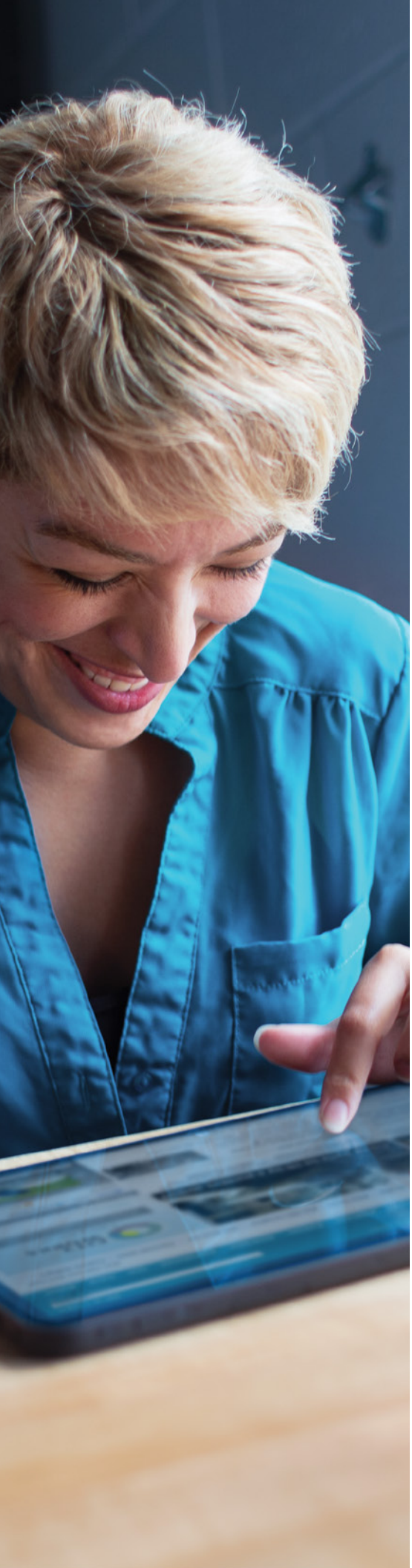
What does this mean for the attackers? If an organization has the latest technology installed with smart people in place to create effective policies and remain vigilant, attackers have few options. Nonetheless, attackers will:

- Try harder. No security is 100% foolproof. If attackers really want your data, they will get to it. It takes just time and effort, which ramp up almost exponentially when smart people and good technology are in place.
- Go after someone else. Those organizations that spent their budget ineffectively (maybe buying the latest tech, but not funding additional headcount to run it) will continue to be (relatively) easy targets and continue to be hacked.
- Attack employees at home or while traveling. If attackers really want to get at your data, but find themselves blocked at every attempt against the corporate data center, then the relatively insecure home systems of the employees become the next logical target.

Getting into the enterprise via employees outside of the protected network is nothing new. One of the first highly visible examples (Operation Aurora) took place in 2009. Since then many other incidents have breached a corporate network after compromising either a company laptop connecting from a coffee shop or hotel, or a personal system at the employee's home.

Research indicates that the number of attacks continues to grow. Next year, we should expect to see at least one, if not more, major attacks that start with an employee-owned system or a company system that is in an insecure location such as a hotel or coffee shop. Given that the recent Stagefright vulnerability highlighted some areas for potential exploitation, we should also expect Android devices to serve as a gateway into secure environments for malware or advanced persistent threats.

This threat should lead to IT organizations taking a hard look at what it means to be secure. It isn't enough to worry about security only on your company's network. Smart organizations need to expand their protection into the homes of their employees.



Currently, most organizations provide employees with VPN software to allow for a secure connection to the enterprise network. That is a great way to ensure that the communication from the employee's work system to the office is secure. However, most people access the Internet from multiple devices. Although a company laptop may be secure, who knows what protection employees use on their home systems? Most organizations deploy firewalls, web and email gateways, IPS, and other technology to secure their infrastructures, yet most home users barely have antimalware installed and typically have no firewall or gateway. These omissions leave employees wide open at home as targets of an attack directed at their employers.

In the next year or so, we expect to see organizations providing more advanced security technology for employees to install on their personal systems—to help protect against threats entering through social networks and spear phishing.

—Bruce Snell

Cloud services

Business-oriented cloud services have become ubiquitous. Companies have embraced cloud-based collaboration for the convenience of conferencing, cost-effective data storage, and accessibility of connecting with anyone, anytime. The adoption of cloud services and storage is pervasive in our increasingly connected global business environment.

The level of confidential company data shared on these services and platforms is alarming: business strategy, company portfolio stance, next-generation innovation, financial data, acquisition and divesture postures, employee data, and much more.

Because cloud services such as these often contain or are used to convey trade secrets, they are attractive to cybercriminals, competitors, and nation-states who wish to steal the information. Customers of these services are at the mercy of security controls at the hosting service and have little insight into the service provider's security posture.

Recently hackers penetrated the computer systems of a major newswire service and stole confidential information that they used to illegally make stock trades, resulting in millions of dollars in unlawful profits.

The hacking and exposure of stolen sensitive client information against the online dating site Ashley Madison, covered by Fortune and Krebs on Security among many others, caused plenty of embarrassment and concern for all the parties involved. This breach bypassed weaknesses in the site's security.

We saw multiple examples of data breaches throughout the year that exposed information about employees, including emails and salary information, as well as cases in which unreleased content was stolen and made public. No one was immune to attacks—even the controversial Hacking Team was a target earlier this summer.

With or without IT's consent, most businesses use low-cost or free cloud collaboration services, but security details are often not shared; the risk of hacking and data exposure is unknown. Whether using video conferencing and voice mail, project management tools, data storage sites, or cloud-hosted applications, employees can put companies at risk by accessing and storing company data on third-party sites that do not offer proper oversight on security management. The opportunity for attacks targeting the back-end infrastructure to steal information, or listen to private conversations, including your conference meetings, can be exploited.

A cloud service provider must be always alert to the emerging threat landscape and adapt its security controls to address hackers' evolving techniques. Protecting cloud services requires taking a comprehensive approach to security controls, including addressing the potential opportunities for social-engineering capabilities used to gain access to data. Protection also requires ensuring that a strong level of encryption is implemented, with access to data only by authorized users.

We predict, as these examples show, that cybercriminals, nefarious competitors, vigilant justice seekers, and nation-states will increasingly target hacking into cloud services platforms to exploit companies and steal valuable and confidential data, using it for competitive advantage, or financial or strategic gain.

—*Jeannette Jarvis*

Wearables

During the past two years, we have seen tremendous growth in the Internet of Things (IoT). When the IoT movement began, the focus was primarily on making current devices and products "smart" by embedding computing and wireless connectivity. Categories such as smart TVs and the connected home quickly showed a lot of promise. Recently we have seen rapid growth in the number of wearable devices—such as activity trackers, smart watches, and other portables. (I am wearing two devices as I write this.)

Although today much of the focus is on the Apple Watch, the increase in wearables will continue to grow, thanks to a robust industry led by well-known names such as Fitbit and Pebble. These established companies and newcomers will contribute to an estimated 780 million wearable devices by 2019, according to ABI Research, which works out to a wearable device on one of every 10 people on earth. If we allow for fewer wearables in developing countries, that number is probably closer to one of every four or five people in wealthier countries who will have some sort of wearable device.

From a hacker's perspective, such densely populated areas will be a target-rich environment for attacking wearables. Although breaking into a wearable device does not necessarily provide immediate value for a hacker (although farming for GPS data could improve spear phishing), the real value lies in the wearable's connection to a smartphone.

Most wearables collect a lot of just simple data, and then feed it to an application on a smartphone or tablet for processing. Most of these devices use Bluetooth LE (low energy) technology, which has suffered a number of very well documented security flaws and likely will produce more with each new version. (Researcher Mike Ryan has done a lot of great research.) Bluetooth is the weak link.

Wearables Attack Surfaces

- Operating system kernel
- Networking software/WiFi
- User interface
- Memory
- Local files and storage system
- Access control/security software

- Cloud virtual machine and control apps
- Web app
- Memory
- Local files and storage system
- Access control/security software

Poorly written wearable code will create a back door into your smartphone. Initially, we doubt that a smartphone will be completely compromised by an attack through a wearable device, but we expect to see the control apps for wearables compromised in the next 12 to 18 months in a way that will provide valuable data for spear-phishing attacks.

One potential scenario: GPS data collected from a running app that is tied to a fitness tracker. The spear-phisher could use that data to craft an email that you would be more likely to open. If you stop by a coffee shop after your run, using the GPS data an attacker could write an email saying "I think you dropped this at the coffee shop this morning" and include a link to an infected image file.

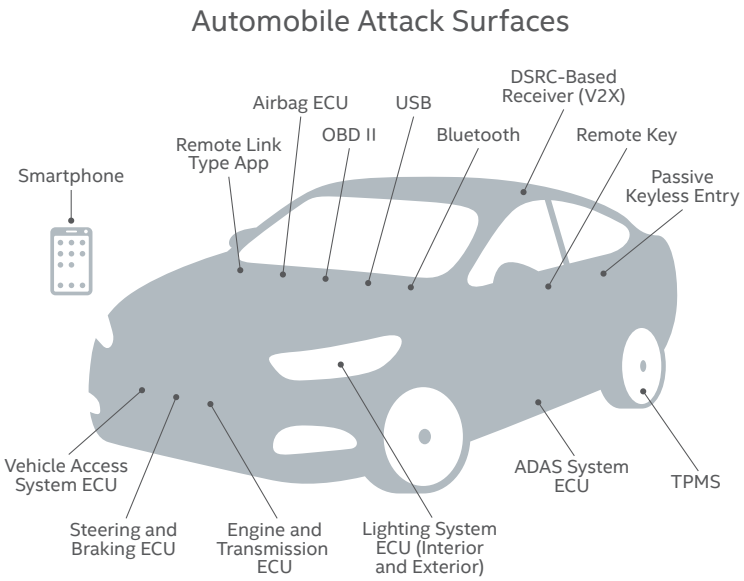
Wearables present a great way to motivate people to interact more with the world around them instead of staring at their phones or laptops, but they also pose a growing security risk from hackers as more people use them.

—Bruce Snell

Automobiles

Attacks on automobile systems will increase rapidly in 2016 due to the rapid increase in connected automobile hardware built without foundational security principles. Even cars need defense in depth, with layers of protection to reduce the risk and impact of a cyberattack. Poorly secured driverless cars and smart highways will further expose drivers and passengers in 2017 and beyond, likely resulting in lost lives.

According to the Business Insider "The Connected-Car Report," there will be 220 million connected cars on the road by 2020. Analysis portal Statista, citing a McKinsey report, predicts that 12 percent of cars will be connected to the Internet by 2016. Further, consumers want to surf the Internet via a monitor in the car (57%), automatic identification of traffic signals, congestion, and accidents (52%), a system that allows the passenger to stop the car (51%), front/rear end collision alarm warning (45%), night vision capability (42%), a fatigue warning device (41%), and access to social media while in the car (40%). All these features require software and hardware in the car to connect with external systems in a secure way to avoid unwanted or unauthorized actions in the automobile that could put passengers at risk.



Fifteen of the most hackable and exposed attack surfaces, including several electronic control units, on a next-generation car.

The Intel Security report *Automotive Security Best Practices* advises that the consolidation and interconnection of vehicle systems requires a security design that includes features such as "secure boot, trusted execution environments, tamper protection, isolation of safety-critical systems, message authentication, network encryption, data privacy, behavioral monitoring, anomaly detection, and shared threat intelligence." Today, many connected cars lack some or most of these security features. In August, several security researchers demonstrated that is possible to hack different types of connected cars, including a Jeep Cherokee, by sending commands through the Jeep's entertainment system to its dashboards functions, steering, brakes, and transmission, all from a remote laptop.

Even on systems designed to be secure, there is always the possibility that a bug or a vulnerability will be discovered, so there should be a way to easily and remotely update the software to fix the issue. Apparently, remote updates aren't possible with selected Cherokees, as well as Dodge and Chrysler vehicles because the parent company issued a safety recall affecting 1.4 million vehicles in the United States shortly after the security researchers disclosed the details of their research to the public. The only known manufacturer able to remotely update software is Tesla, which issued a remote patch after researchers disclosed a vulnerability at Def Con 23.

So far, current vulnerabilities have been responsibly disclosed to the manufacturers. We predict that in 2016, more automotive system vulnerabilities will be found by security researchers. It is also quite possible that zero-day vulnerabilities will be found and exploited in the wild by cybercriminals who may threaten people's lives, impact road safety, and create transportation deadlocks.

Some threats could already be lurking in automobiles. Non-safety-related threats that invade the privacy of the vehicle's owner by monitoring its location or listening to conversations using the car's microphone, or by even recording video using the car's cameras, could already be happening. We predict that 2016 will be the beginning of attack campaigns that may be discovered only months after the original infections.

—Carlos Castillo, Cedric Cochin, and Alex Hinchliffe

Warehouses of stolen data

Because security components such as firewalls, gateways, and end-point security products work well against common attacks in corporate environments, adversaries are looking for new ways to bypass these technologies. One way is through the acquisition and use of valid credentials. Cybercriminals can either harvest them through vulnerabilities or buy them on the "dark market."

Using valid credentials, adversaries fly below the normal security radar because they appear to be valid users. Often, the only giveaway is their behavior. Is the user's behavior normal or is it an outlier in some way? While the security industry is working hard to develop behavioral-detection capabilities using big data coupled with advanced analytic technologies, adversaries are abusing the current lack of behavioral detection by adjusting their attack methodologies to stay hidden. This adversary behavior will continue throughout 2016 and beyond, until behavioral-detection technology is in place and successfully detecting abnormal activities.

In 2015, a vast amount of data was stolen from businesses and governments. Some of the stolen records have limited value, but some is very likely waiting in secret locations for use in upcoming attacks. Further, the linking of stolen data sets may make the data significantly more valuable to cyberattackers. What if stolen data from a health-care provider, donor information, Madison Ashley, and the U.S. Office of Personnel Management were combined and stored in a data warehouse in the cloud? This information could lead to blackmail, the generation of new credentials, or identity theft.

This accumulation of stolen data has been going on for a couple of years. We predict that a robust dark market for stolen personally identifiable information and credentials will develop in 2016. Specialized underground warehouses will surface, offering stolen personal data, compromised credentials, and infrastructure details from multiple sources. Cybercriminals who are trusted customers of the dark web will be able to select specific sets of data to purchase for use in subsequent attacks.

—Christiaan Beek

Integrity

The one constant in cybersecurity is change. The industry continually evolves based upon the changes in technology, capability of attackers, value of potential targets, and relevance of resulting impacts. In 2016 we will see yet another expansion of tactics. One of the most significant new attack vectors will be compromises to the integrity of systems and data.

Confidentiality and availability attacks are loud, brute, and obvious. They break things and expose data—causing embarrassment, inconvenience, and some losses. Integrity attacks are stealthy, selective, and can be much more devastating. Instead of doing damage or making off with vast amounts of sensitive data, they instead focus on carefully changing particular elements within transactions, communications, or data to gain a significant benefit.

We have seen this in the past with a few elite state-sponsored attacks. Stuxnet and supporting Duqu, Flame, and Gauss malware were developed to stealthily target specific devices and make minor configuration changes that resulted in a major impact to a national nuclear program. Their intent was not to destroy a computer or harvest massive amounts of data. Instead, they selectively modified working systems to achieve the attacker's goals.

In early 2015 we witnessed cybercriminals use these tactics to attack banks. Carbanak was significantly different than previous banking malware, which focused on stealing account and login data. Carbanak stealthily compromised about 100 banks and enabled attackers to understand how internal operations were handled. The malware conducted reconnaissance for attackers who then began modifying selected transactions. When the attack ended, only a small number of accounts were targeted but somewhere between $300 million and $1 billion were stolen.

We see integrity attack research gaining momentum. Recent vehicle hacks are a great example. Researchers are not focused on shutting down the vehicle or harvesting data, but rather selectively modifying communications and commands so they can take control or affect what the vehicle does. This has a potentially terrifying result.

In 2016, we will witness an integrity attack in the financial sector in which millions of dollars will be stolen by cyber thieves who will modify selected data in the transaction stream, resulting in a significant redirection of payment to anonymized accounts. The detection of that incident and others like it will be very difficult. Integrity attacks can appear to be operational problems, accounting errors, audit issues, acts of a disgruntled employee, or simply dumb mistakes. To compound matters, the tools, mechanisms, and processes currently available and in use are mostly blind to these types of attack. Attribution will be challenging. Retail billing and sales; government identity records such as birth/death, taxes, and national insurance IDs; and banking accounts and ATM transactions will also be targeted. Other sectors such as healthcare records, billing, and prescription management and transportation control and management of cars, trains, and planes will eventually follow.

Perhaps one of the most prevalent vectors for integrity attacks is in the rise of ransomware, which modifies only a few files. Ransomware, a permanent form of a denial-of-service attack, leaves the system working with all data present, but due to the integrity compromise certain files are no longer usable. Attackers then demand a ransom to restore the original integrity. This attack vector will also grow significantly in 2016.

—Matthew Rosenquist

Cyber espionage

Last year, McAfee Labs predicted that in 2015 cyber espionage attacks would increase in frequency and become stealthier. As of this writing, we don't yet know whether there will more than the 548 cyber espionage incidents reported to have occurred in 2014 by the Verizon Data Breach Investigations Report. But we do know that espionage attacks have become stealthier and that they have become more impactful than prior breaches.

In one significant example, detailed in the blog post Stealthy Cyberespionage Campaign Attacks With Social Engineering, the threat actor used a sophisticated spear-phishing campaign to breach defense, aerospace, and legal-sector targets and minimize its footprint by running only JavaScript. The attackers were able to develop profiles for the breached systems and exfiltrate them to control servers.

In another example, a nation-state successfully breached systems in another nation-state's energy sector and inserted (among other things) custom-developed master boot record wipers that can disable or destroy their adversary's systems and networks. Again, the initial attack vector appears to be spear phishing.

And, of course, the successful breach and theft of roughly 20 million background checks from the U.S. Office of Personnel Management is a very clear illustration of the increasing strategic impact of cyber espionage activities.

In 2016 we will see more of the same. Some of the specific techniques threat actors will use:

- Legitimate services such as cloud file hosting (Dropbox, Box, and Stream Nation) will be used as control servers in upcoming cyber espionage campaigns. Threat actors will use legitimate infrastructure to remain under the radar and to evade the efforts of security researchers to sink-hole their assets. These cloud drive services will enable the malware to send and receive commands without raising suspicion, in addition to evading gateway defenses by appearing to be associated with valid traffic—thus increasing the longevity of the campaign.
- The use of the Tor network to anonymize connections to control servers will become more prominent in cyber espionage campaigns. Control servers will be hosted within the Tor network and will allow malware to make a connection without the need for the victim to have a Tor browser installed.
- In past years, threat actors exploited a variety of vulnerabilities in Microsoft documents. In 2016 we will begin to see the use of other file formats outside of .ppt, .doc, and .xls.

—Ryan Sherstobitoff

Hacktivism

The concept of hacktivism is not new. Driven by a clearly defined political or social point to make, a very skilled hacktivist group attacks a well-known entity and uses that platform to make its point. Hacktivists have been quite successful in making headlines and building their own hacktivist "brands" for more than 20 years. Anonymous is probably the best-known hacktivist group, but there are many others.

Source: "Anonymous at Scientology in Los Angeles" by Vincent Diamante. Originally posted to Flickr as Anonymous at Scientology in Los Angeles.

Licensed under CC BY-SA 2.0 via Commons—https://commons.wikimedia.org/wiki/File:Anonymous_at_Scientology_in_Los_Angeles.jpg#/media/File:Anonymous_at_Scientology_in_Los_Angeles.jpg

What has slowly changed over the past few years is the ease with which nonhacktivist actors can associate their own actions with such well-known groups using copy-cat operations. This trend appears to be obfuscating the ideology behind true hacktivist operations. The Ashley Madison hack, in which an unknown group released personal user data because purchase details were not removed as promised, does not sound like a high-minded, clearly defined political or social action, which is a cornerstone of a true hacktivist attack.

In another instance, a group claiming to be Anonymous executed a series of cyberattacks on Canadian police, court, and government institutions last year. Anonymous denied involvement, saying that they would not condone some of the actions taken by the attackers. No credible explanation was ever given for the attacks.

It is possible that these actions and others like them are the work of chaotic actors—those who just want to see things burn. If that is true, then we may be entering a world of vandalism at an industrial scale. It is also possible that the actual motivations are classic corporate cybercrime that is simply using hacktivism as a mask. Or, they could be a "false flag" operations, as Anonymous claimed in the Canadian attack. Whatever the true motivations for these attacks, the reality is that victim organizations will suffer significant major financial losses.

In 2016, we predict hacktivism in its true sense will continue; but it will likely be limited in scope in comparison with the past. Many of the most dedicated hacktivists promoting their causes have been arrested, prosecuted, and imprisoned. What is likely to increase, however, are attacks that appear to be inspired by hacktivism but actually have very different, hard-to-determine motives. The reality is that modern hacktivism is nothing more than a case of copy and paste and, as we have seen, our ability to lift the fog of obfuscation will be harder than ever before.

—Raj Samani

Critical infrastructure

If we believe the press reports coming from some security vendors, our future has become considerably more uncertain—with targeted attacks aimed at our critical infrastructure. Many of those highly publicized reports came after the 2010 attack by Stuxnet, which caused significant physical damage. However, it took years before a second successful attack against critical infrastructure appeared in the news. With only two publicly recognized instances since 2009, our 2016 predictions about critical infrastructure attacks must acknowledge that they are low-incident, but high-impact events.

That said, we are witnessing an ever more connected world, from digital oilfields to water treatment applications being hosted on the public cloud. The "isolated" nature of operational technologies is no longer the case, as discussed in research highlighting Internet-facing critical infrastructure devices. It should concern all of us that some of these devices use nothing more than default login credentials for protection. Add to this to an emerging trend in which criminals are selling direct access to critical infrastructure systems. The reality we now face is that the number of critical infrastructure vulnerabilities is increasing.

It is perhaps this escalation in vulnerabilities that led 48% of respondents representing critical infrastructure organizations to say that it is likely or extremely likely that a cyberattack will take down critical infrastructure and cause loss of human life in the next three years. Such a stark prediction is worrying, and although we don't want to overstate the threat, we must acknowledge that the broadening attack surface does increase exposure to such attacks.

Taking down a critical service may not be the attackers' only objective. The 2014 Dragonfly attack on energy companies illustrates that disrupting availability was not the malicious actors' near-term intent. In that instance, the attackers' objective appeared to espionage and persistent access.

Critical infrastructure attacks are less appealing to cyber thieves and more attractive to nation-state adversaries. The cybercriminal landscape is entirely focused on making money. Aside from examples of blackmail of critical infrastructure operators or the sale of access credentials to critical infrastructure, the return on investment for cybercriminals is better when they target other industries. As a result, the volume of attacks on critical infrastructure is and will continue to be far lower than on other targets. There are far more cyber thieves than there are nation-state attackers.

In 2016 and beyond, the growing number of vulnerabilities to critical infrastructure will be of significant concern. Successful attacks against these targets will have an enormous detrimental impact on society. However, most nefarious actors are making too much money elsewhere, so these attacks will likely come from nation-state actors who will be very selective and strategic in their actions.

—Raj Samani

Sharing threat intelligence

In the White House Summit on Cybersecurity and Consumer Protection held at Stanford University in February, President Obama announced a new U.S. government focus on sharing threat intelligence among government agencies so they can detect and act more quickly on cyber threats. He signed an executive order to promote even more information sharing around cyber threats between the public and private sector.

His action was an early indicator that sharing cyber threat intelligence is critical to improving national security. Although this move was a step in the right direction, much more will be required around the world to protect national security and the intellectual property of businesses while simultaneously protecting the privacy of citizens. Cyber threat intelligence is "curated" information about an attack or adversary that can be distributed for the purpose of improving defenses against these attacks. It typically includes context, indicators of compromise (IoCs), and actionable steps that can be taken to stop them. Shared threat intelligence allows companies and governments to combine internal evidence with external information to better spot attacks and react accordingly.

Intel Security became one of four founding members of the Cyber Threat Alliance to facilitate threat sharing across a trusted community of industry participants in an automated and efficient way. Cyber Threat Alliance members share IoCs and other information focused on the complex and subtle aspects of active cyberattacks, providing timely visibility in the activity and techniques being used.

Shared threat intelligence and collaboration is instrumental in rapidly combating the adversaries' aggressive drive, whether they are targeting critical infrastructure, a company's intellectual property, or an individual's personal information. Leveraging the Cyber Threat Alliance members' expertise will help us react smarter to complex multidimensional attacks.

In 2016, the Cyber Threat Alliance will adopt the STIX/TAXII standard for threat intelligence sharing, which will speed time to detection and correction for all Alliance members. The Cyber Threat Alliance is one of many industry-driven threat intelligence sharing cooperatives, all in various stages of maturity but all with similar goals. In 2016, metrics for success will begin to emerge so that customers and governments will have a better understanding about how much these cooperatives can enhance protection.

It is less clear whether systematic cyber threat intelligence sharing between industry and government will take off in 2016. We may see legislative steps taken to reduce businesses' potential legal liabilities, thereby enhancing the ability to share threat intelligence. But if laws are enacted, we will undoubtedly see significant challenges to these steps in the courts.

The Department of Homeland Security recently awarded a grant to the University of Texas at San Antonio to work with threat information–sharing organizations and operators of critical infrastructure, federal agencies, and the public and private sector to develop guidelines around rapid information sharing. As a result in 2016 we will see an acceleration in developing best practices for sharing emerging threat information to suit industry needs.

—*Jeannette Jarvis*

Follow McAfee Labs

About McAfee Labs

McAfee Labs is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

www.mcafee.com/us/mcafee-labs.aspx

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world.

www.intelsecurity.com

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com