QUESTIONS AND ANSWERS:

THE 2017 SECURITY LANDSCAPE

2017

FireEye

CONTENTS

INTRODUCTION

It has been said that “the future is uncertain,” but in the cyber security industry we know that certain types of attacks and crime will continue unabated. FireEye and other experts in the industry have been making predictions about the year ahead for longer than a decade now. Some of those predictions have come to fruition and are no longer relevant, but others – such as ransomware, talent shortages and nation-state threats – continue to be named as problems to expect when looking forward.

For a look at what to expect in 2017, our Questions and Answers: The 2017 Security Landscape report features predictions from CEO Kevin Mandia, CTO Grady Summers and other members of our executive team. Additional commentary is provided by top experts at Mandiant, a FireEye company and leader in helping organizations respond to and proactively protect against advanced cyber security threats.

Other contributors include the FireEye iSIGHT Intelligence team and FireEye Labs. The FireEye iSIGHT Intelligence team produces actionable intelligence that arms global enterprises with rich contextual information about the motivation and intent of adversaries, their campaigns and technical indicators, the malware they use and the vulnerabilities they exploit. FireEye Labs is the threat research and analysis division of FireEye that continuously monitors and analyzes threats detected by 11 million network and endpoint sensors deployed across 60 countries.

What investments in security will organizations make in 2017?

Our discussions with CSOs and other security leaders throughout 2016 have a common theme: simplification. This is why FireEye expects to see organizations making significant investments in the form of orchestration and automation in 2017.

The past few years have seen organizations spending high dollar amounts on security technologies and other infrastructure that either do not work well together, or require a great deal of effort and personnel to follow and address the myriad alerts. Organizations seeking to simplify everything in 2017 will set their sights on integration. A single pane of glass for all security needs will drastically improve the organization's security posture and show companies the true value of all the products they have acquired. We refer to this as security orchestration and it is part of the reason we acquired Invotas in early 2016.

Automation is the final piece of this puzzle and – considering the resource struggle impacting the industry – will likely enter the mainstream as we move into 2017. Automation enables organizations to more efficiently address critical needs, which is particularly useful for enterprises that are struggling to keep pace with an escalating threat landscape and constant advances in cyber attacks. FireEye plans to take the lead in helping customers deal with the severe shortage of resources by automating the security process and building intelligence into their operations. We expect security orchestration capabilities will enable organizations to move from alert to remediation in minutes.

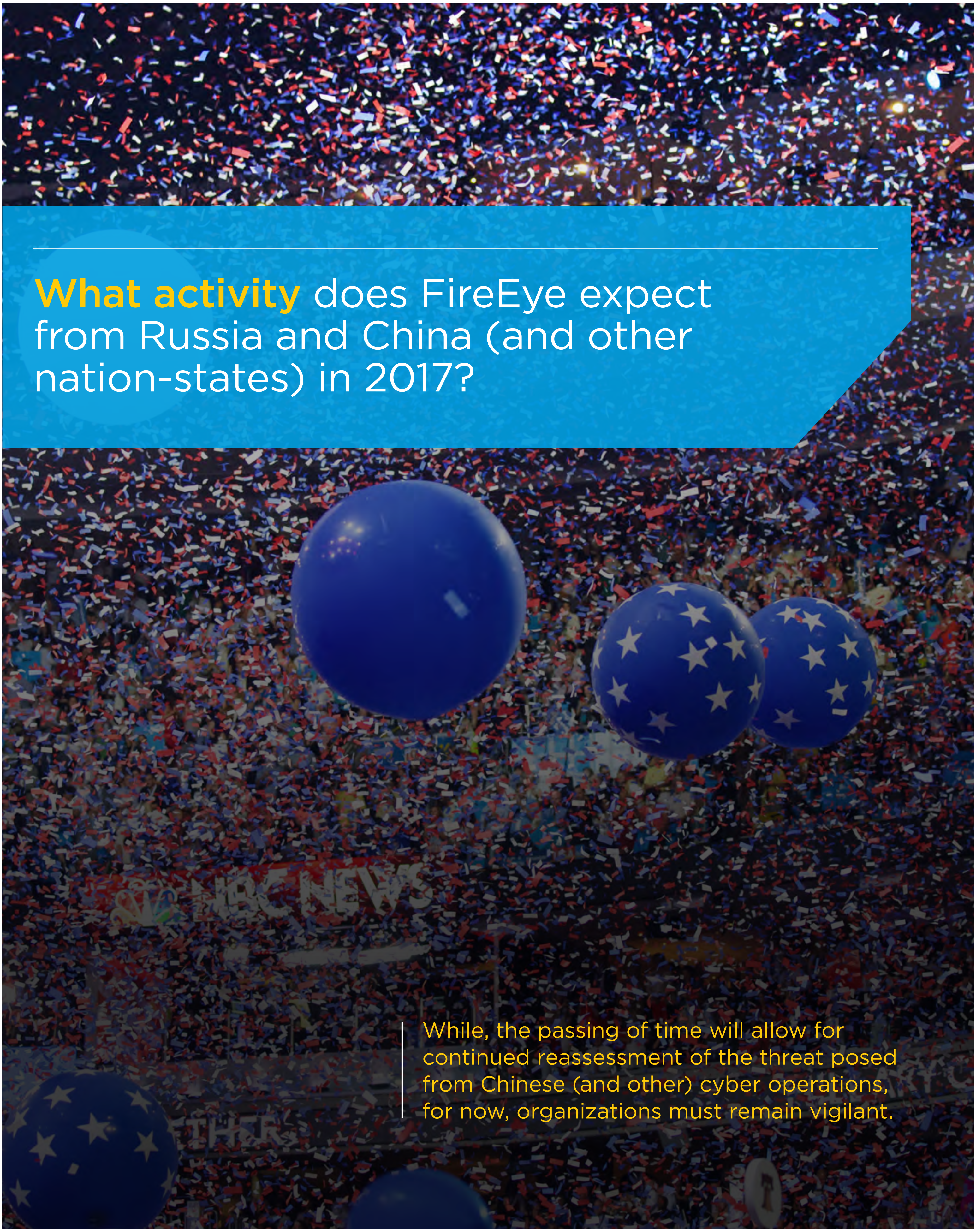
> As the talent shortfall continues, the cyber security industry will see more innovation in the form of automation.

We also expect automation to help address a common topic of discussion in the security industry: the talent shortage. The talent shortage is very real and not something that will be resolved overnight. If anything, it will likely begin to get worse as more and more "things" become connected. The constantly expanding Internet of Things requires specialized knowledge to understand and secure properly.

As the talent shortfall continues, the cyber security industry will see more and more innovation in the form of automation. FireEye expects to see an increased adoption of security tools that can react to attacks with minimal human intervention. We also anticipate an increase in technologies that adopt artificial intelligence and security orchestration across independent security tools.

It is important and beneficial for companies to begin simplifying and consolidating technologies, and it is something we are already seeing at organizations such as large banks, which must manage and secure hundreds of branches and tens of thousands of employees.

What activity does FireEye expect from Russia and China (and other nation-states) in 2017?



While, the passing of time will allow for continued reassessment of the threat posed from Chinese (and other) cyber operations, for now, organizations must remain vigilant.

We've seen an increase in overt Russian aggression in 2016 and we expect that to continue in 2017. The attacks on the Democratic National Committee and other election-related organizations are clear examples of Russian aggression. Russia has a well-funded cyber capability and excellent operational security to hide the source of their attacks. In addition, the complex relationship between the Russian government and private Russian hackers contributes to the difficultly in attributing attacks to Russia and understanding how their hacking groups operate. Russian President Vladimir Putin has denied responsibility for the attacks despite accusations by the FBI and senior U.S. national security officials and it is difficult to prove otherwise through non-clandestine means.

Historically, diplomatic policies have proven that they can address cyber threats from countries such as Russia. Perhaps in 2017, or possibly in 2018, Russia could end up seeking a deal with the U.S. similar to the one made between the U.S. and China.

On Sept. 25, 2015, President Barack Obama and Chinese President Xi Jinping agreed that neither government would "conduct or knowingly support cyber-enabled theft of intellectual property" for an economic advantage. While we have observed an overall decrease in successful network compromises by China-based groups against organizations in the U.S. and 25 other countries since mid-2014, it still remains to be seen what impact these possibly temporary factors will have in China's cyber operation policy.

One thing that is likely to remain in 2017, however, is China continuing to use its cyber operations to achieve key strategic objectives. Outside the U.S., nations such as Japan, Australia and South Korea are a consistent focus of targeted Chinese cyber espionage activity. This focus will continue and relevant geopolitical events will maintain this threat moving into next year. While, the passing of time will allow for continued reassessment of the threat posed from Chinese (and other) cyber operations, for now, organizations must remain vigilant.

Despite the focus on cyber threats originating from China and Russia (as well as Iran and North Korea), many additional countries have shown the desire to conduct cyber espionage operations, and we should expect that to continue in 2017. After all, reports indicate that dozens of government intelligence and military agencies worldwide were clients of offensive cyber security vendor Hacking Team at the time of its highly publicized breach in 2015, and 21 different nations hosted infrastructure used to launch Hacking Team-related operations.

Those countries and others have used purchased tools and foreign expert guidance to improve their understanding of how to conduct cyber espionage and attack over the last several years, and as their operational maturity and local technical sophistication improve, we expect more of these nation-states to sponsor cyber operations that target regional rivals, terrorists living abroad, regime critics, major corporations, and Western governments. Additionally, several emerging cyber powers – particularly in South Asia and Latin America – are already centers for the development of cybercriminal talent, which their national governments are increasingly tapping into.

Most worryingly, many of the emerging cyber powers have poorly defined military doctrine around cyber operations, control their operations at different levels of approval ranging from head of government to frontline commander, and have fought significant lethal conflicts with one another in the past few decades – all factors that suggest those countries may be willing to launch damaging cyber attacks against one another, including against critical infrastructure and public services, if tensions escalate.

What industry or type of organization might unexpectedly become a target of threat groups in 2017?

International political trends and security concerns are likely to increase the importance to prominent advanced persistent threat (APT) sponsors of **penetrating religious institutions**. Likewise, the fact that many religious institutions do not have robust cyber security, yet maintain contact information and other sensitive data, will make targeting them a particularly good return on investment for APT sponsors.

Religious institutions in Western countries are at particular risk, both because of the likely state actors that would target them and because in many Western countries most religious institutions would not be viewed as legitimate targets for cyber espionage.

Russia could increase its focus on Western missionaries in their country and on foreign religious leaders who play a role in international politics. Starting on July 20, new restrictions on unregistered religious groups – notably Mormon missionaries and Jehovah's Witnesses living in Russia – and street proselytizing will go into effect that could lead to cyber espionage to aid in monitoring their activities. We have already seen Russian government-sponsored actors APT28 use a domain name similar to one belonging to the Vatican to trick some of their other targets into thinking malicious network traffic was normal.

China probably believes it faces threats to stability and public safety as millions of Chinese take advantage of easing government restrictions on religion to join Christian and Islamic faith groups. China will likewise probably want increased intelligence on the activities of faith-based NGOs operating within its borders, on religious leaders with domestic constituencies such as the Dalai Lama, on the impact religious leaders have on the foreign policy of China's neighbors, and the role of faith groups in organizing the country's ethnic minorities.

India has also seen a rise in religious identity politics, particularly among Hindu nationalists currently in control of the Union Government. Inflamed domestic religious sentiments could easily lead to a recurrence of cyber attacks from non-state or state hackers protesting perceived Indian government mistreatment of its Muslim minority.

How will attackers take advantage of a constantly expanding Internet of Things and a growing number of cyber-physical systems?

In 2017, we expect more nation-states to target cyber-physical systems – both critical infrastructure such as power plants and consumer devices such as home appliances – to coerce other nations by disrupting government functions, instilling fear and holding physical systems hostage not for ransom, but as political bargaining chips.

In general, the proliferation of cyber-physical systems and the Internet of Things (IoT) will present new opportunities for adversaries to abuse their connectivity and cause disruption at scale for a bigger payoff. The combination of tools such as ransomware with more formalized illicit software-as-a-service franchised business models will become a more attractive and lucrative option for criminals with the proper skillsets and motivations. They will also help to lower the barrier to entry for criminals eager to reduce upfront costs and avoid pricey infrastructure setup.

The growth in IoT devices provides a newly available slew of poorly protected or monitored devices that can be coopted for malicious purposes. These range from enslaving IoT devices to launch distributed denial-of-service (DDoS) attacks or serve as command and control hop points, to enabling network credential theft or remote access Trojan (RAT) malware distribution.

From a disruption standpoint, compromising connected vehicles that comprise a logistics or rental fleet would allow criminals to demand higher ransoms than targeting individual drivers' vehicles. This is because the business lost due to downtime will likely outweigh the cost of the ransom payment. Other corporate systems that similarly take advantage of connectivity may also be targeted to increase the attack scale and potential payoff.

Will threat groups continue to target industrial control systems in the near future?

> Perhaps most shocking is that security patches were not yet available for more than 30 percent of identified vulnerabilities.

On the heels of our Overload: Critical Lessons from 15 Years of ICS Vulnerabilities report, FireEye expects that threat actors will continue to focus on these critical systems in 2017. Most nations are heavily reliant on industrial control systems (ICS) for fundamental government services, utilities and commercial systems, yet our research in this report and on the front lines of incident response and Red Team operations highlight that these systems are usually poorly protected and often not patched. Perhaps most shocking is that security patches were not yet available for more than 30 percent of identified vulnerabilities. Additional risks exist for countries that rely heavily on the resource and industry sector, as ICS also plays a critical role in large commercial field and mining operations.

The lack of awareness of many industrial control system assets by relevant security personnel is worrying, as is our observed trend for more daring and disruptive cyber events. The Ukraine power grid cyber attack in late 2015 is just one event that highlights what can be achieved by attacking ICS. These factors, coupled with the observed demand for vulnerable ICS systems by threat actors, will likely culminate in extortive and disruptive industrial system incidents across many countries and many ICS-reliant sectors in 2017, especially resource and heavy industry.

Now that the U.S. has elected their next president, what could we expect as the new administration begins settling in?

A new U.S. President will take office in January 2017, presenting an opportunity for foreign governments to test the new administration's resolve through various provocations. The aggressive intercept of – and eventual collision with – an EP-3 Aries II surveillance aircraft in April 2001 and a similarly aggressive attempted blocking of the ocean surveillance ship USNS Impeccable in March 2009 both occurred within the opening 100 days of new U.S. administrations.

Cyber capabilities will give each of these nations – and others – the ability to use both the reach and relative anonymity of cyberspace to assess the new U.S. administration's ability to manage provocations. These could include measures ranging from propaganda exploiting civil discord in the aftermath of a close election to conducting more aggressive operations against U.S. allies to test the strength of defense partnerships.

Other nations that have not previously participated in the cyber domain may find the arrival of a new and relatively inexperienced administration the perfect opportunity to test fledgling capabilities, either against the United States or a regional competitor.

What does the immediate future have in store for less security mature regions?

Next year we expect to see a continued rise in attacks against less security mature regions, notably in the EMEA and Asia Pacific regions. The FireEye M-Trends 2016 reports for each respective region show that the median time of compromise to discovery of an attack was 469 days in EMEA and 520 days in Asia Pacific. As a point of reference, the global median time of compromise to discovery of an attack was 146 days. Meanwhile, the Mandiant Red Team is able to obtain access to domain administrator credentials within an average of three days after gaining initial access to an environment, so it's clear that every region still has a long way to go.

The Asia Pacific and EMEA experiences of 2016 around financial sector compromises, and continued focus of threat activity against relevant critical systems such as SWIFT, are a sobering reminder of the reach and capability of a determined and motivated cyber adversary. We will continue to see sophisticated financially motivated espionage actor groups focusing on these and other critical systems in 2017. Additionally, we will see credit and debit card fraud, illicit bank transfers, and ATM fraud. Underdeveloped countries will also continue to be a primary target for cybercriminals looking to successfully empty ATMs, as those countries more than others still have old ATM software and are running Windows XP. This makes them the perfect target for an easier score.

The EMEA and Asia Pacific regions are often where we see emerging businesses starting to strive to be competitive in the regional and global markets. Many markets and sectors, especially in the Asia Pacific region, continue to slowly mature from their previous developing nation status. Technology adoption is critical for increased efficiency benefits; however, in 2017 these enterprises must also focus their resources on cyber security. The FireEye experience across the world has shown that maturing businesses and enterprises are often vulnerable to compromise and will be breached.

At a minimum, less security mature organizations should check for evidence of compromise by reviewing network ingress and egress points, reviewing each security logging device and ascertaining how security risks will be identified and alerted when they occur, focusing on authentication and whether a user account has been compromised, and adopting a behavioral analysis detection approach with log data to identify high-risk security threats. Responding to a security breach should include assembling a crisis management team, fully scoping an incident, avoiding premature remediation, and reaching out for professional incident response support when required.

The FireEye experience across the world has shown that maturing businesses and enterprises are often vulnerable to compromise and will be breached.

What malware will attackers be using in 2017, and how should organizations respond to these threats?

Ransomware activity continues to increase, likely due to low overhead and a high return on investment. Media coverage of successful attacks against hospitals and other organizations in 2016 also show that the threat is working. While we expect ransomware attacks to continue in 2017, law enforcement has already made a dent in some groups by shutting down ransomware infrastructure and going after criminals. Law enforcement will continue to focus on this next year and for as long as it's a problem. As organizations become more aware of the threat, they are taking action by creating and testing backups. They are also testing their security tools and controls to better prevent and detect ransomware. A major medical center was in the news in 2016 for paying $17,000 in Bitcoins, but what didn't make the news later in the year were the many other companies infected by Locky and other ransomware that were able to recover via backups.

Script-based malware – JavaScript, VBScript, macros and PowerShell – has seen plenty of use throughout 2016. We expect cybercriminals will continue to migrate towards script-based malware in 2017 due to improvements in machine learning-related solutions at identifying traditional executables such as EXE and DLL. Script-based malware threats are typically tougher for security vendors to detect, and we are seeing them become increasingly common in both email campaigns and lateral movement.

Macro-based malware in particular will keep switching to unexpected formats as an evasion technique. Toward the end of 2016, we observed Microsoft Publisher documents (PUB) being used to deliver malicious macros and, due to the unexpected extension, many spam filters were bypassed. Another similar case involved Microsoft Word 2007 template files (DOTM). Other formats not widely exploited, such as PPTM files created in Microsoft PowerPoint, could be the next focus for threat actors.

We expect attackers to continue making their malware more stealthy and effective – a necessity given the success in security technology and vendor security controls. For example, threat actors are hiding malicious code in unused sectors, and maliciously modifying master file tables (MFT) and volume boot records (VBR) to load malware before security software loads is becoming more prevalent.

Focusing on Layer 8 of the Open Systems Interconnection model – the user level – is pivotal in preventing malware infections. Organizations should be enforcing security awareness programs that aim to reduce the social engineering attack vector. Organizations should also focus some of their monitoring efforts on looking for anomalous user account activity. Finally, organizations should protect users from themselves by ensuring macros are disabled by default, and training staff to never enable them unless they are required to operate on a known-good document.

THE BATTLE AHEAD

Consumers must remain vigilant. The good news is that increased focus on secure operating systems and applications means consumers only have to perform basic security hygiene to remain reasonably protected. Other basic steps consumers can take to stay ahead of threats include enabling two-factor authentication on all of their systems and accounts, using password managers to protect their systems and accounts, and automatically backing up data in the event that they are affected by ransomware or their data becomes compromised by a threat actor.

Enterprises on the other hand will continue to be under attack in what seems to be an asymmetric battle. Mandiant has been advising clients to prepare for when attacks happen, not if they happen, and to be ready to respond to and contain an incident. One way to be prepared is to hold incident response tabletop exercises to simulate typical intrusion scenarios, thus exposing participants – such as executives, legal personnel and other staff – to incident response processes and concepts.

> Mandiant has been advising clients to prepare for when attacks happen, not if they happen, and to be ready to respond to and contain an incident.

One sobering thought is that the threat activity we expect to hear about in 2017 may be taking place right now, with adversaries already inside many of the systems and networks necessary to be in for them to achieve their mission. We know that most cyber threat actors operate within environments for many months before they are discovered, and in some instances for longer than a year. These adversaries, many of which are tracked and monitored by FireEye, are likely moving through corporate or government networks at this moment and exfiltrating datasets – activity that could continue into next year. Therefore, most of the events that will make headlines in 2017 – and the many that won't – are already underway.

Finally, it is important to keep in mind that many organizations are still responding to cyber attacks from 2016. Moving into 2017, we expect there will be more actuarial data on the cost of breaches and the security products and technologies that are likely to be effective. This increased focus on numbers in 2016 will prove useful to the community at large. With this information, organizations will be able to make more informed decisions on what to protect, and how to protect it.

To get the latest executive perspective
about how FireEye can help
your organization stay safe in 2017,
visit: **www.fireeye.com/company/why-fireeye.html**

ABOUT FIREEYE, INC.

FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye®