CYBERSECURITY TRENDS 2019:

Privacy and Intrusion in the Global Village

INDEX

INTRODUCTION

For several years now, ESET experts from around the world have been contributing to our annual Trends report, which offers a brief review of the milestones reached in the world of cybersecurity and our predictions about possible attack scenarios and measures to counteract them in 2019.

The basic scenarios regarding these issues vary little: it comes down to defending the confidentiality, integrity, and availability of data belonging to individuals and companies against repeated attacks by cybercriminals who try to access, use, and/or steal these data. For these reasons, in the 2019 edition of the Trends report you will find a section focusing on data privacy and the rising importance for businesses to manage data privacy correctly, especially in light of the Facebook/Cambridge Analytica controversy, as well as the Google breach and subsequent decision to shut down Google+.

Those incidents, in conjunction with the General Data Protection Regulation (GDPR) coming into effect, are starting to have an impact on the industry's big players. This raises questions about how the giant's cases could affect other, smaller businesses that might not have the resources needed to adequately protect the privacy of their customers.

Consequently, considering the immense volumes of data belonging to individuals but being managed by these services, some government bodies are beginning to pay attention to how they process and protect the data. Moreover, these government bodies are starting to exercise controls, such as GDPR in the European Union, which came into effect on May 25, 2018. In the *EU GDPR chapter* we consider some of the most important issues related to this regulation and also evaluate what the future implications may be with respect to future government controls taking effect in various parts of the world.

Data protection and privacy remain the underlying issues that connect through the other sections. Just as technology is continually progressing, the way in which it is used also changes and evolves, which in turn results in cybercriminals looking into new ways to take advantage. Hence, in this document we present a section on home assistants, the precautions that need to be taken when using IoT (Internet of Things) devices, and their implications for security, both at work and at home. Another related issue is a threat that has attracted a lot of attention over the past year and that takes advantage of legitimate blockchain technology: Coin miners, a threat that seeks to take advantage of victims' computer processing power in order to mine cryptocurrencies and give the attacker a financial return.

Of course, there is a counterpart to all these technological advances and the attempts by cybercriminals to take advantage of them, and that is the utilization of technology to protect users and organizations. One example of this progress is machine learning (ML), through which it is possible to make maximum use of the vast quantity of information generated from interactions between users and systems, by processing it and using it to improve the systems. It is also worth noting that ML is only a tool, not an all-inclusive solution. However, history has shown us that any technology can be used and misused for all kinds of purposes and therefore in the ML section we look consider the question: Could this technology be misused?

Part of the ongoing task of protecting the individual's and company's information involves knowing what lies on the horizon and the challenges to be faced in IT security; so we invite you to read all the sections of the Trends report in order to to learn what ESET experts predict the security trends will be in 2019.

1

COIN MINERS: THE NEW KIDS ON THE BLOCK?

- Remember ransomware?
- Getting rich from coin mining
- Protecting your system

AUTHOR

David Harley
ESET Senior Research Fellow

Coin miners: The new kids on the block?

For many people, their first encounter of *virtual currencies* or *cryptocurrencies* may well have been when they, or someone they know, fell victim to ransomware, which generally requires its victims to pay for the recovery of their encrypted data in a cryptocurrency such as *Bitcoin*.

Using such a means of payment is advantageous for the criminal because transactions are not easy to tie to a real-world identity, especially if converted to other cryptocurrencies before they are finally exchanged for cash or items with real world value. In consequence, many ransomware victims have found themselves having to follow a criminal's instructions on how to sign up for a Bitcoin wallet or other means of making a ransom payment.

This doesn't mean, of course, that ransomware victims are well acquainted with the esoterica of cryptocurrency or understand what is meant by cryptocurrency mining (sometimes known as cryptomining, or coin mining), even if they've used cryptocurrency to pay a ransom. An exhaustive description of how *blockchain*, *cryptocurrency and coin mining* work is well out of scope for this article. In brief, however, while it's not exactly 'mining' for virtual coins in quite the same way that the *Seven Dwarfs* mined for jewels, it does involve investing work in terms of computer processing and electrical power in order to 'find' something. Simplistically, *cryptocurrency mining* consists of devoting processing power to a mathematical process that creates and distributes virtual coins.

Cryptocurrency mining (or, indeed cryptocurrency) is not, in itself, necessarily *illegal*, though there are plenty of app providers and commentators who could be accused of misrepresenting the profit potential of the mining bandwagon. Some of the enthusiasm from app vendors and commentators, urging anyone who'll listen to get involved, has been compared to *Ponzi schemes* and the *South Sea Bubble*.

While Bitcoin is surely the cryptocurrency that everyone has heard of, there are plenty of others. *Monero*, for instance, is popular with cybercriminals because it is designed to be privacy-centric, which has obvious advantages for criminals — even more so than for the rest of us.

In fact, Bitcoin mining is *a costly process, now barely* profitable for any but the largest-scale operations and much too demanding for individual PCs and devices, though some alternative currencies are less demanding. The processing load can, however, be shared between multiple machines and devices, which is why there are legitimate apps that (often for a fee) interface with a 'mining pool'. But that doesn't mean that the owners of participating machines are *always* aware of their role, and it doesn't always mean that profit is *also* shared. Increasingly, we see instances of *legitimate services* being provided in exchange for 'borrowing' of an individual device's processing power for mining purposes, but when a device is hijacked illegitimately (cryptojacking), there is no such quid pro quo. Most notoriously, (some of) the victim system's processing power is hijacked by on-disk or fileless malware (often referred to as a coin miner) or by scripting *on a website* (in-browser cryptojacking).

Heigh-ho, heigh-ho...

Individual systems dedicated to cryptocurrency mining tend not to rely solely on Central Processing Unit (CPU) *cycles* but also processing from auxiliary devices such as Graphics Processing Units (GPUs), and dedicated application-specific integrated circuit (ASIC) chips. Will we see more miner malware intended to take advantage of such hardware? It's likely that individuals or organizations consciously dabbling in the mining business with comparatively expensive dedicated hardware will be watching for stolen cycles (they might even be using security software!), but users of high-spec gaming machines, for example, might be less cautious.

Noticeably high usage of CPU and GPU cycles may well suggest the presence of cryptocurrency mining malware. Other possible symptoms include overheating (resulting in persistent fan activity or a notably hot device for phones and tablets), unexplained crashes or restarts, and inexplicably high volumes of network traffic. Of course, these could also be symptoms of *other* issues which may or may not be related to malware or other security problems.

Whatever happened to ransomware?

In recent years, ransomware might have been described as the *succès fou* of cybercrime. Opinions and estimates as to the 'market share' and financial impact of specific types of threat at any one time vary so widely as to be of debatable value. Still, there's little doubt that until recently the media and the public seemed to be more aware of ransomware than of any other current cyberthreats.

By early 2018, we were seeing cryptocurrency-mining malware described as 'the new ransomware'

Nevertheless, a slowdown would probably be noticeable if systems used for resource-intensive applications are covertly recruited for cryptocurrency mining, the more so if they're relatively underpowered systems like older games consoles and mobile devices. Does this mean that cryptominers will avoid such systems? Not necessarily. Cybercriminals don't usually care about conserving your resources, unless they're going out of their way to stay under the radar rather than have their efforts 'undermined'. Besides, as the frequent use of in-browser mining suggests, a given device can be useful even if it's neither high-powered nor available in the long term.

However, by early 2018, we were seeing cryptocurrency-mining malware described as 'the new ransomware', while ransomware attacks have attracted much less attention in the media. This doesn't mean, of course, that the ransomware epidemic has run its course, but, in particular, we see fewer stories about individuals losing data or having to pay ransoms. It's hard to say

whether this is due to a shift in media interest towards more novel, more "glamorous" malware topics, or a significant decline in ransomware attacks on individuals.

We do still see stories of large organizations attacked by ransomware, though. It is possible that this indicates less interest in 'mosaic' epidemiology, where malware spam campaigns result in many victims, each generating a small profit, in the hope that all those pieces of mosaic will add up to a substantial profit. Instead, there seems to be a trend towards small numbers of *highly profitable victims*. For instance, *it's been estimated* that those behind SamSam ransomware have been making around USD 330,000 per month by targeting enterprises and public sector organizations. Furthermore, there has been further diversification in ransomware circles into – for instance – *sextortion*.

Converging evils

There is, of course, no law of nature that says that malware cannot fit into more than one category. XBash is a recent example of convergent functionality, *reported* to have combined a surprising number of attributes:

- It can be described as ransomware, though perhaps pseudo-ransomware would be a better description, since there seems to be no way in which the gang behind Xbash could restore data to those victims who choose to pay up. This makes it functionally closer to the destructive class of malware we call a wiper, ransom demand notwithstanding.
- It is also described as combining this functionality with botnet, coin mining and self-propagation functionalities.
- It is multi-platform malware, capable of varying its payload according to whether it is executed on Linux or on Windows, and according to what services are available. But there are also, for instance, several third-party add-ons for Kodi *that are used* to distribute Linux and Windows coin miners. And yes, there are examples of cryptocurrency-mining malware that target macOS or Android, too.

Thirty years in the security business have taught me that sophistication and functional versatility are not necessarily indicators of a major trend, but may simply denote a transition between classes of threat, in the way that Melissa was both a high-water mark for macro viruses and an early warning of an incoming tidal wave of mass-mailers. Yet it's likely that — in the short term at least — cybercriminals will continue to hedge their bets with experimental malware that picks up profit wherever and however it can.

We can also expect to see more coin-mining software *attempting to remove* competing coin miners on compromised systems in order to get a higher-calorie slice of the processing pie.

How fat can you get by coin mining?

Research from the Technical University of Braunschweig's Institute for Application Security *suggests* that web-based cryptojacking is common, but only moderately profitable. Overall, however, the trend towards cryptojacking shows no sign of slowing down for the moment. ESET's Tomáš Foltýn reported recently that *one in every three UK organizations was hit by cryptojacking in April 2018*, while nearly two in three IT executives believed that their systems had experienced cryptojacking at some point.

An article by Phil Muncaster cites reports claiming that cryptomining increased by 956 percent in a year and that the number of organizations affected doubled in the first half of 2018, with the cybercriminals making an

Cryptomining increased by 956 percent in a year and the number of organizations affected doubled in the first half of 2018, with the cybercriminals making an estimated USD 2.5 billion in those six months.

estimated USD 2.5 billion in those six months. *Yet another report* asserts that illegal crypto-mining has increased at time of writing by 459 percent in 2018, attributing the increase to the use of *EternalBlue*. I think we can assume this upward trend will continue for a while yet, though I'm not sure how much of it we can blame on the NSA.

The Coinhive miner has been popular as an add-on to websites because it allows the site to "borrow" cycles from a visitor's system in order to mine Monero. However, it *quickly became popular* among cybercriminals, who took it to hack legitimate sites in order to run Coinhive scripts, configured to mine Monero for the hacker's benefit. More recently, Crypto-Loot has been adopted for similar purposes by, *notoriously*, Pirate Bay.

Conclusion: keeping your system safe

Not all the suggestions here are specific to cryptocurrency-mining malware (or ransomware), but will hopefully help with reducing the impact of other threats too.

- Security software helps against coin mining malware and other "poisoned apples". Not only as a means of avoiding all sorts of other malware, but specifically as means of detecting coin-mining malware in the form of executable files that can compromise your systems, and detecting or blocking coin-mining scripts in the browser.
- Such malware is often detected as 'Possibly Unwanted' or 'Possibly UnSafe' (see *this* and *this*), so make sure that your security software is configured to flag such apps.
- Despite the claims of some competing technology vendors, mainstream security software is capable of detecting many malicious processes in main memory or from scripts running on-server.
- Another recommended way of reducing browser-related risks is to install an *ad-blocker*, which has many other advantages... Or use a reputable script-blocker.
- Keep in mind that cryptocurrency miners often find their way in through vulnerabilities like EternalBlue, *which was patched* as far back as March 2017. Apply patches as soon as possible, whatever operating system you're running.
- There is always a risk that cyber-criminals will cause damage, even if it's unintended (as opposed to that inflicted by wipers and ransomware). So keep safe (offline) backups as discussed *here*.
- No product can detect everything. Sometimes common sense and caution will save you where technology fails.

2

MACHINES LEARNING, HUMANS ARE NOT

- Machine learning system
- Technology used to spread malware
- Practical limitations of machine learning

AUTHOR

Lysa Myers
ESET Senior Security Researcher

Machines Learning, humans are not

There is a *saying* that the three virtues of a great programmer are laziness, impatience and hubris. This idea is especially important to keep in mind when discussing the future of the malware landscape. It's also a good rule of thumb, when making cybersecurity predictions, to remember that (regardless of what side of the law one is on) people are trying to get a reasonable return on their investment of both time and effort. What can these rules teach us about the future of cybersecurity when it comes to adopting machine learning?

In regard to predicting how criminals might behave, we can safely say that in all but the most exceptional cases, they're trying to pilfer money or valuable commodities with minimal exertion. For most types of attackers, it's not worth the time or effort to develop or deploy the most bleeding-edge technologies if basic, automated attacks are providing what they want. This is certainly the most frequent scenario, and a significant problem for most people securing their homes or businesses.

Nation-state attackers will almost certainly be employing more complex tools to accomplish their ends. With a far more generous budget, that possibility should certainly not be discounted or ignored. Large organizations, especially those that are safeguarding industry-leading research or the personal information of millions of customers, need to be particularly wary of well-funded attackers. And at some point these more-complex tools will inevitably trickle down to the mainstream of malware operators.

For security practitioners, getting the best return on investment means trying to protect as much and as effectively as possible with a given budget, in terms of both money and personnel. For security product vendors, while budgetary concerns certainly exist, the more important factor is the need to optimize the solutions we provide to our customers so that the products detect as much as possible with the smallest cost to the customers in terms of processing power and any maintenance that must be done by human operators.

In this section we'll discuss how machine learning is used — and will continue to be adopted — by people on both sides of the equation; those who are attacking systems, as well as those defending them. We'll also discuss some of the practical limitations of machine learning, and where humans will still be crucial in the process of creating new tools to attack, as well as to defend, systems.

Employing machine learning to defend

The foundation of any good machine learning system is a large quantity of useful data. Without information from which to learn, machines do not have the raw materials necessary for generating effective rules for making decisions.

Regular readers of WeLiveSecurity will be familiar with the fact that security products have been using automation and machine

The systems used to identify suspicious files and behaviors now have a much deeper context and vocabulary to describe unwanted behavior.

learning for *quite some time*. This has been an important part of ESET's existing toolbox for over 20 years, and its prominence will undoubtedly increase as time goes on.

Researchers within the antimalware industry have been gathering and exchanging data about threats for several decades, so that we can maximize our ability to protect customers against malicious behaviors. For almost as long, we've also been in dialog with a wide variety of software vendors to gather data about the current state of *clean* files. This gives us a huge store of historical as well as current information with which to train machine-learning systems about what files and behaviors are considered suspicious, and what traits are more likely to indicate *benign* intent. This helps us identify problematic files and behaviors, while keeping false positives to a minimum.

When the anti-malware industry began, much of the work of threat analysis was done manually, and the amount of information that was stored was fairly basic. Early machine learning systems used traits of known-malicious as well as clean files to infer whether future samples were suspicious.

As the flood of new malware has grown, much more of the initial analysis work is done by automation, so that researchers can spend less time doing repetitive chores, and more time applying their expert insight to see and understand patterns within individual samples as well as between variants and entire malware campaigns. This automated work has drastically increased the amount and types of data that are stored about the *behavior* of individual samples, and improved our understanding of broader patterns in the threat landscape. Thus the systems used to identify suspicious files and behaviors now have a much deeper context and vocabulary to describe unwanted behavior.

The functionality of security products continues to expand, and the numbers and types of security specialists participating in information exchanges continue to increase. All this added information continues to improve both the depth and breadth of data that defenders are capturing about the evolving malware landscape.

Machine learning has a long history in the defense against malware and other security threats. The future promises a steady

increase in ways to identify problematic or anomalous behavior, not just at the file level, system level or the network level, but also across the internet as a whole.

Using machine learning to attack

As we previously discussed, the majority of malware attacks are implemented as simply as possible; there's no sense in finding new technologies or techniques if the old ones are bringing in a steady stream of illegitimate income. This will likely continue to be the case, as the low cost of entry into digital crime continues to invite additional "ethically-challenged" participants. Without a sea change in the way people understand and implement security, we can never ignore the impact of attacks against the low-hanging fruit of old vulnerabilities and gaps in basic security hygiene.

But as the market for cybercrime becomes more crowded, and more nation-states join the fray, this is likely to push some criminals into using more automation to make their creations more efficient. Cybercriminals are ***already using*** automated searches to assist in finding vulnerable machines and online accounts, and gathering massive amounts of disparate data for subsequent targeted reconnaissance. This automation will undoubtedly increase, to make their existing efforts more cost-efficient and better for social engineering attacks.

And as criminal organizations create more comprehensive databases, eventually they can be used to inform machine learning so that attack rules may be created that will make their campaigns more effective. There are three areas that seem most amenable to assistance by machine learning: target acquisition, exploiting victims, and guarding their resources from disruption.

Currently, reconnaissance automation seems to focus broadly on finding vulnerable targets. By adding better information to a database of vulnerable targets, miscreants can create a more detailed picture that will allow them to get more value from each target. Rather than asking for the cryptocurrency equivalent of a few hundred or a few thousand dollars in ransom from a target whose database is worth millions — where criminals are effectively leaving a significant amount of money on the table — they would be better able to assess the *most* a target would be willing to pay. And with better reconnaissance, they could be more thorough about exfiltrating *all* the valuable assets within a victim's organization, rather than just grabbing the first thing that looks interesting.

Social engineering has always been a fairly problematic area for criminals looking to exploit a chosen target, given the international nature of their efforts. We can all think of phishing or scam attempts we've received that had laughably bad grammar and spelling or that differed significantly from the sort of message one would expect from a source if it had not been badly spoofed. While some phishing and other fraud attacks have certainly improved their ability to mimic legitimate sources, many are still painfully obvious fakes. Machine learning could help increase effectiveness in this area.

Criminals have a model for how to improve the efficiency of their communications, in the existing example of targeted advertisements. While it's unlikely that they'll have the wealth of data that is stored by vendors that track people's regular shopping trips, miscreants could employ web-trackers that follow victims between sites or get information from data brokers to form profiles. This could make phishing and fraud attempts much more personal, and thus more compelling.

Miscreants could employ web-trackers that follow victims between sites or get information from data brokers to form profiles.

The most technically complicated approach — and thus least likely to become common in the short term — would be machine learning to help miscreants protect their infrastructure and evade detection more effectively. This would primarily entail making their command and control structure more resilient, and creating new malware variants.

How machine learning would affect the "arms race"

Since the discovery of the first files created with malicious intent, there has been an arms race between the creators and detectors of malware. Machine learning will not end this struggle. There are — and will always be — limits to the ways in which computers can be helpful in replacing humans as decision-makers. It should always be a relationship of mutual assistance, rather than one of total delegation of our responsibility.

The creativity of human developers (both benevolent and malevolent) will always necessitate the presence of human experts who can see when something falls well outside of previous patterns. It would allow those malicious individuals to gain the upper hand if we completely omitted *people* from the process of analysis for defense.

Many financially-motivated cybercriminals currently have a data-acquisition process that favors quick churn of information, as things like payment card details and login credentials tend to go stale quickly. But they have been moving their focus to more stable types of data, such as insurance and medical data, which retain their value for longer. It is likely that databases having a more permanent presence will become more detailed and thus more broadly useful for illicit ends. As their own resources become more stable and valuable, they may necessitate more advanced protection methods.

Ironically, this would cause the existing arms race to become less of a battle of one side primarily attacking and the other primarily defending, and more of parry-riposte.

In the end, what we're likely to see is a gradual increase in already existing trends; more and better machine learning to defend machines; and an increase in well-funded attackers passing their tools and techniques down into the mainstream of malware. While the power and importance of machine-learning systems should not be ignored by the defense, and probably won't be by the attackers, the fact is that it is not a silver bullet for either side.

Cybercrime is hugely lucrative for the majority of its perpetrators without their having to develop new-fangled tools, though we should *prepare as if* they will be deploying their most formidable weapons. And defensive security is sufficiently complex that not only will humans need computers to assist in identifying suspicious files and behaviors, computers will always need humans to help in identifying new types of weapons.

3

EU GDPR: THE FIRST STEP TOWARDS A GLOBAL PRIVACY LAW?

- Value of data privacy
- EU vs. US
- Privacy regulations on the rise

AUTHOR

Stephen Cobb
ESET Senior Security Researcher

EU GDPR: The first step towards a global privacy law?

For any company or consumer concerned about the privacy of personal information in the digital age, 2018 will stand out as being the year that the General Data Protection Regulation (GDPR) went into effect in the European Union (EU). Already, GDPR is having a big impact on digital privacy, not only in the EU, but also in the US, as well as other countries. This is a trend that will influence the cybersecurity landscape in 2019 and beyond.

The sound of inevitability?

Most corporate privacy officers had heard of GDPR long before it took effect. The language of the regulation was promulgated in 2015 and adopted in 2016 with a two-year post-adoption grace period. The GDPR "start date" that people focus on — May 25, 2018 — was the end of that grace period and the beginning of full enforcement by the EU.

By that time, most American businesses had at least thought about GDPR. If you attended any GDPR-related seminars or conference sessions in the US during 2017, you may have noticed that the question most frequently asked by American companies was: Does GDPR affect us? "Yes" was almost always the answer, for reasons summarized in a *2016 WeLiveSecurity article*. Companies must comply with GDPR if they:

- monitor the behavior of data subjects who are located within the EU, or
- are based outside the EU but provide services or goods to the EU (including free services), or
- have an "establishment" in the EU, regardless of where they process personal data (e.g. cloud-based processing performed outside of the EU for an EU-based company is subject to the GDPR).

So the second-most-common question in US discussions of GDPR was: How can we avoid it? The answers from consultants at firms like Deloitte, PwC, and KPMG, can be summarized like this: don't waste time with technical maneuvers intended to avoid GDPR — plan to align your organization's data strategies with GDPR, because some sort of GDPR equivalent is inevitable wherever you do business.

Data privacy goes big

The prediction of universal "GDPR-style" legislation was initially greeted with skepticism, but then the California Consumer Privacy Act (CCPA) of 2018 burst onto the scene. In fact, the CCPA was signed into law less than 40 days after GDPR came into effect and affirms that, when it comes to businesses handling their personal information, Californians have the right to:

- know what personal information a business has collected, acquired, or derived about them
- access, transfer, or delete personal information held by a business
- know whether or not their personal information is sold or disclosed by the business, and if so, to whom

Plan to align your organization's data strategies with GDPR, because some sort of GDPR equivalent is inevitable wherever you do business.

- forbid the sale of their personal information by the business
- receive equal service and price from the business, even if they exercise their privacy rights.

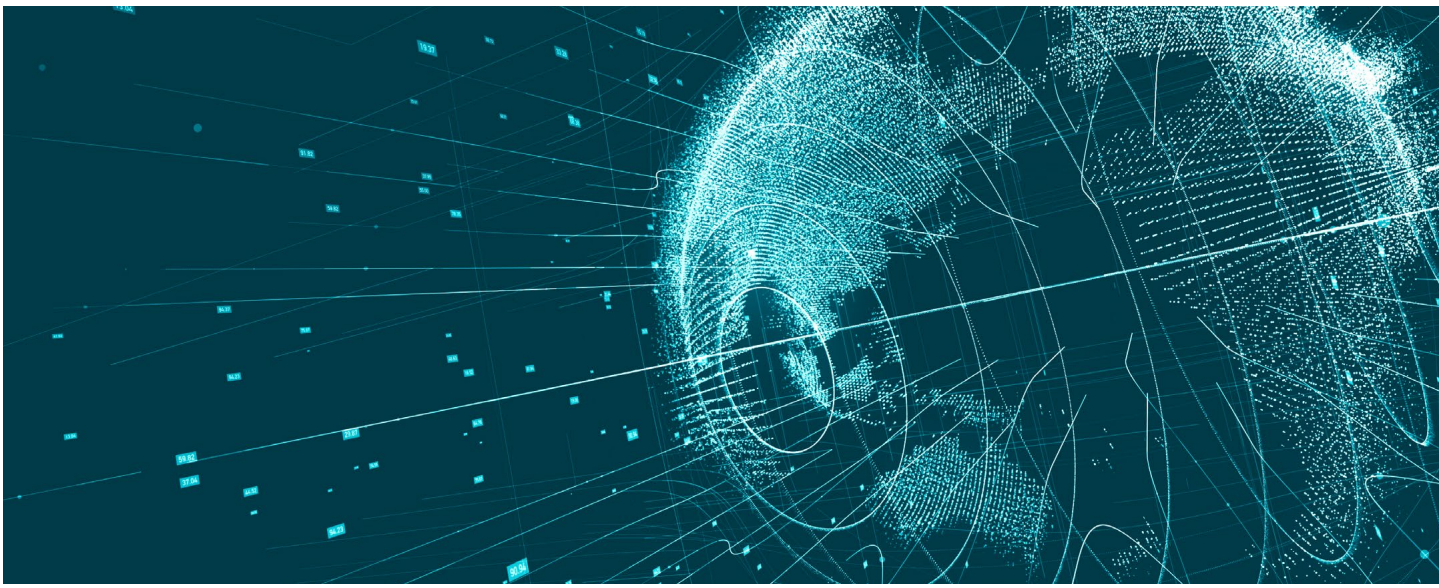
While the manner in which these rights are spelled out *in the CCPA* includes numerous exceptions and limitations, there is no doubt that it marks a huge shift in the privacy landscape in the Americas.

Although California is just one of the United States of America, it would be the *fifth largest economy in the world* if it were an independent country (right behind Germany, Japan, China, and the rest of the US). That makes California very influential in terms of both law and business practices.

and forbids the collection or use of personal information about EU residents without their knowledge and *permission*.

In the US there is no explicit constitutional right to privacy, so sensitive information about you can be collected and used by companies unless a law or lawsuit says it cannot. Here is an example of what that means:

> Suppose you start a business that offers an app-based "rideshare" service such as Uber. Your firm collects data about people who use the service, including names and details of their trips. If your rideshare business is in the EU there are laws restricting what it can do with that data, even if there are no privacy laws specific to rideshare services.



The privacy divide

To understand how California's adoption of GDPR-style protections for personal data might impact the privacy landscape in 2019, we need to look at how the EU and US have handled privacy so far. The EU Charter of Fundamental Rights contains an explicit right to the protection of personal data

In the US, the answer to "What can my rideshare business do with the personal information it collects?" is usually "it depends". The variables include where the business is incorporated and where it operates, but the answer often boils down to ..."Whatever you can get away with." And that may remain the situation until either there is a lawsuit or a *privacy law* is passed to regulate the use of personal data collected by rideshare firms.

In other words, the US has different protections for different types of personal data, created in different ways, at different times. For example, the Video Privacy Protection Act of 1988 was drafted and enacted within days of the video rental records of a Supreme Court nominee being leaked to a newspaper.

What privacy protections there are in the US come from federal law, state legislation, or court decisions at either the state or federal level. (For more detail on US privacy law see the ESET white paper: *Data privacy and data protection: US law and legislation*.)

In the EU, data that pertain to you as an identifiable individual are protected, by default, from inception. That is the practical meaning of the term "data protection" in European usage. Anyone who wants to collect data pertaining to you is required by law to get your permission to do so, and when they have your data they are required to exercise tight control over who can have access it and for what purpose. That applies to new forms of personal data as soon as they come into being, so you don't have to wait for a lawsuit or an embarrassing political incident.

Rising tide of privacy regulations

So how, without a foundational data privacy law in the US, can a single state make a difference in privacy protection? It's all about affluence, influence, and envy. California is America's richest state and can afford to pioneer rights that may be harder to establish in other states. That paves the way for other states, residents of which will probably envy Californians if they have better privacy protections than their own state provides, just as many Americans are increasingly envious of Europeans' rights under GDPR.

History also plays a role: the first step towards the CCPA of 2018 was taken back in 1972. That's when California voters amended the state's constitution to include privacy among the "inalienable" rights of all people (each US state can have its own constitution, in addition to the federal constitution). Just five years later the state passed the Information Practices Act of 1977 to limit the collection, management, and dissemination of personal information by state agencies, a move prompted by the growth of data processing within government departments.

Twenty-five years after that, in 2002, when internet-based business models began expanding the collection of personal information and also increased the risk of unauthorized disclosure, California implemented the first state law mandating data breach notifications. Fast-forward 16 years to 2018 and all 50 states in the US have a breach notification law, strongly suggesting that other protections, like the GDPR-style data privacy rights enshrined in CCPA, will also spread across the US.

There are counter-arguments to this prediction, not least of which is the ongoing fight to amend the CCPA before it goes into effect in 2020. To counter that, privacy advocates are keeping up the pressure on legislators (the pro-CCPA movement has its own website, a strategy that could easily be adopted in other states).

The challenge for companies that think the CCPA will hurt their business is this: how do you convince consumers/voters that they need less privacy protection than people in other countries? Dismissing privacy rights and data protection as "just an EU anomaly" is hard when that anomaly is about to become law in the US state that is home to digital giants like Google, Facebook, Apple, HP, and Oracle. These companies operate globally, and the global trend is clearly set toward GDPR-style privacy, not away from it.

Dismissing privacy rights and data protection as "just an EU anomaly" is hard when that anomaly is about to become law in the US state that is home to digital giants like Google, Facebook, Apple, HP, and Oracle.

The largest country in Latin America — Brazil — adopted a new General Data Protection Law (LGPD) in 2018 to replace a sectoral privacy framework that was akin to what the US has today. According to *global legal analysts*, "Brazil's LGPD echoes many of the components of the GDPR." Furthermore, the LGPD will help Brazil achieve "a reciprocal adequacy finding from the European Commission *similar to the one Japan received*." So yes, another major economy — Japan — is moving toward EU levels of privacy protection. As is China, and although China's internal control of the internet *is a complicating factor*, the fact that one of the world's largest processors of data is developing the skills and technology to handle data in a GDPR-compliant manner is clearly significant.

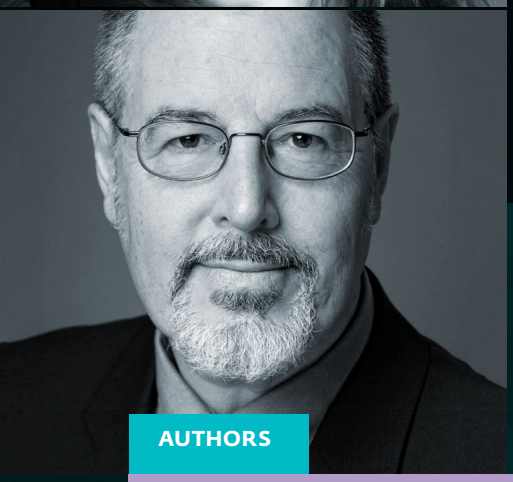
The privacy divide

A basic goal of cybersecurity is to control access to information so that it does not suffer unauthorized exposure. One goal of privacy regulation is to influence the way in which "unauthorized exposure" is defined with respect to personal information, and then spell out the consequences for organizations when they permit such exposure to occur. Consequently, a data breach may do more than damage the trust that people place in an organization — as is discussed in the "*Trends 2019: Privacy Reloaded*" section — it could also prove costly if the breach, and/or the handling thereof, violates privacy regulations.

In October of 2018, the *European Data Protection Supervisor announced* that the world could expect the first GDPR fines "for some cases by the end of the year." At about the same time, the Irish Data Protection Commission began to investigate Facebook for a breach that "*could result in a fine of up to $1.63 billion*". As the impact of GDPR becomes clearer — and more real — in 2019, we predict that many companies will be busy preparing to comply with the CCPA and any similar legislation around the world.

4

PRIVACY RELOADED: WILL IT DECIDE WHO STAYS IN BUSINESS?



- Vulnerabilities and bugs exposed millions
- The Facebook test
- New privacy models

AUTHORS

Lysa Myers & Stephen Cobb

ESET Senior Security Researchers

Privacy reloaded: Will it decide who stays in business?

The number of people whose digital privacy was placed in jeopardy by some sort of data security issue in 2018 probably passed the two billion mark before the end of the third quarter. If that number sounds inflated, remember that just five organizations had exposed almost 1.8 billion records before the middle of the year: *Aadhaar*, *Exactis*, *Under Armour*, *MyHeritage*, and *Facebook*. Indeed, 2018 could fall short of the 7.8 billion records exposed in 2017, or even the previous all-time high of 6.3 billion in 2016.

What may be more interesting about 2018 is that many of the year's privacy gaffes do not neatly fit the common perception of "breach". Whereas most of us think of a breach as attackers breaking into a system in the hope of stealing information, it is not always clear that many of 2018's privacy problems were the work of an attacker. Some of these problems were the result of vulnerabilities or bugs that allowed unintended access, such as the Facebook issues that put at risk the *accounts of 90 million users*, or the bug in *Google+* that exposed the accounts of over half a million users (and contributed to the demise of that platform).

Sometimes privacy problems are produced by products or services behaving as designed, and as they're described in License Agreements, but in ways that turn out to be absolute privacy nightmares. Two examples of this problem are Facebook's *Cambridge Analytica data scandal*, and its data-sniffing *Onavo VPN*. The unintended consequences of sharing aggregated data made headlines from the very beginning of 2018, with the *Strava heat map kerfuffle*.

So what are the implications for 2019? A lot will depend upon two big players: Facebook and Google. Between them these companies have amassed mammoth user bases, along with truly staggering amounts of personal data about those users, and that has to be protected from unauthorized access. People are now wondering if these companies have, in a social sense, become "*too big to fail*".

Facebook and Google have developed very powerful platforms. These platforms have the potential to connect a lot of people for the purposes of sharing and spreading information, for both good and ill. As a result, a lot of people have come to depend on using Facebook and Google products. Anything these platforms do that makes it too risky or dangerous for specific individuals to use the platform has a way of effectively alienating those people.

In other words, from a social perspective, expecting people to choose not to participate in any functionality that is offered by Facebook or Google would be akin to choosing to avoid participation in modern life. While it might theoretically be possible to completely eschew both, to do so these days would be such a hurdle to doing ordinary things in business or personal life that most people would consider it too much of a hardship.

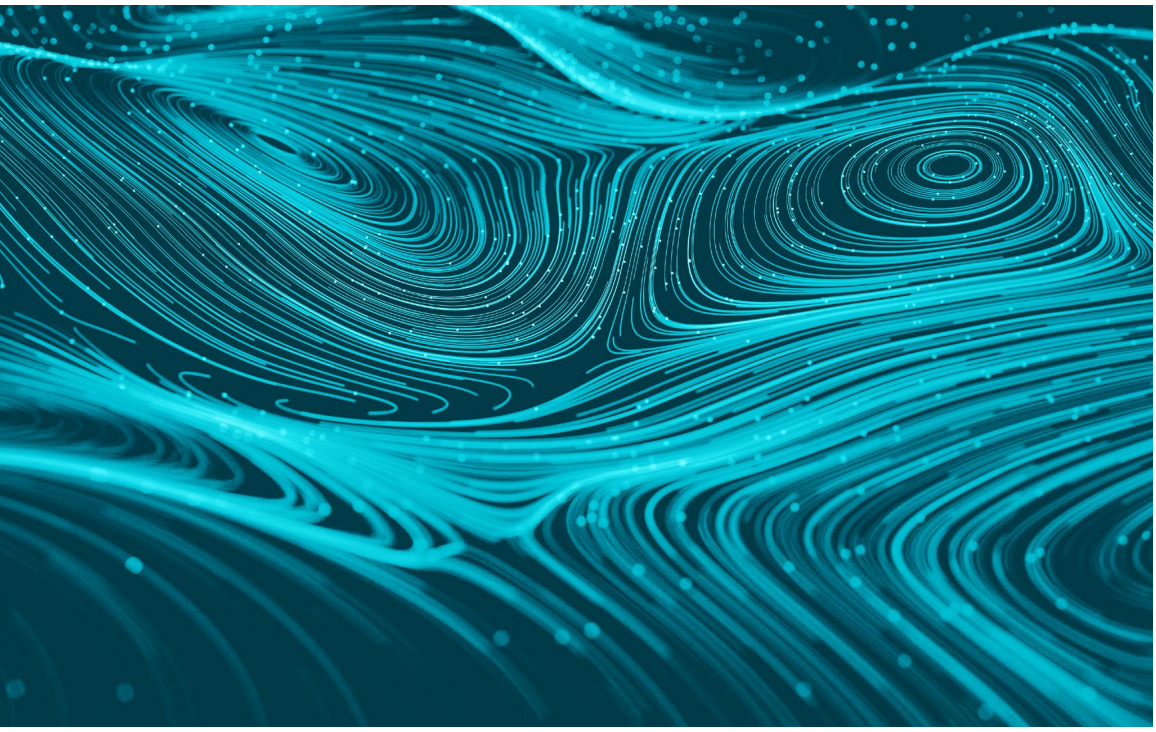
Pushing forward or over-reaching?

People are clearly still using Facebook in massive numbers despite two big data-privacy blunders in 2018, but the feelings of many users have soured in ways that are difficult to capture with statistics. Instead of Facebook being a place where people look forward to connecting and sharing stories with their family and friends, for some it has become a place that people can't leave without losing contact with family and friends.

While it may be that people are leaving the Facebook website with a bad taste in the mouth, they're not completely abandoning the Facebook ecosystem.

Consider the Facebook Portal device for making video calls, set to debut late in 2018. This could prove to be an interesting test of public sentiment towards the company in 2019. As far as privacy is concerned, virtual assistant devices can be described as, at best, a mixed blessing for privacy, which is to be expected whenever we put a devices with an always-on microphone in our private abodes.

Fewer people are spending time and money on Facebook, but they're spending more on Facebook-owned properties like Instagram, WhatsApp and Messenger.



A number of recent studies have shown a decline in Facebook usage, engagement and ad revenue, which has been accelerating for the last several years. But if you look further into this information, there are some rather large caveats. For example, while fewer people are using the service via a desktop web browser, more are doing so via the mobile app. Fewer people are spending time and money on Facebook, but they're spending more on Facebook-owned properties like Instagram, WhatsApp and Messenger.

The virtual assistants that power the most popular "smart speakers" — Alexa, Google Assistant, Siri and Cortana — have been around and widely available for a number of years. That means they're well-tested, popular and probably fairly well-trusted. The challenge the Facebook Portal will face in 2019 is that Facebook's own recent privacy gaffes may make it hard for this device to earn a similar level of trust. And several analysts have noted that launching a surveillance device within days of exposing

many millions of users' accounts suggests Facebook is somewhat tone deaf to the privacy concerns of its users.

If Facebook truly begins to falter, it may be because it seems to keep putting resources into taking advantage of people's dependence on its platform, without apparently realizing that they are losing their users' trust.

It's long been known that breaches and other privacy problems can have serious financial impact, even on very large companies. Just take a look at what happens to the price of shares in a publicly traded firm when a privacy breach is made public. Stock of the credit reporting company Equifax – another huge repository of personal information – dropped 30% in the wake of its data disaster in 2017 and even 12 months later it has not fully recovered. Facebook is in a slightly different position because its customers are not its users, but its advertisers. That said, user distrust may have a knock-on effect if Facebook advertisers see less value in the platform as a means of pushing product.

Defensive diversity and new privacy models

Companies that are so interwoven into our daily lives have something of a captive audience. Will 2019 be the year that mega-companies finally demonstrate they have taken privacy seriously enough that there are no significant privacy breaches? That is not clear, but there is no doubt that 2018 was a year in which many people were forced to consider the dangers of having a mega-business as the portal to their entire internet existence.

What we may see as a trend in 2019 is more people searching for alternatives to the platforms currently dominant, in an effort to diversify their own personal online ecosystems. This diversification has two primary benefits: digital "biodiversity" and maintaining segregated digital "zones". Achieving a frictionless flow of information between every connected person and entity sounds great, as might the idea of using the credentials from one platform to access all your online accounts everywhere. However, the downsides can be hard to predict and are potentially huge.

As a biological example, consider the banana. The Cavendish banana is so ubiquitous that if you say "banana", the image that immediately comes to mind for most people is this standard, yellow clone. Bananas bought in Finland or in Florida will be genetically identical to one another. But for how long?

Cavendish bananas have been teetering on the edge of the fungal disaster that doomed its predecessor, the Gros Michel. Much of the reason that store-bought bananas are such a precarious crop is because there is no genetic diversity to help its plant population withstand disease and other disasters. Once an area is infected with the pathogenic fungus, it stays in the soil for upwards of three decades, so susceptible bananas can no longer be grown there. The only thing that has allowed us to keep the Cavendish banana as a viable crop is establishing biosecurity procedures that keep different plantations separate — not just geographically, but on a microbial level.

By comparison, consider the plight of frogs and toads that have been affected by the *chytrid fungus*; different amphibian populations around the globe were similarly being affected by a fungus that was often transported by humans. There were similar concerns that this pathogen would wipe out species worldwide, if the advance of the threat was not halted. Because these frogs are not clones, but genetically different, they have a variety of genes to help them

What we may see as a trend in 2019 is more people searching for alternatives to the platforms currently dominant, in an effort to diversify their own personal online ecosystems.

adapt to threats. Frog and toad populations have started to develop resistance to this threat; individuals are now surviving in spite of being infected.

A homogenous population or ecosystem — either in the world of molecules and microbes or in the realm of digits and data — creates the potential for widespread risk when a threat appears. If we diversify our digital ecosystem, both individually and as a population, we will decrease risk and make it easier to recover when there are problems. For example, having a single sign-on that links many of our online accounts means that when a threat is found anywhere in this environment, it's a risk to all of those accounts. While it is potentially less convenient to have to put our metaphorical eggs in different baskets, we also stand to lose less if one of those baskets is overturned.

Summary

In 2019 we may see both greater platform diversity as people shy away from places that have proven to be insecure, and a continued decrease in trust and engagement with existing platforms. We may even see some companies and/or product offerings fade away because of concerns around trust and privacy. Also, as the year unfolds, bear in mind that consumer fears are not the only privacy driver at work. Consider the regulatory risk scenarios described in *Trends 2019: GDPR*. The GDPR may not be the only source of sanctions hitting companies in 2019 if they don't get privacy right. Already, other localities — most recently *Brazil* and *California* — have passed similar legislation, and it's unlikely they'll be the last.

5

HOME ASSISTANTS: WHEN YOUR APPLIANCE NEVER SHUTS DOWN

- Attacks continuing at pace
- Usability and security aligned
- Securing data moving forward

AUTHOR

Camilo Gutiérrez Amaya

ESET Senior Security Researcher

Home assistants: When your appliance never shuts down

Considering the electronic devices you use on a daily basis, which of them would you say are the most important? Did you think of your internet modem or router? These devices tend to be nothing more than a little black box in a corner of our homes, but have become critical objects — as important as our computers or cell phones for activities that require internet connectivity.

This is because, in addition to providing access to the internet, much or even all of the device user's sensitive information passes through these devices, and if not kept updated correctly, cybercriminals may commandeer them and then compromise other devices connected to them. Thus, once compromised, these devices can become an attack platform that serves as a bridge to access other devices on the same network.

However, these are not the only devices that collate information from other electronic equipment. Recently, *virtual assistants* (home assistants, voice assistants) have started to gain in popularity, as well as to be connected to various devices, which they actually have the power to control, as is the case, for example, with smart lighting, sensors, cameras, and even household appliances. And as the array of interconnected devices increases, so does the attack surface.

According to an IDC report, the number of internet-connected smart devices is expected to grow *to 80 billion by the year 2020*. In 2019 we expect to see a corresponding increase in the number of attacks, which will employ a range of methods, from automated scripts targeting vulnerabilities in IoT devices, to exploits designed to take control of them. As routers and home assistants are the kinds of equipment that interact most with other smart devices as well as the internet, they are likely to be the primary targets for attackers.

Growth in attacks

Unfortunately, it is not possible to determine by how much the attacks will increase in 2019. There is no doubt, however, that we will see more cases of attacks developed specifically for these devices, as illustrated by the 100,000 device *BCMUPnP Hunter* spam-sending botnet, spreading via a five-year-old vulnerability in Broadcom chips used in at least 116 different device models that was discovered as this article was being prepared for publication. We can also expect to see an increase in the variety of attacks aimed at devices that operate as *hubs*, just as routers or home assistants do, as these are the kinds of equipment that can give an attacker access to an entire network, along with all the other devices connected to that network and, most important of all, to the data they manage.

We cannot lose sight of the fact that during the last few years we have witnessed different types of attacks on routers, such as the "Carna botnet" and its "*Internet census in 2012*", as well as other smaller-scale events that happened prior to Mirai. In fact, it could be argued that Carna was the precursor of the *Mirai botnet*, and although it did not have the malicious intention of the latter, Carna managed to engage several and diverse devices such as SOHO routers. The case of the Mirai botnet was one of the most popular. Com-

posed mainly of compromised IoT devices (it has infected 600,000 devices around the world), it has been used to carry out tens of thousands of DDoS attacks; *including one of the largest in history* in October 2016 attacked when the servers of Dyn suffered an attack that caused disruption to popular services such as Netflix, Twitter, Spotify, and PayPal, as well as several media outlets in the United States and Europe. Studies have also been carried out recently into voice assistants, one of which demonstrated that it is possible to *send hidden commands, which are not detectable by the human ear*, to assistants such as Apple's Siri, Amazon's Alexa, and Google's Assistant. Such commands can direct these systems to make expensive international calls, open websites, or control other devices (change the thermostat setting, etc.) without the owner realizing it is happening.

While many of these studies were initiated as proofs of concept, they demonstrate that it is possible for an attacker to unlock devices, make bank transfers, or make online purchases simply by concealing malicious messages in the playback of a normal audio file.

This means we have a challenge to face in the future, as protecting these hubs throughout our connected world will not be easy. For example, a malfunction in one of these components or an attack making use of them as a platform could lead to information being compromised on many different devices.

While the usability and convenience that smart devices deliver are highly valued, they can also act as an open door through which threats can enter. The reality is that as we continue to progress toward greater adoption of the use of IoT devices grouped together and controlled via a home assistant, the risks to our security and privacy increase. We must not lose sight of the fact that as technology evolves, so too does the way cybercriminals think and act.

The balance between usability and security

If you already have smart devices or are thinking of getting one, you need to consider what increased level(s) of security risk it imposes. In February 2018, ESET researchers published a *report on an analysis of twelve popular IoT devices available for sale* and as well as finding a variety of vulnerabilities (some of which were serious), every single one of the devices analyzed presented some kind of problem in terms of privacy, the greatest worry being around the behavior of the smart assistants. Consequently, it is important to look into the features offered by each device and manufacturer, whether an adequate balance between convenience and security is feasible.

While the usability and convenience that smart devices deliver are highly valued, they can also act as an open door through which threats can enter.

So, if you are thinking of buying an Alexa-powered gadget (one of Amazon's, a Facebook Portal, or some other third-party device), Google Home, Apple HomePod, or any similar service at some point in the next year, above all you need to understand what personal data they capture and share, and thus work out which is the best and most suited to your needs for security and your expectations of privacy.

The same attacks we have seen so far on the internet are going to move to targeting devices with fewer security features. It is therefore necessary to consider everything from the physical location in which these devices are placed to the models we choose, ensuring they offer the best encryption or have solid authentication. These measures need to be taken into account because we are still a long way from having security standards for the IoT.

So, 2019 presents us with quite complex scenarios with regard to the threats we may see when addressing these technologies, and while there may be a great many concerns around security and privacy, now is the time when we as users need to take protective measures and not ignore these issues, or leave it to the manufacturers to address them.

Security needs to be focused on data

What should security be focused on for 2019 in relation to devices such as home assistants? The most important thing in terms of security is to know what data are exchanged and collected by these devices: ID information, data providing access to online profiles, financial information, and, in general, *all* data that could be sensitive. The wide range of devices, technologies, protocols, and providers makes it difficult to imagine how we could easily achieve a standardized range of secuirty measures that could be adopted. This is a process that will take time and we are not going to see any such standards implemented within 2019.

Therefore, until we reach that point, manufacturers need to dedicate themselves to implementing security policies within the application layer of their products that will increase the protection and confidentiality of data. Otherwise, we will see more attacks in which code is injected so that vulnerabilities can be exploited.

What does the future have in store?

At present, we are seeing an expansion of the attack surface, with cases where attackers have accessed systems that use a wide range of technologies and communication protocols. In parallel with this growth, throughout 2019 we will see threats utilizing different attack vectors, taking advantage of the wide variety of options available.

We have already seen how cybercriminals have used IoT devices to launch major denial of service attacks (DoS), but as more devices become connected and incorporated into everyone's lives, attackers will continue to explore their characteristics in order to discover other vulnerabilities (they've already done it with thermostats, video surveillance systems, kid toys, vehicles, etc) and use them to implement threats like scams, ransomware, and cryptocurrency mining more widely via these devices. With the increase in the adoption of cryptocurrencies and the number of devices connected to the internet, smart devices could become the entry point for attackers to build cryptomining farms.

The same attacks we have seen so far on the internet are going to move to targeting devices with fewer security features.

Some people are showing concern about this situation and are already taking measures. One example of this is the approval of *a new law in California* which, starting in 2020, will require all IoT devices to be sold already set up with unique passwords.

In light of the aforementioned discouraging security concerns, as users we need to know about the devices we buy, the features offered by manufacturers, and above all, we need to know how to use the technology securely. The reality is that a wide range of manufacturers, in the frenzied race to sell their products, may launch many devices with vulnerabilities that leave them even more exposed. For this reason, being aware that there are risks is the best way to be prepared, so that you may then take action to protect not only your devices, but also the information that passes through them.

CONCLUSION

2018 was a year in which the importance of data privacy came sharply into focus. Specific cases like the revelations regarding the mishandling of Facebook users' data by Cambridge Analytica, and the coming into force of the General Data Protection Regulation (GDPR) were largely responsible for making data privacy and security such a big talking point.

The various sections of this report have shown the importance of customer data to companies, to individuals, to the people who protect those data, but also to cybercriminals.

As we have seen, the evolution of threats reflects both the evolution of technology and the behavior of computer users. In the same way that marketers seek to gain a better understanding of the ways in which potential customers behave online in order to engage in more personalized advertising, attackers will probably start using technologies like machine learning as part of their efforts to collect data that can then be used to carry out social engineering campaigns that are more personalized and therefore more convincing.

In this digital age when all the online activities in which we engage leave tracks, and when we will undoubtedly keep seeing privacy-related incidents that affect both companies and individuals, the implementation of the GDPR is a beacon of light for the world, which has already begun to be replicated in different countries and regions through various data protection initiatives. And while the GDPR generated many questions within the business sector, particularly in countries outside the European Union, the events of this year seem to have brought about a change in our way of thinking — a change which until now had remained unattainable. Will it be enough? Probably not.

The following scenario, in which data protection regulations are emerging, presents a new challenge: How can the new standards that emerge in each region or country work alongside those of other countries, considering that the very nature of the internet involves a lack of regard for geographic borders? It also raises other questions, such as what will happen when two rules conflict with each other or when there are gaps in legislation failing to address unanticipated scenarios. There is a need to establish rules, but also a system that keeps track of new requirements as they emerge and anticipates evolutionary advances so the rules can be updated over time. Now is the time when companies and governments must demonstrate their commitment and not leave everything in the hands of security companies or individual computer owners, as is the case now.

As technological advances are made, the attack surface increases and so another challenge is to provide computer security education in various areas and for various audiences. In a world crisscrossed by interconnectivity, where all services are linked up in the cloud, where all home assistants, routers, and other smart devices can act as doorways for stealing information, or where a website can be infected by malicious code to mine cryptocurrencies. There is more need than ever for consumers to be more attentive and be better equipped to use technology responsibly and conscientiously, not only to know how

to protect themselves but also to know about liability and the risks involved in uploading personal information to the cloud, and to be aware of what kind of information they are uploading and sharing with legitimate internet services.

Meanwhile, organizations, companies, and manufacturers will need to play their part if they do not want to be affected by their customers losing trust in them as a consequence of being impacted by a security incident. Even companies like Facebook, whose main value is the service it offers built on the processing of large volumes of personal information, is no longer perceived by its users in the same way as before.

The reality, though, is that not all companies will have a second chance to demonstrate that the protection of such information is a priority for them. It could just take one incident in which their customers' personal data are compromised for those customers to lose trust completely, resulting in the service disappearing or the company going bust.

As 2019 gets underway, the issues will continue: there will still be security breaches, devices leaving factories without sufficient security controls, and sophisticated malicious campaigns affecting critical infrastructure. Alongside these issues, people's inboxes will still be hit by phishing campaigns that typically try to take advantage of those of us who are not cybersavvy — or suspicious, or even just plain lucky — enough to use technology prudently. Considering this array of different forms of attack and their inherent complexities, there are many different areas in which the various members of society (companies, individuals, manufacturers, governments, Independent social groups are responsible for ensuring that data privacy and confidentiality are maintained.

We hope this report is useful to everyone involved in decision-making and that we all can work together to enjoy safer technology.

www.eset.com