McAfee Labs 2017 Threats Predictions

November 2016

REPORT

McAfee™
Together is power.

McAfee Labs explores top threats expected in 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.

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


Follow McAfee Labs Blog


Follow McAfee Labs Twitter

Introduction

Welcome to the McAfee Labs 2017 Threats Predictions report. We have split this year's report into two sections. The first section digs into three very important topics, looking at each through a long lens.

- Kicking off the report is our big-picture take on difficult-to-solve problems in cyber security and the security industry's early efforts to solve them. We brought together a wide variety of thought leaders at McAfee to discuss the most pressing technical security challenges that they see. We then grouped and abstracted those challenges. The top six problems are presented in this story.
- Our next story looks at cloud threats. Eleven McAfee thought leaders collaborated to produce this look-ahead at cloud threats and expected legal and industry responses during the next two to four years. What threats and breaches do we expect to see? How will geopolitical issues, legislation, and regulatory actions affect this environment? And what responses do we anticipate from cloud service providers and security vendors?
- Our final long-lens story is about threats to the Internet of Things. Using the same approach as the cloud threats story, 10 McAfee thought leaders offer predictions about threats and breaches, laws and borders, and vendor responses.

The second section makes specific predictions about threats activity in 2017. Our predictions for next year cover a wide range of threats, including ransomware, vulnerabilities of all kinds, the use of threat intelligence to improve defenses, and attacks on mobile devices.

Among other things, we:

- Predict that ransomware will peak in the middle of next year but then begin to recede.
- Discuss why threat intelligence sharing will see major advancements in 2017.
- Explain why the physical and cyber security industries will edge closer together.
- Predict that hacktivists will target consumer privacy and describe how lawmakers and businesses will respond.
- Discuss why there will be even more cooperation between security vendors and law enforcement agencies to take down cybercriminals.
- Detail why vulnerabilities in several of the most common apps will continue to drop in 2017.
- Describe how the volume of "fakes"—product reviews, likes, ads, security warnings, and more—will continue to grow, eroding trust in the Internet.
- Explain why machine learning will be used to enhance socially engineered attacks.

We hope that these topics will provide valuable insight as you develop both near-term plans and long-range strategies.

We continue to receive valuable feedback from our readers through our Threats Report user surveys. If you would like to share your views about this Predictions Report, please click here to complete a quick, five-minute survey.

Happy holidays to you and your loved ones

—Vincent Weafer, Vice President, McAfee Labs

Contents

McAfee Labs 2017 Threats Predictions

These thought leaders collaborated to produce this report:

Jonathan Anderson
Yuriy Bulygin
Peter Bury
Torry Campbell
David Coffey
Carric Dooley
Brian Dye
Lynda Grindstaff
Barbara Kay
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Shishir Singh
Martin Stecher
Jamie Tischart
Ramnath Venugopalan
Lori Wigle
Candace Worley

The 2017 Threats Predictions were researched and written by:

Christiaan Beek
Yuriy Bulygin
Douglas Frosst
Paula Greve
Jeannette Jarvis
Eric Peterson
Matthew Rosenquist
Fernando Ruiz
Craig Schmugar
Rick Simon
Bruce Snell
Dan Sommer
Bing Sun
Adam Wosotowsky

Hard-to-Solve Security Challenges

Share feedback

Hard-to-Solve Security Challenges

—McAfee Labs

The world of digital information security does not lack for challenges. We see never-ending updates and patches in response to incremental changes by our adversaries. Major software releases introduce important new features but also unexpected vulnerabilities. Urgent notifications and fixes arrive after new exploits are discovered.

Big, hard-to-solve problems are those that require foundational research, new classes of products, heavy development time and effort, and a sustained focus, often by multiple industry participants working together. In this article, we discuss six of those challenges.

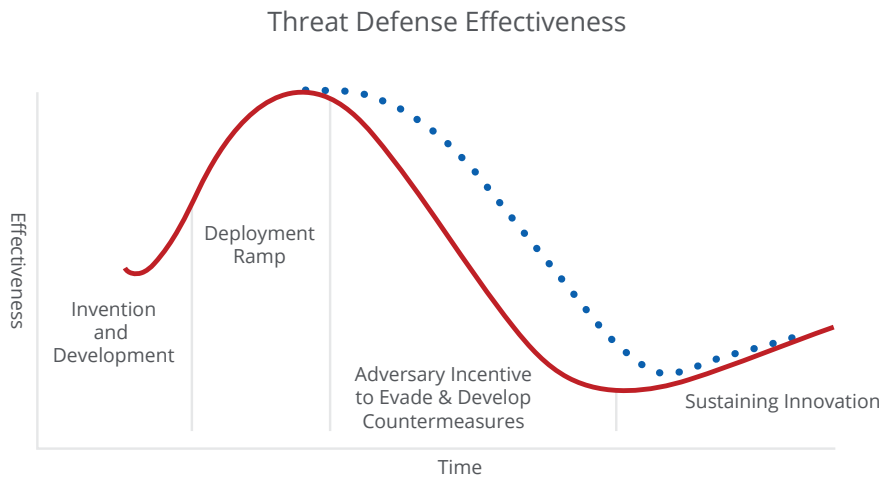
And then there are the big, hard-to-solve problems. These are the big-picture problems that cannot be addressed by patches or software updates. Solving these problems requires foundational research, new classes of products, heavy development time and effort, and a sustained focus, often by multiple industry participants working together.

During the past few years, the rapidly growing use of cloud services, the disappearing perimeter between internal and external networks, and an incredible flood of new devices are challenging traditional methods of protecting everything digital. This article discusses six big challenges facing the security industry and some examples of actions that the industry is taking to address those challenges.

Threat defense effectiveness

Attacks and defenses adapt and evolve in a continuing dance. The following chart illustrates the typical evolution of a type of defense over time. As a new technique is developed, its effectiveness increases rapidly until it is ready for deployment. Once deployed, broad exposure to real-world scenarios, feedback to the development team, and inclusion in other defenses further improves its effectiveness. The enhancement continues until it reaches a level of effectiveness that prompts adversaries to respond. At this stage, attackers experiment and discover ways to evade this type of defense and develop countermeasures to reduce its value.

As a new technique is developed, its effectiveness increases rapidly. That continues until it reaches a level of effectiveness that prompts adversaries to respond. Attackers discover ways to evade this type of defense and develop countermeasures to reduce its value. We need to improve threat defense effectiveness by moving the curve up and to the right.



The security industry's challenge is to improve the lifecycle of threat defense effectiveness by moving the curve up and to the right toward the dotted red line. Actions that collectively affect this lifecycle include:

- Reduce asymmetry of information between us and adversaries.
- Make attacks more expensive or less profitable.
- Improve visibility of security operations.
- Identify exploitation of legitimate tools and credentials.
- Protect decentralized data.
- Detect and protect without agents.

Reduce asymmetry of information

Adversaries have more information about our defenses than we have about their attacks. Attacks can be tested against security defenses with impunity. We do not see the majority of their tests, so we do not learn from them. We must find ways to prevent attackers from testing against us, detect and learn from their experiments, and mislead them where possible.

Adversaries have more information about our defenses than we have about their attacks, and this asymmetry significantly influences the threat defense effectiveness curve. Attacks can be tested against security defenses with impunity, whether in labs full of our gear or in the real world against deployed systems. They can test against us and we do not see the majority of their tests, so we do not learn from them. To shift the curve in our favor, can we figure out how to prevent attackers from testing against us, detect and learn from their experiments, and mislead them where possible?

Preventing attackers from testing against us is very difficult and possibly unsolvable. However, sharing info about attacks more broadly is one of the critical initial steps that we can take to address this asymmetry. When we share and combine information about attacks, we better understand what they are doing to find weaknesses in our algorithms. That allows us to more quickly adapt and improve defenses.

The greater volume of and detail in the telemetry flowing from such elements as cloud environments, virtual machines, and IoT devices helps us understand more. We are learning to apply data science to this information to better identify patterns of attack and more quickly create indicators of attack. We also have the potential to alter the predictability of our defenses, making it more difficult for adversaries to pinpoint specific weaknesses. This requires different layers of defenses to coordinate in real time so that an attack or probe that gets through one layer is stopped by another layer.

Make attacks more expensive or less profitable

Investigation and prosecution of cybercrime is inversely related to the severity of the crime. We must change the economics of the attack process, reduce the success rate of attacks, and make capture more likely, so we can make targets less interesting.

Money is the primary motivation of most cyberattacks. Can we make attacks more expensive or less profitable? If we can change the economics of the attack process, reduce the success rate of attacks, and make capture more likely, then we can make targets less interesting. Analyzing law enforcement data, we find that investigation and prosecution of cybercrime is inversely related to the severity of the crime. With physical crimes, prosecution is oriented toward the most serious crimes. With cybercrime, high-level attacks are more difficult to investigate and prosecute because they often cross multiple jurisdictions, and often more skills and resources are required to help them evade detection and prosecution. One potential response to this is to deceive attackers and increase their time spent on a given attack, making them easier to trace, identify, capture, and prosecute.

Security vendors have significantly increased their collaboration with law enforcement. We explicitly collect information that can help law enforcement and prosecution. Security companies focused on deception have entered the market, creating honey pots to trick adversaries with lures to draw them away from more valuable targets. Similar to historic law enforcement efforts with marked bills, vehicle tracking, and other traceability and recovery tools, cybersecurity is increasing the use of digital bait, alarmed files, and other indelible markings to help find attackers.

Improve visibility

We have finite control over information assets, and the level of control is diminishing due to the massive increase in the number and location of assets. We need to help organizations improve their security visibility.

Too often, organizations learn how well their assets are protected after they suffer a breach. Shadow IT, clouds of all types, and the bring-your-own-device movement further obscure visibility into the effectiveness of security operations. For decades, enterprises have been chasing the holy grail of identification and control over all corporate assets. The reality is that we have finite control over information assets, and the level of control is diminishing due to the massive increase in the number and location of assets. Almost no company will claim that they have a solid grasp of information asset locations and controls. So we need to help organizations improve their security visibility.

Security operations within companies and security vendors are shifting their focus from IT assets to data assets and from "pseudo-absolute" defensive coverage to informed risk management. We have tools that can identify and classify data, monitor its usage, apply appropriate policies, or block movement if necessary. With these tools, organizations can more effectively quantify their risk profile, identify critical gaps, and appropriately focus resources. Good organizations compare basic statistics to the previous month, much like accounting. Better organizations work to build regional, national, and industry benchmarks for comparison, like investors. However, many common security metrics are not very actionable. We think there is much more to be done to be able to act, in near real time, on threatening activities seen in the protected environment.

Identify exploitation of legitimacy

Many attacks begin through the use of stolen credentials. Telling the difference between when a legitimate tool is used for a legitimate purpose versus a suspicious activity is very difficult. We need to move toward a model that conducts legitimacy tests for every transaction.

Many attacks begin through the use of stolen credentials, followed by the use of legitimate administration tools that explore the target system and exfiltrate data. Traditional methods to detect illegitimate activity by looking for malicious or suspicious objects based on a file signature or other criteria do not work in this scenario. The objects used are known to be good, but are being used for bad purposes. So we are left trying to determine the intent of an action. Is this a business login or an attack? Is encryption being used for data purposes or exfiltration? Is this PowerShell session an admin function or reconnaissance?

Telling the difference between when a legitimate tool is used for a legitimate purpose versus a suspicious activity is very difficult. The only approach we have now is behavioral analytics, which is in its cybersecurity infancy. It is a good start, but we also need to move toward a model that conducts legitimacy tests for every transaction, not just for files and credentials. We need to analyze actions and data movement and try to determine intent, whether from an external actor or an unauthorized insider. This step requires knowing a lot more about the context of the activity.

One controversial possibility is the development of user reputation and predictive analytics. The concept is to assess the probability of a given account's being breached, stolen, or used for unauthorized insider activity. By collecting user behavior in context, from the tendency to reuse passwords on different systems to the job description and typical working hours, we can compare each action to a set of expected legitimate activities and flag those that are outside a given level of risk. This is a sensitive area. We will have significant privacy, ethics, and legal issues to address before this technique enters the mainstream.

Protect decentralized data

Data is moving around outside of the corporate perimeter, making it much more vulnerable to unintentional leaks and targeted attacks. It is moving to clouds and personal devices, but also to partners, suppliers, and customers. We need to better protect data as it moves and when it gets to its destination.

Data is moving around outside of the corporate perimeter, making it much more vulnerable to unintentional leaks and targeted attacks. It is moving to clouds and personal devices, as well as to partners, suppliers, and customers. How do we protect data as it moves and when it gets to its destination? Less than 20% of an organization's data ever moves in this extended ecosystem, yet 70% of data loss is connected to this movement. Today some try to protect this type of data movement by encrypting it and sending decryption keys in a separate email, passing on the responsibility for protection to the next person in the chain. This results in a very small sphere of trust. We need to figure out how to extend the sphere of trust while maintaining better control.

Data classification and loss prevention systems represent early efforts to manage and extend the sphere of trust for decentralized data. Security that moves with the data, enabling persistent policy enforcement, is the next step. We need to be able to protect data during its next use, similar to digital rights management mechanisms.

Detect and protect without agents

The ability to place agents on devices to protect them will not be possible in many future instances. We must find other means of protection.

So much of our history and strength in security is based on having an agent running on the device we are protecting. This will not be possible in many future instances. We see IoT devices with very little memory or computing capacity, operating systems that try to improve security by becoming more closed, a proliferation of operating systems and device types beyond the R&D capacity of any security vendor, and long lifecycle components in industries such as automotive and critical infrastructure that cannot be readily updated. The future of cybersecurity, and the solution to most of these big, hard-to-solve problems must take place in an agentless security world.

The evolution to agentless security is already underway, with early solutions attacking the problem from multiple directions. Chip designers are enhancing hardware-level security, memory protection, and trusted execution environments. Behavioral analytics products watch from the outside, ready to quarantine and investigate devices that are doing something suspicious or anomalous. Processing and analysis still has to happen somewhere, but we will increasingly leverage flexible computing resources instead of dedicated agents. Distributed enforcement points are already emerging that will spread enforcement throughout a network of devices, with multiple points communicating and collaborating in real time about their detection and protection actions.

Conclusion

Increasing our threat defense effectiveness throughout the security industry will be key to staying ahead of the adversaries. It is critical that multiple industry participants work together to solve big-picture problems that cannot be addressed by simple patches or software updates. We need to share information more broadly among industry leaders to not only give us greater volume and detail in telemetry, but also aid in deception techniques. By increasing our use of predictive analytics, improving security visibility with both organizational assets and decentralized data, and reducing our use of dedicated agents, we can increase our effectiveness in the threat defense lifecycle.

Cloud Threats, Regulations, and Vendor Responses

Share feedback

Cloud Threats, Regulations, and Vendor Responses

You can outsource the work, but you cannot outsource the risk

Cloud service providers are building trust and gaining customers. Increasing amounts of sensitive data and business-critical processes are shifting to public and hybrid clouds. Attackers will adapt to this shift, continuing to look for the easiest ways to monetize their efforts or achieve their objectives. Our focus is on the evolution of cloud security during the next two to four years. What threats and breaches do we expect to see? How will geopolitical issues, legislation, and regulatory actions affect this environment? And what responses should we anticipate from cloud service providers and security vendors?

Eleven thought leaders from McAfee collaborated to produce this look ahead at cloud threats and responses during the next two to four years.

Our lineup:

Yuriy Bulygin
Peter Bury
David Coffey
Carric Dooley
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Shishir Singh
Jamie Tischart
Candace Worley

In this article, we answer these questions:

- What cloud threats and breaches do we expect to see?
- How will geopolitical issues, legislation, and regulatory actions affect the cloud environment?
- What responses should we anticipate from cloud service providers and security vendors?

Threats and breaches

Cloud services continue to multiply, mature, and grow at a rapid pace, providing organizations, criminals, and nation-states with new opportunities and threats. We distilled the following 11 predictions from our discussions, as the most prominent and probable outcomes in the next two to four years.

Trust in the cloud will increase, leading to more sensitive data and processing in the cloud, leading to more interest in attacking the cloud. This first prediction is easy, but it sets the foundation for the rest of our cloud threat forecast. During the past couple of years, the shift to cloud applications, processing, and storage has accelerated, and we expect this trend to continue. Cloud service providers have significantly improved and will continue to improve their security controls and assurances to customers. Absent a major breach or outage affecting multiple companies, countries, or segments of the economy, trust in the cloud will continue to rise. Organizations of all types and sizes will move more and more of their processing and data into clouds, and many businesses will become completely cloud dependent. Attacks will adapt, new threats will emerge, and breaches will happen.

Businesses will continue to hold the crown jewels in their own trusted data centers and networks. Despite this move to the cloud, most businesses will not completely divest themselves of their private processing and storage capabilities, and will keep some of the data and intellectual property that is core to the business close at hand. Ironically, public clouds are arguably more secure than private clouds, as they often have a broader and deeper security team with expertise from chip through app. Companies building a private cloud must be confident that they can secure all layers of the stack, from apps to operating systems, from hardware to hypervisor. Today, companies find it increasingly difficult to protect the crown jewels because the perimeter is less clearly defined. The growing use of cloud services will exacerbate that, requiring companies and their cloud service providers to become more articulate about what is allowed to go where, and under what type of protection.

We will continue to see conflicts of speed, efficiency, and cost pitted against control, visibility, and security in cloud offerings. Providers and their clients will choose different balancing points.

We will continue to see conflicts of speed, efficiency, and cost pitted against control, visibility, and security in cloud offerings.
For organizations that have not yet embraced the cloud in a meaningful way, the number one barrier to greater adoption is security. (However, these organizations already are in the cloud because many of their employees have files on Google, Dropbox, iCloud, OneDrive, or other services.) For those that have already moved to the cloud, security drops to the number two or number three barrier, after operational consistency and financial oversight. This will be reflected in cloud offerings, as service providers walk the line between offering speed, efficiency, and cost on the one hand versus the desire for control, visibility, and security on the other. Providers will choose different balancing points, which will ultimately manifest in prices and service agreements, providing companies with options that best suit their desired risk profiles. Although cloud services today are mostly virtualization of storage, servers, and applications, during the next four years we expect services to become increasingly granular. The cloud will become more event-driven containers and less server-based code. Containers will have much shorter average lifespans than virtual machines, operating on code and data that then disappears. This shift toward greater speed and efficiency will drastically increase the pressures on and conflicts with security.

Antiquated authentication schemes and their control systems will continue to be the weakest technology link in cloud protection. We expect an increase in targeted credential theft and brute-force attacks against administrator accounts.

Antiquated authentication schemes and their control systems will continue to be the weakest technology link in cloud protection; many attacks will focus first on credential theft.
Passwords, and the people who create and use them, will remain the biggest weakness throughout most technologies for the foreseeable future. Cloud authentication is no different and represents a much bigger payoff for thieves. Attackers, some of them very patient and sophisticated, will mine social networks, previously stolen passwords, and other personally identifiable info to steal credentials, especially focusing on cloud administration credentials. Targeted phishing attacks, fake recruiting campaigns, and other techniques are already in use, and will continue. In-house authentication systems, such as Active Directory, have limited ability to interact with the authentication systems used by cloud service providers. The proliferation of cloud apps and services, and human fondness for using the same or similar password for each cloud service, exacerbates the problem. Expect an increase in targeted credential theft and brute-force attacks against administrator accounts, and pay close attention to administrator account activity.

Attacks will come from all directions and leverage both east-west and north-south attack vectors.
As we have heard discussed at Black Hat and other security conferences, cybercriminals continue to explore and successfully exploit new vectors of attack. In traditional systems and networks, most attacks follow a "north-south" pattern, trying to move up or down the stack to increase their privileges, exploit a vulnerability, or gain access to data or applications. Cloud attackers will continue using this model, but will also look to take advantage of "east-west" opportunities. East-west attacks look to move from one virtual machine, container, or other cloud artifact to another, jumping between services and even between organizations. Attackers will use the scale of clouds and their increased attack surfaces to broadly scan for vulnerabilities, and then look to hit multiple organizations within the same cloud service provider or spawn malicious processes to provide a foothold for ongoing surveillance and exfiltration.

Gaps in coverage between service layers, and inconsistent settings or controls are the second weakest link. Attackers will successfully exploit these gaps and inconsistencies.

Gaps in coverage between service layers, and inconsistent settings or controls are the second weakest link; attackers will successfully exploit these gaps and inconsistencies.

There are many cloud service provider variants, from infrastructure to applications. Organizations are not always clear on the division of responsibilities between their cloud providers and themselves, leaving potentially exploitable openings in security. This is not a technology failure; it is a process failure. Organizations have the tools and know what has to be done, but sometimes assume that the other party is taking care of it. Furthermore, organizations that use multiple cloud service providers may have different security postures among providers, due to different or inconsistent controls or terminology. This is partly due to the multitude of security standards in use among cloud service providers—impacting consistency and, subsequently, the ability to compare like for like. These process failures and security control inconsistencies will provide fertile ground for cyber attackers until processes are better understood and cloud security control standards are more mature.

Visibility and control will continue to be key problems for businesses as they move computing and data to the cloud.

Cloud computing's ability to move processes and data around as needed provides tremendous benefits, yet also potentially serious security or privacy problems. We have already seen cases of employees being paid off to share their passwords. Not knowing, or not being able to control, where data resides or which processes execute will cause headaches for organizations of all kinds. Whether they are trying to keep data within a country's borders to comply with national privacy regulations, keep processes from executing in certain cloud environments due to security concerns, prevent sensitive data or intellectual property from leaving the premises, or simply understand their cloud usage patterns, the ability to view and constrain movement within and among clouds lags far behind the need. This use of legitimate things (apps, credentials, etc.) for possibly illegitimate purposes requires a move to context-based behavioral analytics. We expect these visibility and control problems to remain for the foreseeable future.

Attackers, including for-hire attackers, will use clouds for scale, speed, and anonymity.

Unfortunately, there is no simple way to prevent cloud resources from being used by attackers. Once these abuses are found they are shut down, of course, but this process can take months. In the meantime, attackers will leverage cloud resources for massive brute-force attacks, complex attacks along multiple vectors, and agile attacks that rotate among sites and countries to evade prosecution. Cloud data storage services will enable warehouses of stolen data, which can be mined for valuable connections and correlations. Constantly changing accounts, IP addresses, service locations, ephemeral containers, and other cloud characteristics will help the bad guys hide their identities longer and make them more difficult to track. This will not change during the next two to four years.

"Denial of service for ransom" will become a common attack against cloud service providers and cloud-based organizations.
Because one cloud can contain many tenants, there will be increased incentive to mount denial-of-service attacks against cloud service providers. Most service providers can defend against traditional denial-of-service attacks reasonably well. Nonetheless, attackers will continue to look hard for vulnerabilities that they can exploit. Once found, attacks will follow quickly. And if an organization becomes completely cloud based, there are multiple points between the business and the cloud that can be attacked to effectively shut down the business. This includes the Internet connection, DNS services, and other infrastructure components. To take down a cloud-dependent business, it is not necessary to directly disrupt the cloud service provider. Instead, attackers can disrupt access to the cloud and then hold the company for ransom.

Except for those based on credential weaknesses, successful public cloud data breaches will continue to be small in number, but they will have a growing impact.
Cloud service providers often have a higher level of cloud security expertise on their staff than the customers they serve, so we expect the number of successful cloud data breaches, except those that result from credential theft, to remain low. However, when a breach can provide access to large data stores from multiple customers, the potential consequences of a cloud data breach are significant. Whether the cloud service provider or the affected organizations will be more impacted by a breach will likely depend on who can demonstrate that they made all reasonable efforts in their area of responsibility.

Growth in the number and variety of Internet of Things devices will break some cloud security models, leading to successful attacks through these devices.
Most authentication involves interactions between people and a device, or between two devices. As more IoT devices and services come online, those devices will communicate with multiple other IoT devices and make trust decisions at machine speeds. The security fabric, trusted authority, and control over this type of communication is significantly lacking, resulting in leaks and vulnerabilities that can be exploited. Cloud service providers will struggle to force their current models onto this new environment, introducing significant amounts of latency and high degrees of complexity that are ingredients for security failures. We have already seen successful breaches through unsecured IoT devices into corporate networks, and clouds are next on the menu.

Laws and borders

Cloud threats and breaches will prompt political and regulatory responses. The speed of technology advancement will hinder effective legislation, and vice versa. Differing and even contradictory regulations among countries will make things more difficult for consumers, businesses, and cloud service providers.

Laws will not be able to keep up with technology advancement. Cloud service providers, their customers, and the emerging cyber insurance industry will face years of litigation before appropriate behavior is clearly established.

Laws will not be able to keep up with technology advancement. Regulations will use phrases such as "due diligence" and "reasonable efforts," leaving cloud service providers and their customers exposed to litigation.
The inability of laws to keep pace with technology change is not news. Laws pertaining to data protection and consumer privacy in the cloud are no different. Jurisdictions will look to phrases such as "due diligence" or "reasonable efforts" when referring to cloud data security in an attempt to deliver legislation that is effective and not immediately obsolete. Unfortunately, it will take time and a lot of litigation to define these terms in sufficient detail through legal precedence. There are often no simple yes-or-no tests that can be applied to cybersecurity for systems and data, especially in the cloud, in which multiple entities must together provide protection. Meanwhile, cloud service providers, their customers, and the emerging cyber insurance industry will face years of litigation as plaintiff and/or defendant over whether their efforts were "reasonable." Public perception will play a role, as companies whose cloud has been breached strive to demonstrate that they did everything they could to protect their customers.

The movement of data in and out of jurisdictions will be an ongoing challenge. Legislation to protect consumers will inhibit cloud adoption.
In an attempt to protect consumers' privacy, political bodies will pass legislation that requires organizations collecting personal information to store it within the same borders as the citizens they represent. This will be a challenge for corporations, which will be required to identify and classify their data, and for cloud service providers, which will be required to provide increasingly granular controls for data and process movement. What happens to the service agreement if a major cloud data center in one country is affected and the closest backup is across a border? How will a multinational corporation separate customer, sales, and product data so that controls can be applied in accordance with these new laws? These and similar challenges will inhibit cloud adoption, as organizations will either be forced to build their own data centers in some countries or decide that it is too expensive to do business there.

Some jurisdictions will impose minimum operating requirements, certification, and/or auditing on cloud service providers and their business associates.
What happens to the data when a cloud service provider goes bankrupt? How are businesses and consumers protected from criminals or nation-states creating malicious cloud services whose primary purpose is data collection? What are the legal requirements between a cloud service provider and their subcontractors or business associates? Another likely response from political bodies is the imposition of minimum operating requirements, independent certifications, or auditing conditions on cloud service providers operating in their countries. Defining the terms and relationship tiers will be a significant challenge, provoking strong opinions and intense discussion within the industry. Regardless of the laws, the risks and biggest consequences of a data breach will be borne by the lead service provider, not the subcontractors or associates.

Vendor responses

Threats, breaches, and legislation will prompt technology and service responses from cloud providers and security vendors. Authentication systems will be enhanced, business-level controls developed, security functions automated to reduce gaps and inconsistencies, and threat intelligence sharing will improve detection. Below are our expectations of the top ten responses to cloud threats during the next two to four years.

Passwords must be replaced by more secure authentication systems, but they cannot overly impede the login process. Biometrics, multilevel authentication, and behavioral analytics will help "protect the cockpit" for both cloud service providers and their customers.

Biometrics, multilevel authentication, and behavioral analytics will help "protect the cockpit" for both cloud service providers and their customers.
Passwords must be replaced by more secure authentication systems, but they cannot overly impede the login process. In the short term, we expect to see an increase in multifactor authentication, often using mobile phones, or challenge-and-response systems. We will see this first for administrators because the impact of administrator credential theft is most acute. We will also see some use of behavioral analytics to detect abnormal activity in account logins. In the long term, we expect to see a big increase in the adoption of biometrics, in form factors that people find comfortable and easy to use. Fingerprints will be replaced or augmented by other unique factors, such as faces, heartbeats, or retinas, as implementation becomes commercially viable.

Business-level visibility and control will help manage the movement of information to the cloud by shadow IT and orchestrate the complexity and volume of work performed in the cloud.
Cloud service providers make it possible for a department or line of business to move a workload to the cloud without involving IT. In many companies, the security or IT teams may not know when data or processes are moved to the cloud by these entities, potentially exposing the entire business. Vendors are being asked to respond to this with tools to increase the visibility and control of data. We expect data loss prevention and policy orchestration tools to become increasingly cloud aware. The next step will be cloud-enabled extensions that make it possible to apply security controls and policies directly with the cloud service provider.

Security assessment, authentication, mitigation, and cloud auditing are some of the areas in which automation can augment human experts, which will help address the talent shortage.

Security automation will help address the talent shortage.
The security skills shortage will be a threat and an opportunity for cloud service providers. Turning the threat into an opportunity requires building security experience into automated tools and bots that simplify cloud security controls so that more people can effectively set and monitor their protections. Security assessment, authentication, mitigation, and cloud auditing are some of the areas in which automation can augment human experts, add contextual awareness, and extend functionality to business managers.

Cloud access security brokers will continue to mature, offering better security, increased visibility, and more control.
Discovering and applying policies and authentication to cloud services will remain important for protecting the organization. A cloud access security broker (CASB) is a good way to enact and enforce policy, but it will not solve the core problem of authentication. Most value is in the data, and that will increasingly be the focus as CASBs mature and coordinate or integrate with other security systems to decide which data in the cloud needs to be secured and how.

Increased protection of data at rest and in motion will become a competitive advantage for some cloud service providers.
Some foundational cloud services, such as storage or processor rental, are becoming commoditized. To differentiate themselves, some cloud service providers will offer additional protections for data stored on, processed by, and transiting through their systems. More than offering just encryption, these premium services will include integrity checks, real-time monitoring, and enhanced data loss prevention techniques to deliver a long-term competitive advantage.

Auditing and visibility of cloud service provider operations will become the norm.
Whether as a result of customer demand, competitive pressures, or industry regulations, real-time auditing and visibility will become a standard offering for most cloud service providers within four years. The ability to answer the customer question "Where has my data been?" will move rapidly from differentiator to standard cloud service component. Static audits and historical views are not enough to ensure sufficient levels of protection for high-value data and workflows.

Security solutions will become predictive and prescriptive, helping detect emerging threats and stop attacks well before systems are compromised.

Security solution vendors will begin to use machine learning to predict and stop attacks before they have done harm.
Security solutions that protect the cloud infrastructure itself will become extremely critical, because compromising the infrastructure delivers direct access to the applications and data of multiple customers. The volume of events will be overwhelming, so we will see continued development of sophisticated, automated tools that can quickly diagnose and resolve incidents. Building on those using machine learning and big data analytics, security solutions will become predictive and prescriptive, helping detect emerging threats and stop attacks well before systems are compromised.

We will see much more threat intelligence sharing among businesses and cloud providers, which will improve identification of and reaction time to attacks.

Threat intelligence sharing organizations will form among cloud service providers, which will improve identification of and reaction time to attacks.
Today, some organizations and cloud service providers do not perceive the benefits of threat intelligence sharing. Within the next few years, whether driven by legislation or the aggressiveness of attacks, we will see much more threat intelligence sharing among businesses and cloud providers and the benefits will become clear. Although it may sometimes be embarrassing, organizations will realize that the benefits of sharing intelligence in real time about failed and successful attacks easily outweigh the disadvantages.

Cloud security technical and assurance standards will continue to strengthen.
The Cloud Security Alliance, among others, has developed standards, guidelines, certifications, and best practices for the management of cloud services. To date, they have focused on the development of standards and guidance that deliver better transparency to customers. Cloud security standards are currently a bit of a patchwork, but there is growing agreement on the meaning of secure cloud design and operation. We anticipate during the next two to four years that assurance standards will become well defined, more consolidated, and be embraced by leading cloud service providers.

The cyber insurance market will grow, but will be challenged by the interpretation of reasonable efforts and whether an insurable event occurred.

We expect insurance companies to offer cyber insurance, as well as security ratings that will help reduce insurance costs. Some countries will introduce legislation and regulations, and combined with the maturity of cloud service offerings, will help increase trust in them. However, cloud insurance will remain a subjective business, with many escape clauses. The infrastructure and experience necessary to make objective decisions about costs, claims, and insurable events will not exist within this timeframe.

Conclusions

Continued rapid growth in the use of cloud services means that those services will become increasingly valuable as targets of attack. Although many companies will continue to hold their most sensitive information within private data centers, the pressures of speed, efficiency, and cost will push more data outside the trusted network and into clouds, where those benefits can be realized. As enterprises learn how to cloud-enable their operations, gaps in control, visibility, and security will lead to data breaches.

Attacks will come from all directions—moving both up and down an organization's stack and between co-located businesses. Credentials and authentication systems will continue to be the most vulnerable point of attack, so cybercriminals will work hard to steal credentials, especially admin credentials because those can provide the broadest access.

The certification of cloud service providers, minimum operating requirements, and other regulatory controls will be a common legislative response to security and privacy concerns. These will vary widely by jurisdiction, in some cases acting as a brake on cloud adoption. Multinational organizations will find themselves carefully navigating around and across borders. Laws will fail to keep up with advancements in cloud technology and service offerings. Litigation will play a role, mostly after breaches, as plaintiffs and defendants try to determine whose efforts were "reasonable."

Cloud service providers and security vendors will work to enhance authentication systems, gradually adopting biometrics as the best solution. Service providers and their customers will push for greater visibility, and real-time auditing will become a standard offering. Technologies will emerge to better protect data at rest and in transit. To address the volume and speed of threats, behavioral analytics, security automation, and shared threat intelligence services will be leveraged to improve detection and correction capabilities. Machine learning will emerge as a way to predict and stop attacks before they can cause harm.

IoT Threats, Regulations, and Vendor Response

Share feedback

IoT Threats, Regulations, and Vendor Response

So promising, but welcome to the Wild West

Ten thought leaders from McAfee collaborated to produce this look ahead at IoT threats and responses during the next two to four years.

Our lineup:

Jonathan Anderson
Yuriy Bulygin
Carric Dooley
John Loucaides
Scott Montgomery
Raj Samani
Rick Simon
Ramnath Venugopalan
Lori Wigle
Candace Worley

In this article, we answer these questions:

- What IoT threats and breaches do we expect to see?
- How will geopolitical issues, legislation, and regulatory actions affect the IoT environment?
- What responses should we anticipate from IoT device developers and security vendors?

The threat of IoT attacks is real, but opportunities for profit-seeking criminals are still unclear. Cybercriminals will find profitable models, and financially motivated attacks will become widespread.

The Internet of Things encompasses hundreds or thousands of types of devices in every industry. In fact, IoT should not be thought of as devices, but as networks of devices enabling and offering services, many of which are cloud based. As a result, IoT threats and responses are intimately linked with cloud threats and responses.

In many industries, those cloud-enabled device networks can be thought of as communities of interest. For example, a factory floor is a community of interest for the manufacturer, and the network contains the devices required to manufacture goods. In a hospital setting, the medical devices and associated network that serve the needs of medical staff represent a community of interest.

The opportunities to steal data, deny operations, or cause damage will be very broad. For this article, we focus on the evolution of IoT security during the next two to four years. What threats and breaches do we expect to see? How will geopolitical issues, legislation, and regulatory actions affect this environment? And what responses should we anticipate from IoT device developers and security vendors?

Threats and breaches

IoT devices are attractive to cybercriminals or nation-states for one or two reasons: They are a potential source of data or metadata, or a potential attack vector to cause damage. We distilled the following 10 predictions from our discussions, as the most prominent and probable outcomes during the next two to four years.

The threat of IoT attacks is real, but opportunities for profit-seeking criminals are still unclear.

Vulnerabilities and opportunities to attack IoT devices exist today, but opportunities to make money from attacks are limited by insufficient quantities of any particular IoT device in high-value locations on networks, and the lack of clear models for monetizing an attack. Should IoT devices be held for ransom, targeted for stolen data sold on the dark web, or used to cause damage such as widespread outages to an organization? Within the next four years, cybercriminals will answer these questions, and financially motivated attacks will become widespread. Interestingly, opportunities to cause damage are far more feasible, but we have seen only a few of these to date, possibly because the potential perpetrators are afraid of retaliation.

Ransomware will migrate to IoT, as it has proven to be a relatively easy way for criminals to make money.

Ransomware will be the primary threat.
One of the challenges when making threat predictions is linking potential motivations with actual opportunities. Some widely publicized IoT device hacks or vulnerabilities are simply too difficult to conduct on a large scale. We are certain that ransomware will readily migrate to IoT, as it has proven to be a relatively easy way for criminals to make money. Disrupting one or more IoT devices, their control plane, or their cloud aggregation point, and holding them hostage is an easier and faster way to make money than compromising a large number of devices quietly to siphon data. We already see IoT devices being held for ransom in the power distribution and health care verticals.

Hacktivism will be the biggest fear.
Although ransomware will be a reality for many organizations with IoT devices and connections, hacktivism will be their biggest fear. Our reasoning is that most criminals want to make money, so damaging or seriously disrupting a business is not in their interest. However, activists usually look to make their point with a disproportionate display. Whether it is taking control and altering voting machine tallies, opening valves at a dam, or overriding safety systems at a chemical plant, the potential for catastrophic damage is real. Within the next two to four years, we expect hacktivists to try, but few if any will succeed.

Nation-state attacks on critical infrastructure will be an ever present concern, but will occur sparingly due to concerns over physical or cyber retaliation.
Nation-state attacks are the big brother of hacktivism. The opportunity to damage or disrupt the military or economic capabilities of another country is real, and we have already seen a few attacks during the past year. Those attacks have mainly been on SCADA systems, which are a type of IoT device. However, the fear of military, economic, or cyber retaliation by the victim will limit the frequency of nation-state attacks on critical infrastructure.

IoT devices will rapidly push the boundaries of current privacy laws, and political bodies will continue to slowly react.

IoT will significantly reduce consumer privacy.
Reports of privacy's death have been exaggerated in the past, but IoT will move us closer to its demise. There are simply too many IoT devices watching, listening, recording, accumulating, and otherwise paying close attention to consumer actions. In many cases, consumers are paying a company for service and letting themselves be tracked for free. Sure, the details are in user license agreements, but most consumers don't read them and cannot opt out anyway. IoT devices will rapidly push the boundaries of current privacy laws, and political bodies will continue to slowly react. Privacy expectations will impact device vendors and service operators, as some governments will require explicit agreements, opt-ins, and even compensation for using or sharing someone's data.

We will see more instances of IoT devices used as gateways to data and intellectual property theft, critical infrastructure disruption, and other major attacks.

IoT devices will be useful attack vectors into control, surveillance, and information systems.

During the next two to four years, we will see more instances of IoT devices used as gateways to data and intellectual property theft, critical infrastructure disruption, and other major attacks. Many new IoT devices coming to market have weak or no security. IoT devices already in use often have similar weaknesses or known vulnerabilities that cannot be patched or upgraded. In other cases, innocuous devices are connected to the network without appropriate isolation or segmentation, inadvertently providing access to trusted environments. Finally, there is pressure from operations: "It's working. Don't touch it!" These elements add up to IoT devices becoming open windows into many types of systems and organizations.

Device makers will continue to make rookie mistakes as they IP-enable their products.

There are two primary reasons why companies will IP-enable their devices: to improve efficiency and to collect data about device usage. Some of these companies have little or no prior experience with Internet-connected devices. As a result, many will make rookie mistakes, learn lessons, and otherwise repeat the history of Internet security. Unfortunately, they will be doing so in a more hostile environment. Some combination of breaches, regulations, and learning are necessary to make security by design a part of regular activities at all organizations. This learning period will last longer than four years.

The control plane of IoT devices will be a prime target.

When people talk about IoT attacks, they often mean attacks aimed directly at IoT devices. Although device-level attacks are certainly common, they are often difficult to scale. Attacking one autonomous car, connected valve, or smart door lock does not provide much in the way of payoff. As a result, attackers will often prefer going after the control plane for IoT devices. Control planes have some level of privileged access to monitor processes and change settings on multiple devices. While security efforts have been focused on IoT devices themselves, less effort has been applied to the systems that control those devices. The expected scale of most important IoT device deployments means that their control planes will be complex, with a very large attack surface. Attackers who can affect the integrity of messages in the control stream, or can compromise the controller itself because of weak authentication or stolen credentials will have a bigger payday.

Aggregation points, where data from IoT devices is collected, will be a prime target. Credentials and authentications systems are the weak points.

Aggregation points, where data from devices is collected, will also be a prime target.

Another potential weakness in IoT systems is the aggregation point, where data from multiple IoT devices is collected. Like the control plane, compromising the aggregation point presents an opportunity for a big payday. Instead of attacking multiple devices and slowly gathering data in small increments, why not just take the motherlode? Instead of trying to hold cars for ransom one by one, take over an entire car dealer's worth of cars through their maintenance systems. Credentials and authentications systems are again the weak points. Of course, most IoT device aggregation points will be in the cloud, so cloud vulnerabilities and threats apply, too.

Ransomware will attack Internet-enabled medical devices.
We do not yet know why attackers are breaching medical devices that collect patient information, but it is happening and medical data is being exfiltrated. That is likely to continue for the next two to four years, and we will also learn why they are stealing medical data. More ominously, medical devices that monitor and control human systems—including pacemakers, insulin pumps, and nerve stimulators—are all becoming Internet enabled. Unethical attackers will see these medical devices as the next step in their journey beyond hospital ransomware attacks. Hospitals are successful ransomware targets partly because they need immediate access to information. A pacemaker is an ultimate example of the need for immediate access, so attackers will attempt to find vulnerabilities in these devices as they become Internet enabled and will be able to extort a great deal of money if they are successful.

Laws and borders

IoT threats and breaches will prompt political and regulatory responses. The speed of technology advancement will hinder effective legislation, and vice versa. Differing and even contradictory regulations among countries will make things more difficult for consumers, device manufacturers, and service providers.

Honor among thieves?
After a recent ransomware attack on a California hospital, some members of the hacker community belittled the attackers as the "dumbest hackers ever, like they couldn't hack anything else," and "if someone were to die or be injured because of this it is just plain wrong." As unlikely as it sounds, hackers usually have some degree of compassion. As financially appealing as some IoT attacks appear, the potential to cause injury or death will make some of them think carefully about their actions and limit the number and severity of attacks.

Laws will lag behind IoT device technology and its adoption, giving rise to litigation.
The inability of laws to keep pace with technology changes is well known. The benefits of IoT devices and systems—whether to improve health care outcomes, manufacturing efficiency, the home, or a host of other possibilities—will drive adoption despite security and privacy concerns. As a result, we will see incidents that provoke litigation, protests, and consumer outrage. Legislation will vary widely by country because of cultural norms and the speed of legislative action. Writing laws will be a big challenge for lawmakers due to competing and conflicting interests. Some jurisdictions, such as the European Union, will likely be leaders in this area, and others will watch and wait as long as they can.

Privacy will be the primary focus of legislation related to consumer-oriented IoT devices, services, and the data they collect. Responses will be influenced by cultural norms and navigating those differences will be a challenge for companies.

Laws and cultural differences concerning privacy will be wildly divergent from jurisdiction to jurisdiction.
Privacy will be the primary focus of legislation related to consumer-oriented IoT devices, services, and the data they collect. This emphasis will largely be driven by consumer pressure and will intensify after a few major data thefts. Responses will be considerably influenced by cultural norms, and significantly different by country, by industry, or other subsets. Navigating these differences will be a sizable challenge for companies, and will cause some to delay or even avoid participating in some markets.

IoT device security will become an important buying criterion for businesses. Privacy will become a more important buying criterion for consumers.
Two separate but related points will produce some conflict within the IoT device and security industries. Businesses will consider the security of IoT devices and systems to be a top purchase criterion. This will drive features such as device attestation, data encryption, trusted updates, hardware-based security, and trusted execution environments. Consumers will increasingly consider privacy when purchasing an IoT device, but will continue to err on the side of convenience. This view will encourage improved encryption, and it may drive features such as device anonymity and direct or indirect compensation for allowing personal data to be collected and used.

Vendor responses

Threats, breaches, and legislation will prompt technology and service responses from IoT device manufacturers, service providers, and security vendors. Device security and privacy will be enhanced, user identity protections developed, hardware-based defenses extended, and insurance will evolve to cover IoT implementations. The following are our top seven expectations of responses to IoT threats during the next two to four years.

If you are not paying for the product, you are the product.
Consumers are gradually coming to realize that their data on IoT devices such as smartphones has a value and they should be compensated for sharing it. Free products and services that generate revenue through data collection or targeted advertising will become much more explicit about this in the next two to four years. Some will offer paid options that do not collect data, while others will pay the consumer varying amounts based on how much they collect. All of this will require IoT devices and system developers to build in security and privacy.

New and improved encryption options.
In a corollary to the previous prediction, the ability to secure IoT device–generated data in transit, from its origin to its destination, will become extremely important to prevent man-in-the-middle attacks. Whether remote cameras, payment card readers, location tracking devices, or manufacturing monitoring systems, capturing IoT-generated data midstream is currently too easy. Vendors will respond with more encryption options and larger keys to improve security, and hardware assistance to minimize the performance impact. We will see these options within the next four years.

Hardware-based privacy and security will be built into some IoT device hardware.
Whether because of their form factors, high volumes, or lack of human interaction, IoT devices are more difficult to protect in software than traditional IT devices. As a result, hardware-based security is going to be much more important. For example, trusted execution environments, which allow only specified processes to run and access data, already exist in some processors; IoT device developers will begin to use them. Within two to four years, IoT device manufacturers will promote this product feature, and we will even see the beginnings of partitioned or trusted apps available for devices through their app markets. The more security is built into IoT device hardware, the better chance there is to provide a solid foundation for good security and privacy.

Security vendors will introduce and support industry standards to protect IoT device identity.
One approach to enhancing privacy is ensuring that service providers never know IoT device identities. Authentication and verification of device identity can be abstracted and provided by a third party, which then provides confirmation to the service provider that an IoT device is a member of a trusted group. An interesting possibility is the use of blockchain technology, similar to what Bitcoin uses, to provide transaction anonymity so that it cannot be linked to a particular IoT device or account. Data could still be collected and sold, but as an aggregated set and not personally identifiable. We expect this to move quickly from proprietary techniques to industry standards within four years.

Control systems will be developed to manage and secure IoT devices automatically and in aggregate.

IoT device control systems will emerge to integrate and secure the huge number of IoT devices expected to come online by 2020.
The high volume and sometimes limited capabilities of IoT devices make it impossible to manage and secure them the way we secure traditional IT systems. As a result, control systems will be developed to manage and secure IoT devices automatically and in aggregate. Key capabilities will include autonomous device authentication and verification, IoT device software and update management, and privacy and security policy managements. Because it will be difficult to quickly update all devices in the field, additional security defenses will be required to protect them from zero-day exploits.

Behavioral monitoring of IoT devices will emerge.
One protection technique that will emerge within the next two to four years is behavioral monitoring to detect and act when IoT devices perform unusual or unauthorized actions. This will be especially important as a defense against zero-day exploits and credential theft, which can evade traditional security precautions. When unusual activity is detected on an IoT device or its controller, whether it is based on time of day (why is this activity being requested at 2 am?), the context of other IoT devices (why is this valve open when the related process is not running?), or a blacklist (my car's brakes should never be disabled remotely), it can block the command, take immediate action to mitigate the threat, or prompt a human for instructions.

Cyber insurance and risk management for IoT system implementations will grow.
Vulnerabilities in IoT devices and systems exacerbate risk. While companies and consumers will still adopt IoT devices because of their benefits, businesses will look to manage the risk. Insurance offerings will emerge for this purpose. This will require businesses and insurance companies to define and monitor minimum operating requirements, in concert with the evolving legal and regulatory landscape. Due to the potential damage of a successful IoT attack, insurance policies will become an integral part of IoT system planning.

Conclusion

With billions of IoT devices coming online during the next several years, the threat of cyberattacks is very real. However, it will take a while for criminals to figure out how to monetize attacks, so the number of successful attacks against these devices will likely remain small.

IoT adoption will greatly increase the attack surface. Weak security and rookie mistakes by IoT device manufacturers will compound that problem. Some of these vulnerabilities will be exploited as initial attack vectors into control, surveillance, and information systems. Ransomware will be the most likely near-term threat. Aggregation points, where data from IoT devices is collected, will also be a prime near-term target.

Loss of consumer privacy and legislative responses to citizens concerns will capture headlines. However, the conveniences and efficiencies made possible by IoT devices will outweigh their disadvantages, so adoption rates will remain high. Regulations will vary widely by jurisdiction, they will lag the market, and litigation will play a significant role in shaping the IoT market's direction.

Vendors will develop a wide array of responses to encourage and support market adoption. New encryption options, security and privacy embedded in silicon, device control systems to automatically manage and secure IoT devices, and behavioral monitoring of IoT devices will rapidly come online and evolve.

An important change will be a better understanding of the intrinsic value of personal data. Consumers will expect options for sharing personal data collected by IoT devices, including compensation.

2017 Predictions

Share feedback

2017 Predictions

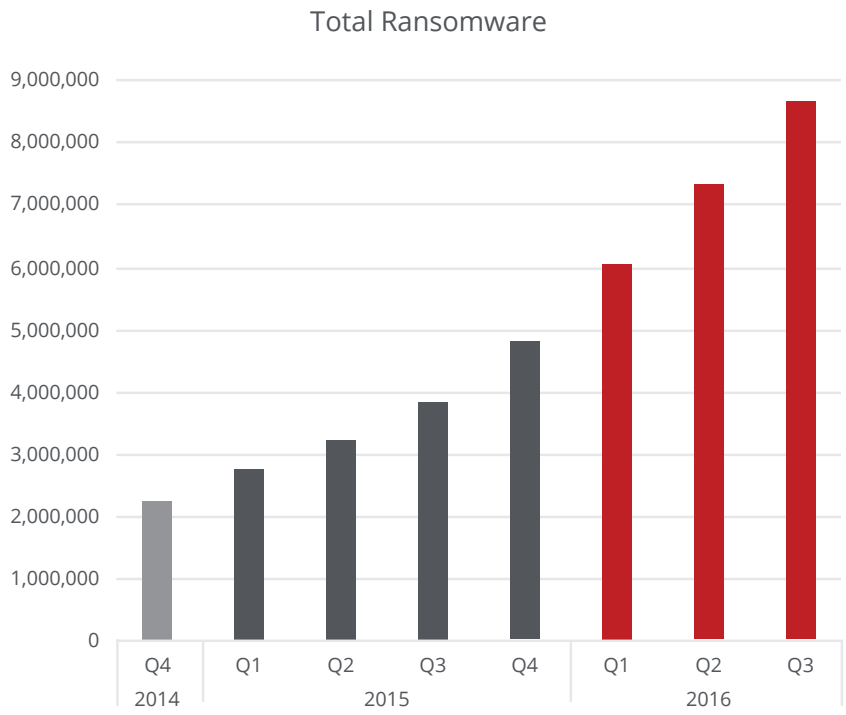
Ransomware subsides in the second half of 2017

—Christiaan Beek

We predict that the volume and effectiveness of ransomware attacks will go down in the second half of 2017.

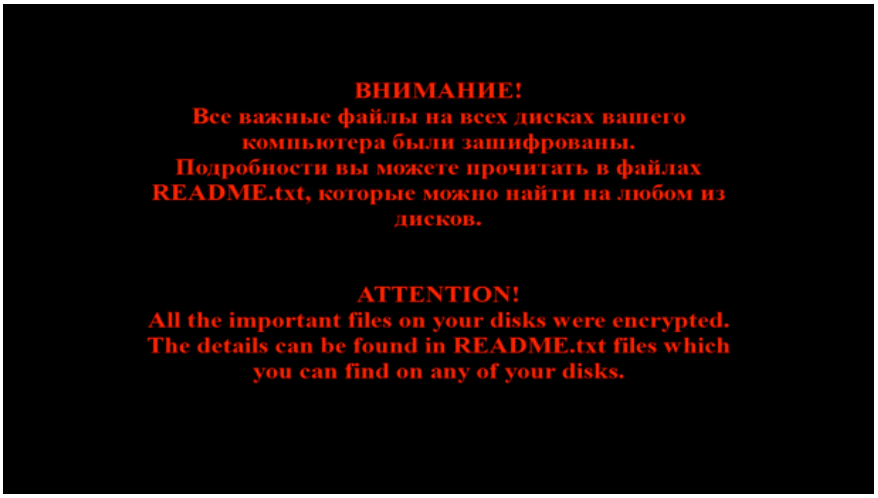
Ransomware will remain a very significant threat until the second half of 2017. Ransomware-as-a-service, custom ransomware for sale in dark markets, and creative derivatives from open-source ransomware code will keep the security industry busy through the first half of the year. Ransomware's impact across all sectors and geographies will force the security industry to take decisive actions. We predict that initiatives like the No More Ransom! collaboration, the development and release of antiransomware technologies, and continued law enforcement actions will reduce the volume and effectiveness of ransomware attacks by the end of 2017.

The concept of ransomware was first demonstrated in the early 1990s. When Bitcoin was introduced and used for the first time by the CryptoLocker ransomware family in 2013, it opened the door to anonymous ransom payments, shielding attackers from being caught. The "pioneer" creators of ransomware such as CryptoLocker and CryptoWall came from the world of banking Trojans and were very experienced in how to run a successful cybercrime operation. They quickly learned important lessons and have been able to rapidly adapt and change either their infrastructure or code as soon as business slows. These are the groups that will continue in the ransomware business and seek new ways to make profits. Currently, we face many smaller, less sophisticated groups who are attracted by the revenue generated by the organized groups. As discussed in the Cyber Threat Alliance's *CryptoWall Version 3 Threat report*, revenue from a single ransomware family can exceed $325 million. Such examples have led to a massive increase in ransomware families and attacks, as we have discussed many times. Individual criminals want to tap this gusher, too, and either sign up as affiliates or build upon public code. We expect these small initiatives will decrease in 2017 as the security industry and international law enforcement join forces to actively detect and respond to these cases.



Source: McAfee Labs, 2016.

Further, the security industry has started developing tools and functionality to assist companies when battling ransomware. During Black Hat USA 2016, McAfee's advanced threat research team demoed ransomware proof-of-concepts aimed at IoT devices, including one that targets an automobile's in-vehicle "infotainment" system, allowing the ransomware to control the car's brakes and starter until the ransom is paid. The advanced threat research team is focused on the future of threats and industry cooperation to create awareness and mitigate these ransomware threats at an early stage.



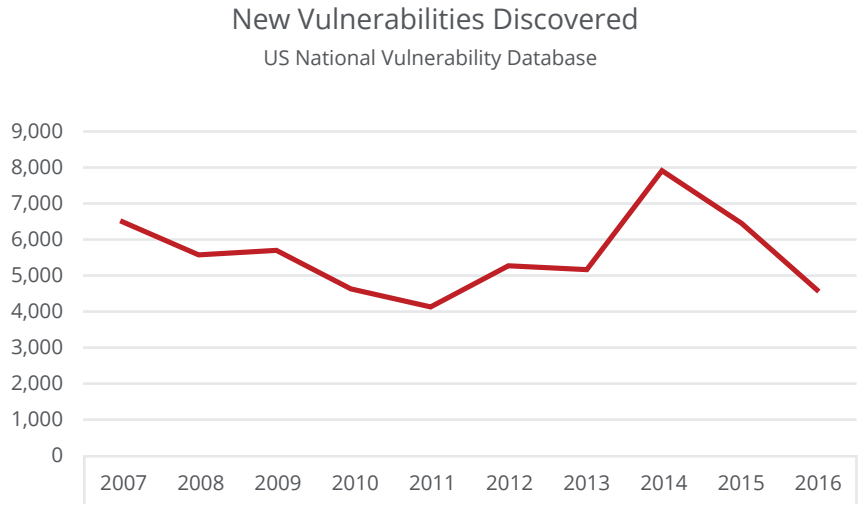
A Bitcoin mixer: Breaks the connection between a Bitcoin address sending coins and the addresses they are sent to.

What about virtual currencies, which opened the gate to ransomware growth? Will Bitcoin survive or will ransomware actors move away from it and seek new payment methods? Even the use of Bitcoin mixers is not enough to block the analysis of transaction links. Also, other Bitcoin services have been criticized at the Bitcoinference by attendees who complained about nonmixing by some services and unsecure usage of supernodes that could expose identities. As a result, we predict that there will be a shift in ransom payment methods toward virtual currencies such as Monero and Zerocoin/Zerocash.

Vulnerability exploits on Windows cool down as other platforms heat up

—Bing Sun, Haifei Li, Stanley Zhu, and Debasish Mandal

Exploiting client-side software vulnerabilities has become significantly more difficult in recent years, thereby increasing the development cost of generic and reliable exploits. To successfully penetrate the latest operating systems (for example, a fully patched Microsoft Edge browser running on the 64-bit Windows 10 operating system), attackers must often combine several high-quality vulnerabilities with advanced exploitation techniques. Although successful attacks have been demonstrated in hacking contests (such as Pwn2Own 2016), we have not yet seen sophisticated exploits such as these in the wild. We suspect these exploits are available only to a handful of people and will appear only in very significant advanced attacks.



2016 data through September 20.

We believe that vulnerability exploits in Windows and Flash will continue to decline but those targeting infrastructure software and virtualization software will increase.

Looking back at the *McAfee Labs 2016 Threats Predictions* report, many of our vulnerability exploit predictions came true. Based on our observations this year, we will aim for the same success rate in foreseeing vulnerabilities in 2017.

- **Adobe Flash:** This is still the primary target of in-the-wild attacks based on vulnerabilities. Flash zero-day vulnerabilities, such as CVE-2016-4117 and CVE-2016-1019, accounted for about 50% of all zero-day attacks discovered by security companies in 2016. In 2015, we predicted that the popularity of Flash exploitation would cool down in 2016 due to a critical mitigation feature (vector length cookie check) introduced in July 2015 that stops many Flash exploits. As a result, in-the-wild Flash exploits in 2016 did drop significantly (only four as of this writing, compared with 11 in 2015). One new Flash exploit (the use of ByteArray and BitmapData) emerged (CVE-2015-7645) soon after vector mitigation was added. Adobe continues to add new mitigations to Flash, such as ByteArray length cookie check, isolated heap, system heap, and memory protector. Although none of these new features is perfect (some introduced new problems), in general they make exploitation more difficult. Therefore, we believe Flash as an attack vector will continue to decline in 2017. Finding vulnerabilities in Flash is getting harder, while exploiting vulnerabilities will be even more difficult.
- **Microsoft Internet Explorer and Edge:** As we stated in the 2016 Threats Predictions report, attacks targeting IE and Edge continue to be minimal. So far this year, there has been no genuine IE zero-day exploit observed in the wild. Although the exploits CVE-2016-0189 and CVE-2016-0034 are delivered and executed from a browser, they are actually vulnerabilities of the Script Engine and the .Net framework, respectively. With a reduced attack surface (no document mode, no Visual Basic Script, no browser helper object and ActiveX, no Silverlight, etc.) and enhanced mitigation, Edge is an even more secure browser. Since its release, we are not aware of any zero-day exploit in the wild targeting Edge. In general Microsoft's browser mitigations appear to be very effective. Some mitigations helped eliminate certain vulnerability classes (for example, use-after-free flaws decreased drastically since the introduction of isolated heap and memory protection), while others made vulnerability exploitation much harder. Control Flow Guard is one more critical mitigation feature that prevents exploits from hijacking the program's execution flow. We predict that IE and Edge exploitation will become more and more difficult in 2017, especially on 64-bit platforms, where creating and controlling specific memory layouts will be extremely challenging.
- **Java, PDF, and Microsoft Office:** There have been few changes to attacks on Java, PDF, and Office apps in 2016. We once thought that Office vulnerability exploits would increase substantially, considering its huge attack surface and complexity of code. However, this has not happened. Perhaps that is because Office lacks scripting language support, making it more difficult to develop exploits. On the other hand, we do expect to see other types of Office-based threats, such as macro-based ransomware, becoming prevalent in 2017.

- **Windows kernel:** Although some mitigations (supervisor mode execution protection, Win32k system call filtering, kernel address space layout randomization improvements, font parsing moved to user mode) have been put in place, the prevalence of kernel-mode exploits continues to be significant. Moreover, they are often the best weapons to defeat application sandboxes (such as AppContainer) and achieve privilege escalation. These have been well demonstrated in zero-day attacks (CVE-2016-0165/0167) and hacking contests (CVE-2016-0176). Considering the large attack surface and weaker protection and mitigation offered in kernel space compared with user space, we predict that kernel-mode exploitation will continue to be hot in 2017.
- **Infrastructure software:** Attacks on infrastructure vulnerabilities will be very active in 2017. Looking at the advisory list for OpenSSL, we see many vulnerabilities patched with every release. Apart from OpenSSL, we also find critical vulnerabilities in other open-source software, such as CVE-2015-7547 (a stack-based buffer overflow in the glibc DNS client) and CVE-2016-5696 (a Linux flaw that allows the hijacking of Internet traffic).
- **Legacy components vs. new features:** Although most malware authors focus on new features such as the Windows Subsystem for Linux, which has 216 new system calls and 700KB of code, others have turned to legacy components. Since the critical vulnerability GHOST (CVE-2015-0234), which existed in glibc for more than 15 years, was discovered last year, security researchers have begun reexamining legacy code. In 2016, for example, a serious bug (BadTunnel) was discovered in the Web Proxy Autodiscovery Protocol. The bug has been in the code for 20 years. Because the security of important legacy components has been neglected for years, security researchers are working to eliminate long-standing vulnerabilities. We expect to see more issues found and fixed in 2017.
- **Virtualization software:** With the continuing rapid adoption of cloud technology, virtualization security is a hot topic that has attracted the attention of security researchers and attackers. Many in-depth research results have become public. In July, a critical vulnerability was patched in the Xen hypervisor that allows a "Guest to Host Escape" (the "Po Tian" vulnerability, CVE-2015-7835). In September, McAfee's advanced threat research team discovered the Xen vulnerability XSA 188, which resulted in the Linode cloud-hosting service rebooting their Xen-based servers. Critical bugs in VMware were documented as well, including CVE-2016-5332, CVE-2016-2077, and CVE-2016-2079. Microsoft Hyper-V is not immune: We saw several CVEs related to Hyper-V (MS16-045 and MS16-046). Moreover, Microsoft's Virtualization Based Security/Virtual Secure Mode in Windows 10 is also a new target; some of its security issues have been found and publicized. On the other hand, although many vulnerabilities have been discovered in virtualization software, when compared to mature browser exploitations virtual machine (VM) attacks still lack systematic and universal exploitation techniques and methodologies that can generically cover certain classes of VM security issues. Most VM escape cases are highly dependent on the vulnerabilities themselves, such as CVE-2015-7835, CVE-2016-3710, and CVE-2015-7504. Because VMs have become targets for attackers, we believe

it is just a matter of time until we see systematic exploits and sophisticated attacks against virtualization software. 2017 could be the year that happens.

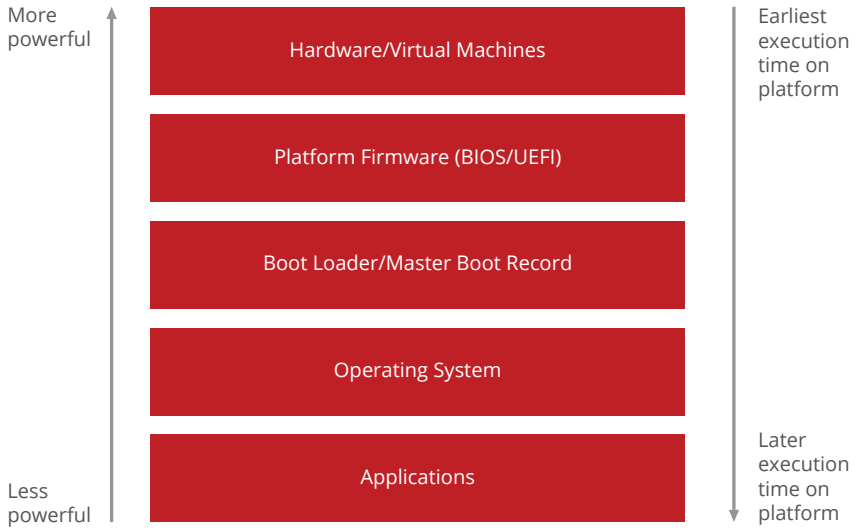
- **Security products:** In 2016, we have seen many serious vulnerabilities in security products. Early in the year, Google researchers found a severe remote code execution vulnerability in FireEye appliances. Then, Google researchers discovered vulnerabilities in products from most major antimalware vendors. And in the summer, the leaked Equation Group data exposed many exploits (including several unpatched zero-day vulnerabilities) targeting various firewall products. This trend will no doubt continue in 2017.

Hardware and firmware threats an increasing target for sophisticated attackers

—Yuriy Bulygin

Software, including operating systems and applications, implicitly rely on hardware to operate correctly. Hardware vulnerabilities can undermine the operation and security of the entire software stack. Exploiting a hardware vulnerability can compromise an entire system and does not require an exploit of the software stack. Further, systems whose hardware is successfully attacked can be difficult to patch without replacing vulnerable hardware. Finally, none of the systems' software-based security mechanisms and protections can be relied upon because they assume the hardware has not been compromised.

There are mitigating factors, though. Hardware is less exposed to attacks than software stacks, and attacking hardware almost always involves exploiting some sort of hardware logic vulnerability rather than the many software vulnerabilities commonly found in software stacks. Hardware's reduced attack surface raises the complexity of attacks. As a result, we see very few vulnerabilities in hardware and incidents in which hardware is either targeted or successfully exploited by attackers. Similarly, common malware almost never targets hardware.



Security researchers have uncovered a few hardware vulnerabilities during the last several years—including vulnerabilities in microprocessors and DRAM technology [1, 2, 3, 4] and vulnerabilities that enable operating system–independent side-channel attacks [1, 2, 3], which might impact cloud environments by exposing co-located virtual machines [1, 2, 3, 4].

Computer systems often have specialized software and hardware that initializes, boots, and performs low-level maintenance tasks on the system. This specialized software and hardware has its own microcontroller and software stack, often referred to as firmware. The BIOS, unified extensible firmware interface (UEFI), EFI, and Coreboot are examples of this specialized firmware. In addition, external devices such as USB, hard and solid state drives, expansion cards, and even power chargers often have their own firmware.

Firmware has properties that make it a significant attack target. It is often stored persistently on nonvolatile storage such as flash memory devices, it has full access to the hardware it manages, and it is mostly well hidden from operating systems and security software. System firmware runs before the operating system takes control. In addition, firmware is just software so it often has similar vulnerabilities but with fewer built-in protections and exploit mitigations.

Threats researchers have demonstrated that vulnerabilities in system firmware [1, 2, 3] can enable attacks on preboot authentication, including attacks on systems with full-disk encryption based on the Trusted Platform Module (for example, Microsoft Windows BitLocker [1, 2]) or Windows Secure Boot [1, 2, 3, 4]. Preboot attacks allow the installation of stealthy and persistent rootkits, backdoors, or worms [1, 2, 3, 4, 5], and break trusted execution environments based on virtualization technology such as Secure Kernel and Isolated User-Mode with Credential Guard and Device Guard, in Microsoft Windows 10 [1, 2].

Besides system firmware, security researchers have identified firmware vulnerabilities in USB devices [1, 2, 3], network cards [1, 2], embedded and keyboard controllers [1], baseboard management controllers [1, 2, 3], LTE/3G/GSM baseband modems [1, 2], CPUs [1, 2], batteries [1], home routers [1, 2, 3, 4], office printers [1, 2], IP phones [1], firmware and secure software for ARM TrustZone [1, 2, 3, 4, 5], and many others.

Adversaries such as nation-state–sponsored hacking groups, industrial espionage teams, and organized crime groups are interested in attacking system firmware. Two years ago, the Equation Group targeted firmware on hard drives [1]. In 2015, we saw the first commercial UEFI firmware rootkit from the Hacking Team [1]. Most recently, a dump by the Shadow Brokers revealed that the organization believed to be linked to the Equation Group targeted firmware on network firewalls with persistent implants [1, 2].

Hardware and firmware are complex targets, but successful attacks on them offer adversaries ultimate persistence, significant stealth, access to a great variety of hardware resources, and the ability to implant backdoors into systems' software stacks. We predict in 2017 that advanced adversaries such as nation-state attackers will continue to look for vulnerabilities in hardware and firmware that they can exploit. We believe that advanced adversaries possess the ability to exploit systems whose firmware is based on legacy BIOS or (U)EFI as well as firmware on other types of devices such as solid-state drives, network cards, and Wi-Fi devices.

We predict in 2017 that advanced adversaries will continue to look for vulnerabilities in hardware and firmware that they can exploit. We believe that they possess the ability to exploit systems whose firmware is based on legacy BIOS or (U)EFI as well as firmware on other types of devices such as solid-state drives, network cards, and Wi-Fi devices. Some of these advanced exploits will likely appear in common malware attacks.

Some of these advanced exploits will likely appear in common malware attacks. In 2017, we will see malware using bootkit components that attack UEFI-based operating system boot loaders or even install firmware rootkit components; firmware attacks that compromise virtualization-based trusted execution environments such as VBS in Windows 10; and ransomware infecting early stages of operating system boots, including boot loaders and firmware.

On the defensive side, we will likely see more commercial security technology that provides visibility into the firmware and other low-level system components beyond that provided by traditional software stacks.

"Dronejacking" places threats in the sky

—Bruce Snell

Drones continue to become more and more mainstream. What started as a fun toy for kids and a slightly expensive hobby for enthusiasts has really taken off, if you'll forgive the pun. Drones are well on the way to becoming a major tool for shippers, law enforcement agencies, photographers, farmers, the news media, and more. It is hard to deny that drones have become a lot more valuable to many types of businesses and government agencies. Recently, we saw an example of a drone outfitted with a full hacking suite that would allow it to land on the roof of a home, business, or critical infrastructure facility and attempt to hack into the local wireless network.

In 2015, a proof of concept hack was demonstrated at DefCon that showed how someone could easily take control of a toy drone. Although taking over a kid's drone may seem amusing and not that big of an issue, once we look at the increase in drone usage potential problems starts to arise.

- **Deliveries:** Both Amazon and UPS have announced plans to deliver packages via drones. This creates a realistic target for a criminal looking to make a quick buck. Shipping drones will most likely be launched from a dedicated location, making traffic patterns easy to spot. Someone looking to "dronejack" deliveries could find a location with regular drone traffic and wait for the targets to appear. Once a package delivery drone is overhead, the drone could be sent to the ground, allowing the criminal to steal the package. To be fair, such thefts would be hit or miss as there would not be an easy way to know what is in the package, but it could turn out to be lucrative.
- **Camera crews:** Aerial photography is now much easier with the advent of drones. A quick search for "photography drone" returns pages of results pointing to high-quality and expensive equipment for both amateur and professional cinematographers. This high-quality equipment would be a very tempting target for a criminal to dronejack. Pulling down a drone would allow criminals to resell the equipment, effectively making money fall from the sky.
- **Personal no-fly zones:** There have been a few incidents in which people became annoyed with drones over their houses and took active measures (shotguns, throwing rocks, etc.) to deal with them. Exploiting software vulnerabilities in drones could allow someone to set up an electronic barrier around a house that either kills or redirects drones that fly too close. Although this may seem like a boon to those who prefer the "get off my lawn" approach to neighborhood life, drones are still a gray area in many local

regulations and ordinances. This gray area could lead to heated debate and potential lawsuits over someone creating a personal no-fly zone.

- **Law enforcement:** More and more law enforcement agencies are turning to drones to assist in surveillance and crowd control. In a highly charged situation like a protest or active shooter situation, a police drone would be a tempting target for someone looking to remain unseen by law enforcement. This scene has played out countless times in action movies. The bad guys (or heroes) go through elaborate measures to take out the security feeds of their target. Now, instead of wall-mounted security cameras, we have cameras attached to drones. As protestors and hacktivists start to mix more, the odds of a protester with the technology to knock out surveillance drones dramatically increases.

How will these attacks take place? Various researchers have found many consumer drones shipping with open ports and weak authentication methods, allowing a person with the right equipment to send commands to the victim's drone. So far, this has been a fairly manual process but, as we've seen in the past, new exploits typically appear sooner or later in easily reproducible format.

The majority of the vulnerabilities discovered on commercial drones can be easily fixed with a software update. Of course, this requires the manufacturer to release a patch. While high-end drones will most likely be patched quickly, cheap drones will most likely fly a long time before a patch is available. As we have seen with other IoT technology, once a device is connected to a network, people quickly start looking for ways to hack it. This effort is made easier by the general rush to market for IoT devices, including drones, that have little or no security. What makes drones potentially easier to hack is they are designed to have a quick and easy setup, often using unencrypted communication and many open ports.

In 2017 we will see a drone taken out of the sky by software running on a laptop with a directional antenna. We will also see more drones used by law enforcement agencies to monitor crowds, Drone takedown hacks will be launched by protesters as a way to quickly remove surveillance drones from the equation.

We predict in 2017 that drone exploit toolkits will find their ways to the dark corners of the Internet. Once these toolkits start making the rounds, it is just a matter of time before we see stories of hijacked drones showing up in the evening news. Even without a dronejacking toolkit in hand, we will begin to see an increase in drone-related incidents.

In 2017 we will see a local news report about a person getting fed up with one of the neighborhood kids flying a drone over his back yard. But instead of using a shotgun loaded with birdshot, the drone will be taken out of the sky by software running on a laptop with a directional antenna. Given the viral nature of the Internet, this will soon show up on Facebook walls all over the world with arguments for and against the action, causing heated debates and snarky memes.

During 2017, we will also see more drones used by law enforcement agencies to monitor crowds. Initially protesters will react by throwing objects at police drones, but drone takedown hacks will be launched by protesters as a way to quickly remove surveillance drones from the equation.

How will policymakers respond to these incidents? Already the US Federal Aviation Administration is scrambling to put rules into effect that govern when and where commercial drones can fly, but there are still a lot of uses that need to be addressed and surely some we have not yet thought of. Whereas commercial aviation grew slowly over time, commercial drone usage is on a steep flight path that will leave regulators struggling to get off the ground.

Mobile threats to include ransomware, RATs, compromised app markets

—Fernando Ruiz

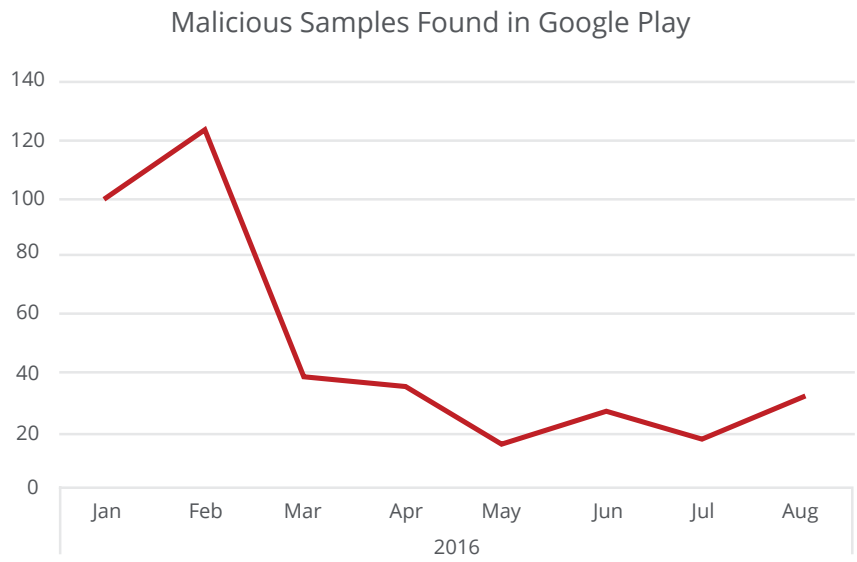
McAfee Labs sees mobile malware continuing its growth in 2017, with ransomware, banking Trojans, and remote access tools among the leading threats.

In 2017, we expect that mobile ransomware will continue to grow but the focus of mobile malware authors will change. Attackers will combine mobile device locks with other forms of attack such as credential theft, allowing them to access such things as banks accounts and credit cards.

The Mobile Malware Research team of McAfee Labs has cataloged a large number of ransomware samples for mobile devices, especially in Q2 and Q3 of 2016. The samples range from small proofs of concept that lock screens to full-scale crypto malware that compromises external memory. One mobile ransomware family prominent in Q2 and Q3 was Android/Jisut. This ransomware changes a mobile device's lock PIN and demands payment via Bitcoins or prepaid card.

In 2017, we expect that mobile ransomware will continue to grow but the focus of mobile malware authors will change. Because mobile devices are usually backed up to the cloud, the success of direct ransom payments to unlock devices is often limited. Because of that, mobile malware authors will combine mobile device locks with other forms of attack such as credential theft. For example, we have observed this year how families such as Android/Svpeng, identified by the security industry as mobile ransomware, are now mutating to target banking credentials, looking to steal money from victims' accounts. We believe in 2017 banking Trojans will reappear and they will come from ransomware authors. This malware will combine mobile device locks and other ransomware features with traditional man-in-the-middle attacks to steal primary and secondary authentication factors, allowing attackers to access banks accounts and credit cards.

We saw a proliferation of remote access tools (RATs) for Android in 2016. They masqueraded as legitimate support utilities and were offered on third-party markets. These RATs are used to spy on Pokémon Go enthusiasts, terrorist sympathizers, and security personnel, and use social networks as their distribution channel. Due the growth in and sophistication of commercial spyware and RATs, we expect that more victims will be indiscriminately targeted by this type of malware in 2017. Vulnerable smartphones are a perfect spying platform that can be controlled by anyone who knows the methods of compromise.



Although we and other sources recommend downloading apps only from trusted apps markets, this step has been proved insufficient to keep all users safe. Several times in 2016 malicious apps appeared on Google Play, even though they were quickly removed. We urge users in 2017 to raise their awareness of app reviews—before installing apps even from trusted markets. This awareness, combined with an effective antimalware app, is essential to prevent infections in smartphones.

Downloading apps from unknown and untrusted markets has always been more dangerous; that will not change in 2017. This danger includes linking to apps whose URLs appear on Instagram, YouTube videos, or Tweets. All can distribute malware or spyware. Using popular social media can lead to infections because familiar environments can lure users into overlooking security risks.

IoT malware opens a backdoor into the home

—Bruce Snell

Consumer electronics continues to grow at a rapid pace. One area in particular is the consumer element of the Internet of Things, which is expected to hit roughly 1.8 billion devices by 2019. Known colloquially as "smart home" or "connected home," this market includes a number of well established brands and products, as well as a huge field of smaller companies looking to break into the scene.

In business, we have the concept "minimum viable product," or MVP. Although the acronym commonly means "most valuable player," in this instance MVP means having the minimum number of features to make a product functional enough so that early adopters want to purchase it. The home IoT market is very "sticky," in that once someone buys a smart thermostat or smart lighting system, they probably will not replace it. Because of this, the rush to market is fast and furious, and home IoT device makers generally employ the MVP approach. Many, for example, rely on third-party code libraries to shorten the development process and reduce costs.

This haste and reliance on third-party software is where potential security threats can arise. Good coding practices dictate that developers should perform thorough code review of any third-party code libraries included in their products. Unfortunately, when rushing to create and ship an MVP to beat competitors to the shelf, code is often thrown together with minimal testing, relying on after-release patches to correct bugs that show up. When developers are pressed for time, security is often left on the back burner. That is if security is even thought of. We have seen a number of consumer IoT products shipped with gaping security holes that have gone unpatched for years.

We will see malicious code hiding in widely used libraries or directly embedded in devices used in the consumer IoT space. The code will hide in such things as HTML rendering libraries, network libraries, and camera libraries.

Let's take the scenario a step further. If a cybercriminal wants a pathway into a wide array of products that will sit on home networks with minimal security, planting a backdoor in consumer IoT devices would be an excellent way to do it. One good example of this occurred a couple of years ago when a Samsung-clone smartphone, the Star N9500, was sold in major online marketplaces with malware installed in the phone's firmware.

Instead of targeting a specific manufacturer and attempting to breach their code base, it is easier to create a "free" version of a widely used code library containing the backdoor and offer it to many IoT device manufacturers. We've seen malicious code in widely used code libraries on the Android side, so it is not a stretch of the imagination to see this play out with IoT devices.

Within the next 12 to 18 months, we will see malicious code hiding in widely used libraries or directly embedded in devices used in the consumer IoT space. We might also see some form of app collusion between consumer IoT devices and smartphone apps.

Where will we see malicious code in 2017? Part of the beauty of a code library from an attacker's perspective is that it often has direct access to key components of the operating system or device hardware. With that in mind, we expect to see malicious code hiding in these places:

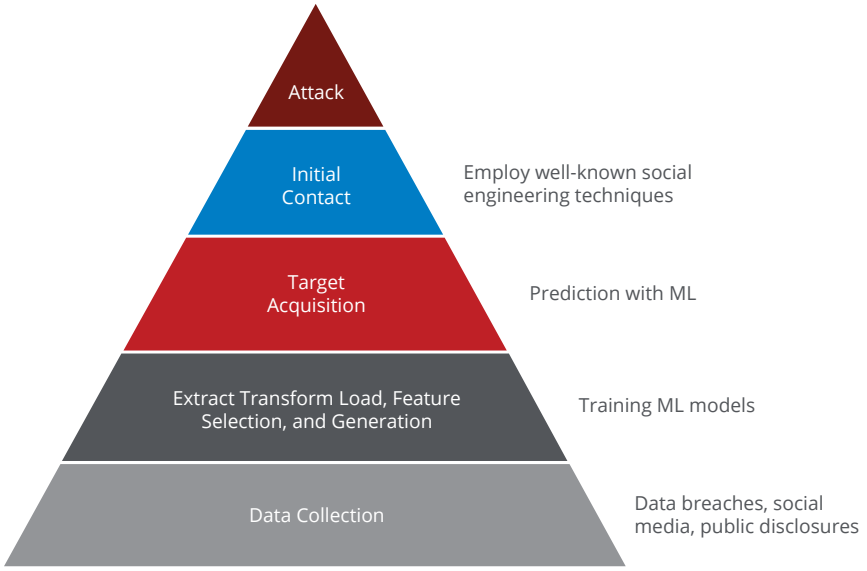
- **HTML rendering libraries:** Some IoT devices have management interfaces that are simply web pages used for configuration. It makes sense to hide malicious code in a library that has direct access to these web pages as they are rendered. Doing so allows the malware to collect usernames and passwords and serve malware in the management interface itself. No one suspects an infection while managing the home's smart lights!
- **Network libraries:** We often think of our home networks as safe. When malware gets a foothold in a home network, it is often able to sniff all of the network's traffic, as home networks are generally very flat and open. The malware sniffs for things such as usernames and passwords and sends those to a control server elsewhere. Because the malware has direct access to the network, this behavior typically goes unnoticed.
- **Camera libraries:** Is there a better way to spy on an unsuspecting person than to tie into the camera in a nursery or home security system? Hiding in security cameras allows the malware to capture and send pictures and videos of unsuspecting people going about their daily lives.

We predict that some home IoT devices shipped in 2017 will have backdoors installed. Due to the nature of these devices, spying and personal information theft may go unnoticed for years.

Machine learning accelerates social engineering attacks

—Eric Peterson

With an ever-increasing footprint in education, business, and research, the availability of machine learning toolkits, documentation, and tutorials has exploded in recent years. In as little as an hour, an individual can be training complex models on large datasets on a distributed architecture. In 2016, we have seen enthusiasts and professional data scientists teach machines how to write Shakespearean sonnets, compose music, paint like Picasso, and defeat professional Go player Lee Sedol. The learning period has become shorter, and accessibility for everyone, including cybercriminals, has never been better. Security is an arms race, and cybercriminals are fine-tuning their methods with the help of machine learning.



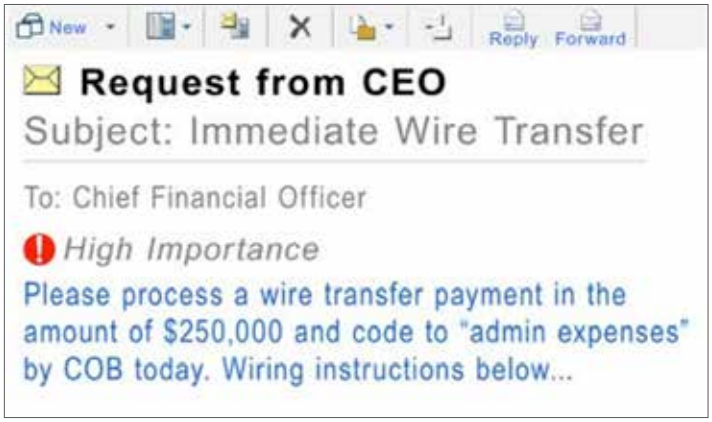
We believe that cybercriminals are leveraging machine learning to target victims. Tools to perform the complex analysis behind target selection are readily available, and there are a plethora of public sources of data required to build and train malicious machine learning algorithms. We expect that the accessibility of machine learning will accelerate and sharpen social engineering attacks in 2017.

One of several persistent threats we track today is the FBI-labeled Business Email Compromise (BEC) scam, which has been escalating since early 2015. With BEC scams, threat actors target individuals with financial responsibility within a business and, through skillful social engineering, dupe the individual into transferring funds into a fraudulent bank account. In some cases, the attacks have even coincided with business travel dates for executives, with the intent of increasing the odds of the scam's success. According to the FBI, more than $3 billion has been stolen, with victims in all 50 states and 100 countries. Although it remains unclear how victims are selected, it is clear that a considerable amount of research is conducted before the attacks are initiated. We believe that cybercriminals are leveraging machine learning to target victims for BEC and similar scams.

When expertly applied, machine learning has the potential to solve important, complex, tangible business problems. Regression algorithms can be used to predict values, clustering algorithms expose structure in datasets, and anomaly detection algorithms can be used to find abnormal data points. Under the hood, the mathematics behind these algorithms are advanced enough to be inaccessible to many. As we have seen with modern malware toolkits such as Trillium, Zeus, and Angler, malware authors can inflict far more damage with the assistance of toolkits than they could with their own individual skillsets. We see the same acceleration in the field of data science

through machine learning tools and libraries such as Google's TensorFlow, Numpy, Scikit-learn, Pandas, and others. Machine learning tools are force multipliers for those of us in security roles. We would be negligent to assume that cybercriminals are not also adopting these powerful tools.

One commonality between illegal and legitimate business models is the bottom line. From either perspective, organizations are constantly honing their craft, striving to increase output while decreasing input. With the BEC attack model as an example and the availability of machine learning tools to perform complex data analysis, we can begin to see the confluence of machine learning and criminal activity. The third leg in this attack tripod is data.



In 2016 alone, there have been breaches involving 30,000 US Department of Justice employees, 2.2 million patient records from 21st Century Oncology, 1.5 million Verizon Enterprise Solutions customer records, and nearly 150 million accounts with major email providers including Yahoo, Hotmail, and Gmail. The data from many of these breaches has been commoditized and sold in open markets, as is the case with leakedsource.com, which claims to have a little more than two billion records in their database. From another perspective, the US Securities and Exchange Commission's EDGAR service provides free access to more than 21 million filings. Between social media information, stolen data warehouses, and publicly disclosed business information, attackers have access to more than enough data to train predictive models to identify high-value targets.

Let us consider the lifecycle of a BEC scam as an example of an attack that can benefit from the use of machine learning. Cybercriminals know that sending a well-crafted email to a financially responsible team member, purporting to be from a leader of an organization and indicating urgency, results in a meaningful success rate in completing fraudulent transactions. A number of environmental factors leading up to the execution of the attack increase the probability of success. From the attacker's perspective, valuable insight can be gained from answering basic questions that may be available from the public domain: Are there indications of fracture within the organization? Have there been recent SEC filings in preparation for acquisition or divestiture? Are there correlations between social media posts indicating movement from multiple employees from one organization to another? Have there been strategic discussions sent to or from personal or private addresses? Responses to each of these types of questions can be represented as feature vectors for machine learning algorithms. With time and diligence, a model for successful execution of fraud can be developed and used to predict the success of future attacks.

Threat actors have developed a successful attack model with the BEC scam. Tools to perform the complex analysis behind target selection are readily available, and there are a plethora of public sources of data required to build and train malicious machine learning algorithms. Looking to 2017 and beyond, we might even see purveyors of data theft offering "Target Acquisition as a Service" built on machine learning algorithms. We expect that the accessibility of machine learning will accelerate and sharpen social engineering attacks in 2017.

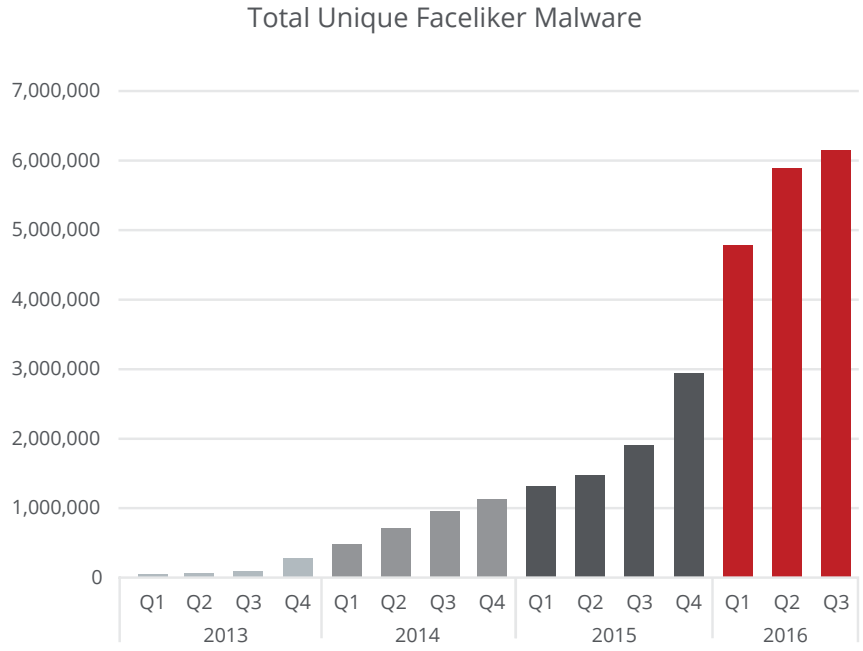
The explosion in fake ads and purchased "likes" erodes trust

—Craig Schmugar

Fake "Likes," advertisements, product and service reviews, online security warnings, alerts and more will make the Internet less trustworthy.

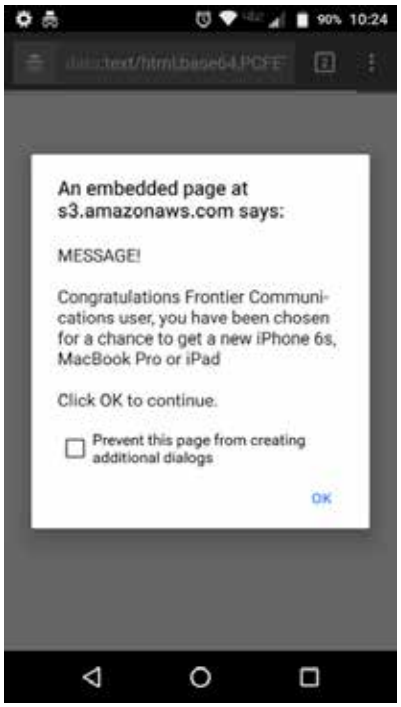
Every Internet user is bombarded with information for making decisions: what to click, what to read, and where to spend. These choices fuel a multibillion dollar online economy and, with that much money on the line, unscrupulous actors are constantly looking for ways to take advantage of others. Reputation is key for many decision makers to feel confident about their choices; this is the trust that some people seek to exploit.

One of the most popular methods to establish trust is through user feedback left by those who have gone before us. The value of a Facebook "like" has been estimated to be worth up to $200 or more. As a result, services have cropped up that offer to raise "like" counts for a fee. Although Facebook has cracked down on such entities, this is a cat-and-mouse game, and the latest round shows an investment by malware authors to keep the mice alive longer. Unlike a "click farm" that pays low-wage workers to click links, Faceliker malware piggybacks on user sessions so that the clicks are more likely to appear as legitimate.



Growth in Faceliker Trojan variants.

Fake advertisements are here to stay, too, with an increasing number of ad networks that take a user's browsing session hostage, whether to deliver malware, scams, or endless surveys. Although such items can be a nuisance when veering off the main path of the Internet, they are even more alarming when delivered through top-tier sites.



Ad hijacking delivered through a top website in Australia, with Amazon AWS serving the ad, which vibrates the phone.

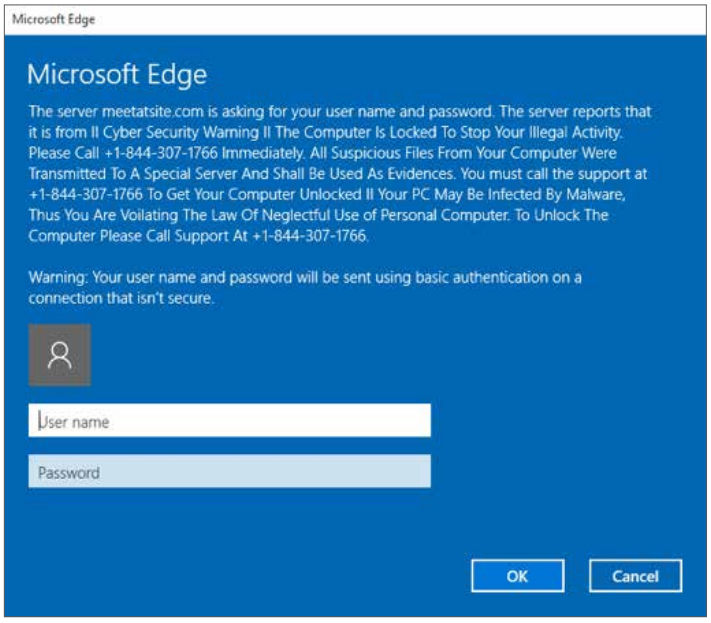
An unwanted page that makes it impossible for a user to reach the desired website.

We regularly find other occurrences of forged content in product reviews posted on top-tier ecommerce sites. Due to the breakneck pace of today's world, many consumers rely on the convenience of at-a-glance product and service endorsements. It is no surprise that sellers cannot resist the temptation to artificially bump up their ratings. Text, audio, and video reviews are readily available for purchase from people willing to create their own content or read from a script.

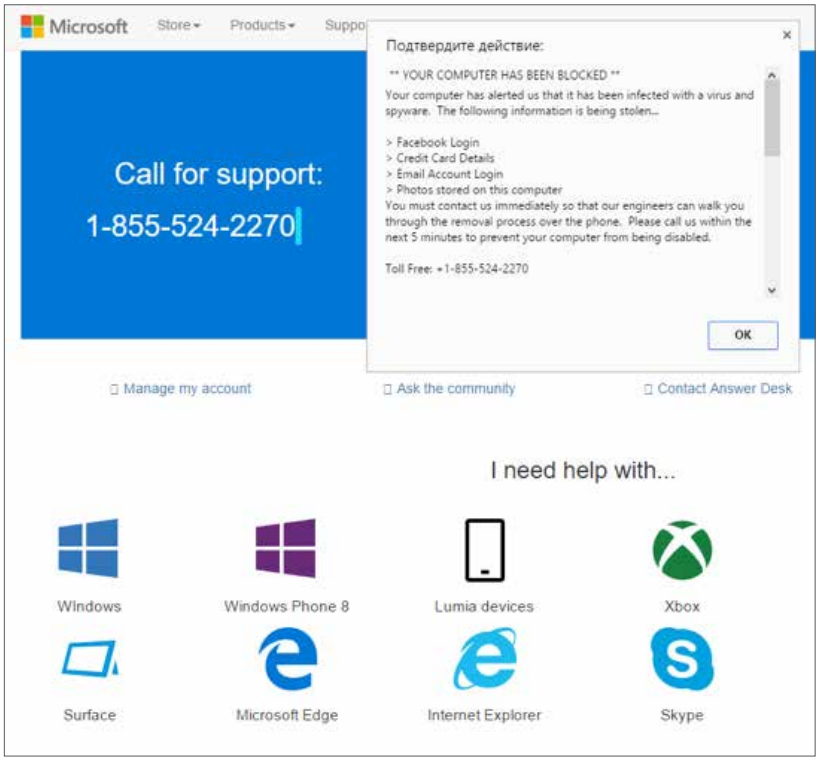
Armed with the latest in machine learning–based defenses, industry leaders are cracking down on this practice, not only by going after the reviewers, but also after the sellers benefiting from this activity. New third-party sites, such as FakeSpot, and ReviewMeta, are building on the foundation laid in past years; we can expect this consumer advocacy to continue to grow throughout the year ahead.

A number of defensive advances took place during 2016, from enhanced static and dynamic malware detection capabilities, to improved Twitter bot identification. We can expect scammers to counterattack in 2017, by either doubling down on their current targets, or moving to the path of least resistance. For malware authors this may manifest through the creation of "evil twin" applications (malicious routines added to copies of legitimate software) or compound programs (single applications that can act as both legitimate programs and malware). These efforts will further blur the line between real and fake for users as well as for defensive scanners.

Earlier this year, a collaboration between the US Federal Communications Commission and industry was announced to put an end to robocalls. What impact this may have in 2017 remains to be seen, but again we can expect those financially impacted to continue to deliver their fake pitches one way or another. One expected outlet will be an increase in fake online security warnings and alternative fake alert malware, such as bogus Windows installation alerts, that ask users to initiate the call. These warnings often grab the attention of unsuspecting surfers and result in naïve victims giving in to their fear of losing access to their systems.



A fake warning from a supposed Microsoft page requesting an access code to unblock the content by asking the user to call support.



This scam page covers the entire screen to appear as a legitimate Microsoft site. It also plays an audio alert demanding the user to call a number for support.

2016 proved to be the year when augmented reality went mainstream, thanks to the wildly successful launch of Pokémon Go. Users embraced "fake" as part of the immersive experience, losing themselves in the game. Undoubtedly this success story is just one of many to come. Will we find it more and more difficult to discern malicious fakes from desired fiction in a world that seamlessly blends the real and unreal?

Escalation of ad wars boosts malware delivery

—Adam Wosotowsky

The cat-and-mouse game between advertisers and ad blockers will continue. Some of the advertisers techniques for bypassing active content blockers will be used by malware distributors to enable drive-by downloads of malware.

Security researchers spend a lot of time in dangerous Internet territory, filled with cracked websites and drive-by malware downloads. To navigate this territory in relative safety, we use security add-ons for browsers that disable active content, read raw site content code, fetch bits piecemeal using different servers, and use virtual machines that get reloaded to avoid local computer infections. These precautions can turn "browsing the Internet" into a much more difficult process.

Most users do not need to go to these lengths. Average users are primarily concerned about the usability of their browsers and the sites they visit. But then came pop-up ads. Websites became hidden behind a slew of new browser windows flashing worthless advertising, rendering the sites unusable. In response, browsers added the ability to block pop-ups, and the ad war began.

Many websites today are copying the poor usability of these mid-1990s websites, though not because of pop-ups. Instead they offer horribly distracting blinking advertisements, ads overlaid directly on content, and video ads—with sound—that automatically play when the user visits a page (resulting in quickly closing the browser while glancing guiltily at those nearby). If an advertiser is pushing 10MB of advertising to a cellphone because someone wants to read 50 sentences of text, that company has gone overboard.

Security tools that stop the execution of active content in a browser also stop these kinds of ads. Like people who spread malware, advertisers use the same hooks to force computers to execute arbitrary code supplied by the website so the ads execute without the user's permission.

If advertisers were simply concerned with having their ads displayed, then the websites that users want to visit would serve ads directly from the primary domains; users could do little to block them. Unfortunately, displaying ads is not as valuable as tracking users without their permission across multiple domains to generate user profiles that are used to sell ad hosting to more clients. These folks use the same techniques malware distributors to collect telemetry and install data for the malicious infections they push. Interestingly, ad blockers that stop ads while we browse use the same methods security researchers do to prevent infections.

The ad wars are heating up between users (and their ad blockers) versus advertisers who are trying to deliver ads and gather telemetry on user behavior. Advertisers have new methods to bypass ad blockers, but those will be followed by updated ad-blocking software that blocks them again. Many ad blockers work by analyzing cross-site scripting and other components of web pages to selectively block content because few browsers actually offer the option (to developers) to fully disable the ability to execute active content. You can see where this will lead: With enough obfuscation, bad actors will be able to avoid protective add-ons. Advertisers who put making money ahead of security implications are doing the malware distributors work for them. In 2017, advertisers techniques for bypassing active content blockers will be used by malware distributors to enable drive-by downloads of malware.

Hactivists expose privacy issues

—Paula Greve

Hacktivists will work to educate consumers about their digital footprints by targeting and successfully breaching some of the corporate clouds that contain customer data. Hacktivists will then expose that personal data to generate consumer outrage and force action. These actions will continue until they are no longer newsworthy or public outrage forces changes in privacy laws and corporate policies.

Over the years, the amount of data collected about users has increased exponentially. This aggregated data has helped us improve our health, get where we want to go faster when we search, find long-lost friends, have a better performing home electronics system, and even stay protected while we go online. The usefulness of this data is even called out in the European Commission's Guide to the EU-US Privacy Shield: "Transfers of personal data are an important and necessary part of the transatlantic relationship, especially in today's global digital economy" (page 7). This year continued to bring increased awareness about information collected from our devices and the size of our digital footprints—from initiatives at schools to educate kids on controlling their data to articles about how businesses use personal information to better target ads. In fact, a TED search returns more than a dozen talks associated with "the dark side of data." This is a trending and controversial topic that will continue to make headlines next year.

Image originally posted to Flickr as "Anonymous at Scientology in Los Angeles," by Vincent Diamante [CC BY-SA 2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons.

Given these trends, we predict that in 2017 hacktivists will use this opportunity to "educate users" about how much of their data they are giving away. We anticipate this will occur through attacks that infiltrate some of the cloud services which collect data (searches, links, connections, page views, product usage, heartbeats, and more) and then post the contents publically as "public service announcements." Based on past behavior, once a hacktivist group targets an area and gains success, similar attacks are executed to prove the point—with each attack attempting to raise increased awareness. With this motivation, we expect to see these data breaches escalate, bringing attention to more respected websites and businesses.

Although we expect a global impact from these attacks, US corporations may see the most pressure. In the United States, businesses want to retain control over customer data. For example, Microsoft has gone to court several times "to protect" user data from the US government. The new EU-US Privacy Shield provides citizens with the ability to see which corporations are collecting which data. Ironically, this list can also be used by determined hacktivists who want to educate European citizens, and the world, about how much data US businesses have collected on them.

These attacks will trigger a number of follow-on security concerns: from companies that were breached dealing with the security ramifications of the breach and the customer trust impact, as well as preparing for the expected onslaught of customer complaints; to which companies will have 45 days to issue a response and the fallout from the options that customers can pursue if they are not happy with the response. Companies will have to take additional measures as a result of these complaints, including proving how long they retain data, the true need for the data collected, and whether the "opt out" vs. "opt in" vs. "just happens" nature of agreeing to send the telemetry was fair to the customer.

Looking back on the fallout from past data breaches caused by cybercriminal groups looking to profit from stolen data, those impacted were alarmed to learn not only how much data was collected but also the age of some data. It is bad enough to have personal data stolen, but trust is further violated when some of the data is no longer accurate. During the next few years, consumers will become more aware of the data collected and demand action, including additional control over their personal information and consistent retention policies.

We may see consumers pushing corporations to establish "right to be forgotten" policies and provide full visibility into the data collected.

In summary, we expect that in 2017 hacktivists will work to educate consumers about their digital footprints by targeting and successfully breaching some of the corporate clouds that contain customer data. Hacktivists will then expose that personal data to generate consumer outrage and force action. These actions will continue until they are no longer newsworthy or public outrage forces changes in privacy laws and corporate policies.

Law enforcement takedown operations put a dent in cybercrime

—Christiaan Beek

The number of takedown operations against the authors of distributed denial-of-service attacks and botnets around the world will grow as the result of increased cooperation between private industry and law enforcement agencies. More countries will see the effects of cybercrime on their economies and increase their investment in cyber response capabilities.

We have seen some notable recent successes of law enforcement and its allies taking down malicious sites or actors. McAfee has participated in some of these. What is a takedown operation? It is a series of coordinated actions in which law enforcement agencies, together with other parties (usually security vendors), shut down a cybercriminal operation. In the best case, it includes arrests, but in all cases the takedown disrupts or seizes the infrastructure used by cybercriminals. A takedown operation is the result of many months, or in some cases years, of investigations.

One example of a large takedown by Russian authorities was the arrest in June of 50 people who were responsible for a multiyear campaign to steal $25 million from Russian banks. Footage of the arrests can be found on YouTube.

In 2016, McAfee participated or assisted in four ransomware takedown operations and supported or assisted in several more that have not been publicly discussed. The ransomware takedown operations are part of the "No More Ransom!" project, in which law enforcement agencies and IT security companies have joined forces to disrupt cybercriminals who employ ransomware in their attacks. McAfee is one of the founding members of this project.

Many ransomware decryptors are provided as the result of takedowns.

We find it encouraging that other security companies are joining the battle against cybercrime. Unfortunately, months of research and a few takedown operations were compromised this year by premature announcements. Verification with the relevant law enforcement agencies would have prevented those compromises. Because many security companies and global law enforcement agencies want to join the No More Ransom! project, we strongly believe we can turn the tide on ransomware.

In 2017, McAfee will continue to assist global law enforcement in takedown operations. We will also actively participate in the No More Ransom! project and similar organizations, sharing our knowledge and expertise to serve the global community.

The number of takedown operations against the authors of distributed denial-of-service attacks and botnets around the world will increase as the result of increased cooperation between private industry and law enforcement agencies. More countries will see the effects of cybercrime on their economies and increase their investment in cyber-response capabilities. The faster we can act, the better we will be able to respond and intervene. Private companies that participate in joint operations with law enforcement agencies should anticipate and prepare for legal ramifications. Next year could be the first time that cybercriminals begin to challenge the relationship between private vendors and law enforcement agencies.

Threat intelligence sharing makes great strides

—Jeannette Jarvis

Sharing threat intelligence shifts the balance of power away from the adversaries and back to us, the defenders. It disrupts the lifecycle of an attack and proves more costly to the bad actors as they shift their resources and techniques onto new tactics. This shift played out in 2016 when the founding members of the Cyber Threat Alliance (CTA) collaborated on research around the CryptoWall Version 3 campaign. Shortly after publishing this research report, the malware authors abandoned their focus on CryptoWall Version 3 and shifted their efforts to a new campaign, Version 4. The CTA will continue to improve our collective defenses by collaborating and conducting further in-depth research in 2017. This research will uncover new attacks and detail indicators of compromise that will be shared and added to members' control systems to stop further attacks.

If sharing threat intelligence is so valuable, then why isn't there more cooperation? Historically, there have been three key barriers to sharing threat intelligence:

1. Unintentionally sharing private customer information.
2. Losing a competitive advantage.
3. Public awareness that an organization has been attacked.

We will see ISAO communities of trust established. We will also see new ISAO platforms emerge that will allow businesses to automatically add threat intelligence into their security systems.

Fortunately, the security industry is changing, and these concerns are fading. For example, the Cybersecurity Information Sharing Act provides legal foundations for sharing threat intelligence between the US government and the private sector, and between private sector organizations with liability protection extending to the sharing entities. With this liability protection now afforded them, American corporations are evaluating their sharing polices. We should see much more threat intelligence sharing in 2017.

Stopping attacks in near real time will require automated tools and processes. Under US presidential Executive Order 13691, the US Secretary of Homeland Security was directed to form the Information Sharing and Analysis Organization (ISAO) Standards Organization. The ISAO Standards Organization has built foundational guidelines and best practices for effective information sharing and analysis. In 2017, we will see many ISAO communities of trust established around affinities of interest based on sectors, regions, and other related domains. We will also see new ISAO platforms emerge that allow businesses to automatically add threat intelligence into their security systems.

We predict that there will be better governance and accountability as ISAOs and other threat-sharing programs evolve. The International Association of Certified ISAOs (IACI), whose mission is to drive guidance and certification of ISAOs, will be fully formed in 2017. IACI will provide assistance to organizations developing and advancing the management of cyber threat sharing programs around the globe.

To improve our cyber defenses, the industry must cooperate. Crowdsourced threat intelligence and collaborative analytics help connect the dots and form better pictures of what is happening in the attack landscape. 2017 will be the year in which threat intelligence sharing makes its most significant strides.

Cyber espionage: industry and law enforcement join forces

—Christiaan Beek

Due to changes in international laws and agreements between countries, we predict that former state-sponsored cyber espionage teams will move into the role of information brokers, providing "access" for money. Their modus operandi will remain the same.

In the first nine months of 2016, McAfee registered 78 public cases of what we classify as cyber espionage or warfare. In most of the campaigns, nation-states were seeking the political views or backgrounds of targeted entities. The targeted entities were in the government sector or, in some cases, individuals or members of a political party.

The modus operandi for these cases is similar and we predict that they will not change much in 2017. Each starts with the actors setting up a host domain infrastructure that will serve either as a control server or deliver a payload. Next is the spear-phishing attack, in which the target receives weaponized email. Sometimes, the attackers include hidden code in embedded HTML that tracks the computers the attackers aim to control and lets them know where in the network they have landed. From there, attackers use an arsenal of tools, ranging from credential editors, pass-the-hash attacks, or custom scripts. In most cases, a backdoor remote access Trojan maintains a foothold in the network. Less skilled actor groups use commercial off-the-shelf RATs such as PlugX and modify the basic settings to serve their campaigns.

Two cyber espionage cases especially intrigued us this year. The first was Irongate. Researchers found a complex piece of malware attacking industrial control systems. Pieces of the code were related to the famous Stuxnet cyber-weapon worm. That is one risk of using malware as a cyber weapon: If the code gets leaked, it is sure to appear elsewhere. At some point, someone is going to adapt and improve upon these malware apps. This leads to the second case, Strider/Sauron, a very advanced piece of malware, using a modular approach and techniques. Strider/Sauron is an impressive example of malware that really deserves the moniker advanced persistent threat. It should concern all of us when code like this is made public; we can expect that nation-state–sponsored groups will learn and adapt some of these techniques.

What will happen with cyber espionage in 2017? Cyber espionage will always be present, either as part of a nation-state's intelligence operations or run by organized groups that will hunt for proprietary intelligence and offer it for sale. Due to changes in international laws and agreements between countries, we predict that former state-sponsored teams will move into the role of information brokers, providing "access" for money. Everyone has information that is worth something, but it takes a creative mind to profit from it.

Another prediction concerns network security. The leak of tools claimed to belong to the Equation Group made it very clear that advanced attackers are looking into compromising firewalls. Successfully attacking core routers or VPN concentrators gives access to a network and provides a great way to fly below the security radar. We will see more research around and detection of these kinds of exploits in 2017.

Physical and cyber security industries join forces

—Matthew Rosenquist

A strategic shift is about to occur in the security industry. The cyber and physical security domains will begin to intersect and extend security across the real and digital worlds. The continued adoption of technology that enhances the lives of people and productivity of businesses will force the security industry to bridge the gap between cyber and physical security. This convergence is a natural outgrowth of the two fields' common purpose—to protect and secure people and assets.

Two giants, one goal

The global cyber and physical security industries are about $80 billion and $100 billion, respectively. The physical security industry is much more mature and stable, while the cyber security market is characterized as more chaotic and rapidly growing.

For years they have both existed largely independent of one another. Physical security focuses on video surveillance, access-control systems such as door locks and badge readers, barriers, safety systems, and tools to protect valuable assets. Cyber security focuses on protecting computers, smart devices, telecommunications, data, clouds, and anything connected to the Internet. These assets and services provide tremendous value but must be protected from different types of threats.

The world changes

As the growth and expansion of digital tools and technology has increasingly permeated our daily lives, the need for cyber security has grown. The trend is to connect, monitor, and control devices from anywhere. Computer systems are being designed with more sensors and capabilities. Everyday devices are now being connected and becoming "smart." The convergence of the Internet of Things is driving an expected 200 billion devices to be connected to the Internet by 2020. Many of these devices will be in homes and businesses, the very core markets for the physical security industry. If your new smart front door lock opens for burglars or your bedroom baby monitor is live-streamed to the Internet, you will not feel safe.

Gartner estimates that by 2020 more than 25% of attacks in enterprises will involve IoT devices. This is fueling the already staggering IoT security spending to double from $282 million in 2015 to more than $547 million in 2018.

Alarm, access control, and video surveillance security products are themselves becoming targets for cyber attacks. Connecting security devices to networks can provide cost benefits and enhanced features for customers, but it exposes them to hackers. The software, firmware, and data can be exploited.

The physical and cyber security industries will join forces and begin hardening security products from digital threats. They will leverage each other to enhance security and safety for the next generation of products and services.

These two markets need each other

Technology associated with physical safety and security is in desperate need of better cyber protection. All devices on IP networks, especially those directly connected to the Internet, need cyber security protection. It is estimated that about 70% of the video surveillance cameras sold are now connected to computer networks. This creates a huge pool of vulnerable devices.

Vast numbers of video surveillance cameras are already being hacked. A simple Google search can locate systems hemorrhaging video data. Highlighting the problem is an openly available search engine, Shodan, that lets users browse vulnerable webcams. Live feeds from cameras all over the world are easily viewable. Feeds from bedrooms, banks, living rooms, baby monitors, pools, colleges, etc. are there for anyone to watch. This is what is available to the public, based upon poor configuration or lack of even basic security controls. Serious hackers are more discrete and have much better tools to gain access to many more systems.

This is just the beginning. As other physical security and safety systems are connected to the Internet, more exploitation and hijacking will occur. Recently, more than a million cameras and DVRs were compromised and reconfigured by an attacker to become part of a botnet. This botnet then attacked other systems on the Internet. Because there were no detection controls, all this took place without the device owners realizing they were supporting criminal activities. The physical security industry desperately needs cyber-based controls to harden their products and services so they can resist cyber attackers.

As the world embraces more digital devices, online services, and broader connectivity, the need for security will increase. Consumers and businesses expect privacy and security, while benefitting from advanced remote features. The differentiation between the physical and cyber domains will no longer be relevant and will begin to merge. Consumers will not be happy if their bedroom camera feed is under the control of strangers on the Internet. They will not care whether it is a software or network problem. They will hold the product manufacturer, security service provider, or installer responsible. The same is true for health care devices, automobiles, and industrial controls in businesses. These must be both physically and digitally secure.

Consumers and executives will want what they have always wanted: a single entity responsible for owning and fixing problems. Recent surveys show how consumers are already cognizant of risks and are ready to walk away from their favorite retailers if a breach occurs. The telecommunications industry has already felt the pain. The recent TalkTalk data breach in Europe drove more than 100,000 customers to leave and go to another vendor. These changing expectations, fueled by technology convergence, will drive the cyber and physical security industries to actively join forces.

Predictions

In 2017, we will see the physical and cyber security industries work collectively to create more comprehensive and cohesive security solutions:

1. The physical and cyber security industries will join forces and begin hardening security products from digital threats. Both markets are already unified in purpose for their customers. Now they will leverage each other to enhance security and safety for the next generation of products and services.

2. Consumers will become upset about cyber attacks on physical devices that undermine their security, safety, and privacy. They will demand a cohesive security experience or look to other vendors and suppliers.

3. Cyber security solution providers will begin to service and support physical security vendors by offering new software, platforms, and architectures for integration. Expect announcements from both large and boutique cyber security companies.

4. Physical security conferences will expand to include cyber security topics, experts, and vendors. This is a true sign of collaboration when vendors begin to cross-pollinate at trade events.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com

Follow McAfee Labs

McAfee
Together is power.

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

SEPTEMBER 2016