CYBERSECURITY TRENDS 2018: THE COST OF OUR CONNECTED WORLD

ENJOY SAFER TECHNOLOGY™

INDEX

INTRODUCTION

A year of cybersecurity headlines

In the Cybersecurity Trends 2018: The Cost of our Connected World report, ESET security experts present the areas that they expect to be leading security priorities in the upcoming year and suggest ways to mitigate the possible risk that they pose. Our writers will be covering ransomware, attacks on critical infrastructure, the power of malware analysis for combating criminal activity, the cyberthreats posed to electoral campaigns, and how privacy will look in 2018.

Before that though, let's take a brief look at what happened in 2017 as it will go down in history as an unfortunate moment in time for our digital world. It was the year when security – or the lack thereof – made the headlines and then took up permanent column 'inches' in the mainstream global media. If you run through the year's biggest cybersecurity incidents, you'll see a number of high-profile cases that not only had an impact upon millions of users worldwide, but also delivered a significant financial blow to major multinational companies and government agencies.

Two of the attacks that stood out most during 2017 were undoubtedly, the widespread ransomware infections: WannaCryptor (known as well as Wannacry), which was followed by DiskCoder.C. The "worm-like" capabilities of these threats meant that data on thousands of endpoints and servers around the globe was attacked on both at unprecedented scale and speed. Furthermore, these ransomware attacks generated significant concern about security issues among a far wider cross section of people.

These attacks were not the only incidents to gain the attention of the mass media. Take the Equifax breach, for example, which may very well have affected more than half of the adult population in the United States as well as many people outside the US, or the attack on HBO in which private information about its actors was leaked along with production-related materials such as scripts and episodes of the "Game of Thrones" series. Even Yahoo! has admitted, albeit just this year, that its entire user database was compromised during a 2013 breach, meaning that data from three billion accounts – including names, email addresses, dates of birth, passwords, and in some cases, security questions and answers – were compromised.

And that's not all. Over the past year, there have been plenty of speculation that the 2016 presidential elections in the United States may have been interfered with. Then there was the discovery of KRACK, a threat to the WPA2 encryption system, which may compromise the security of Wi-Fi connections.

Last, but certainly not least was Industroyer, the biggest threat to industrial control systems since Stuxnet. Industroyer displayed the capability to affect various types of critical infrastructure including water, electricity and gas supplies.

Without a doubt, this has been a busy year in terms of security. Several concerns identified by ESET security experts, and raised over the last few years in our annual Cybersecurity Trends report, unfortunately, came to pass in 2017. This is highlighted by the fact that cybersecurity incidents are becoming increasingly prevalent across all

areas of our daily lives and the events reported now impact a much broader and more diverse spectrum of the global population than ever before.

Technological advances and their accelerated use have led to a number of scenarios considered unlikely just few years prior, are now within the realm of possibility. This becomes increasingly apparent as we discover impacts to security that can be traced back to the fact that several systems and the protocols we use on a daily basis were designed without taking into account the prospect of (widespread) internet connectivity. How then do we solve this paradox without downgrading our technical capabilities?

This brings us back around to Cybersecurity Trends 2018: The Cost of our Connected World report. While our writers can never say for certain that the issues covered in the following articles will come to pass – we certainly wish for a less turbulent year in the cybersecurity world. We as well hope that this report will help readers become more aware of the problems that may occur.

We are optimistic that a forward-thinking exercise such as Trends 2018 will enable all those involved with, and concerned about, cybersecurity to contemplate, discuss, and counter current challenges and those to come.

1

The ransomware revolution

- Wormable ransomware
- Global outbreaks
- ‚Ransom' without ‚ware'
- Others types of ransomware
- RaaS: Ransomware as a Service

AUTHOR

David Harley
ESET Senior Research Fellow

The ransomware revolution

This is actually where I came in, nearly 30 years ago. The first malware outbreak for which I provided consultancy was Dr. Popp's extraordinary AIDS Trojan, which rendered a victim's data inaccessible until a 'software lease renewal' payment was made. And for a long time afterwards, there was not much else that could be called ransomware, unless you count threats made against organizations of persistent DDoS (Distributed Denial of Service) attacks.

All-too-plausible deniability

While Denial of Service attacks amplified by the use of networks of bot-compromised PCs were becoming a notable problem by the turn of the century, DDoS extortion threats have accelerated in parallel (if less dramatically) with the rise in ransomware in the past few years. However, statistics may be obscured by a reluctance on the part of some victim organizations to speak out, and a concurrent rise in DDoS attacks with a political dimension rather than a simple profit motive. There are other complex interactions between malware types, though: there have been instances of ransomware variants that incorporated a DDoS bot, while more recently the charmers behind the Mirai botnet chose to DDoS the WannaCryptor (a.k.a. WannaCry) "kill switch" in order to allow dormant copies of the malware to reactivate.

The worm turns

Of course, there's a great deal more to the malware ESET calls Win32/Filecoder.WannaCryptor than the Mirai factor. The combination of ransomware and worm accelerated the spread of the malware, though not as dramatically in terms of sheer volume as some of the worm attacks we saw in the first decade of the millennium, partly because its spread was reliant on a vulnerability that was already widely patched. However, its financial impact on major organizations caught the attention of the media worldwide.

Pay up! and play our game*

One of the quirks of WannaCryptor was that it was never very likely that someone who paid the ransom would get all their data decrypted. That's not unique, of course: there are all too many examples of ransomware where the criminals were unable to recover some or any data because of incompetent coding, or never intended to enable recovery. Ranscam and Hitler, for example, simply deleted files: no encryption, and no likely way the criminal can help recover them. Fortunately, these don't seem to have been particularly widespread. Perhaps the most notorious example, though, is the Petya semi-clone ESET detects as DiskCoder.C, which does encrypt data. Given how competently the malware is executed, the absence of a recovery mechanism doesn't seem accidental. Rather, a case of 'take the money and run'.

Wiper hyper

While the DiskCoder.C malware sometimes referred to as NotPetya clearly doesn't eschew making some profit by passing itself off as ransomware, other

'wipers' clearly have a different agenda, such as the (fairly) recently revived Shamoon malware. Malware with wiper functionality aimed at Ukraine include KillDisk (associated with BlackEnergy) and, more recently, one of the payloads deployed by Industroyer.

What can you learn from these trends?

Holding your data to ransom is an easy way for an attacker to make a dishonest profit, and destroying data for other reasons such as a political agenda seems to be on the rise. Rather than speculate about all the possible variations on the theme of data mangling, let's look at some measures that reduce the risk across the board.

1. We understand that people choose to pay in the hope of getting their data back even though they know that this encourages the criminals. Before paying up, though, check with your security software vendor (a) in case recovery may be possible without paying the ransom (b) in case it's known that paying the ransom won't or can't result in recovery for that particular ransomware variant.

2. Protecting your data proactively is safer than relying on the competence and good faith of the criminal. Back up everything that matters to you, often, by keeping at least some backups offline – to media that aren't routinely exposed to corruption by ransomware and other malware – in a physically secure location (preferably more than one location). And, obviously, backups defend against risks to data apart from ransomware and other malware, so should already be part of a disaster recovery plan.

3. Many people and organizations nowadays don't think of backup in terms of physical media like optical disks and flash storage, so much as in terms of some form of cloud storage. Which are very likely to be offsite, of course. Remember, however, where such storage is 'always on', its contents may be vulnerable to compromise by ransomware in the same way that local and other network-connected storage is. It's important that offsite storage:
   a. Is not routinely and permanently online
   b. Protects backed-up data from automatic and silent modification or overwriting by malware when the remote facility is online.
   c. Protects earlier generations of backed-up data from compromise so that even if disaster strikes the very latest backups, you can at least retrieve some data, including earlier versions of current data.
   d. Protects the customer by spelling out the provider's legal/contractual responsibilities, what happens if the provider goes out of business, and so on.

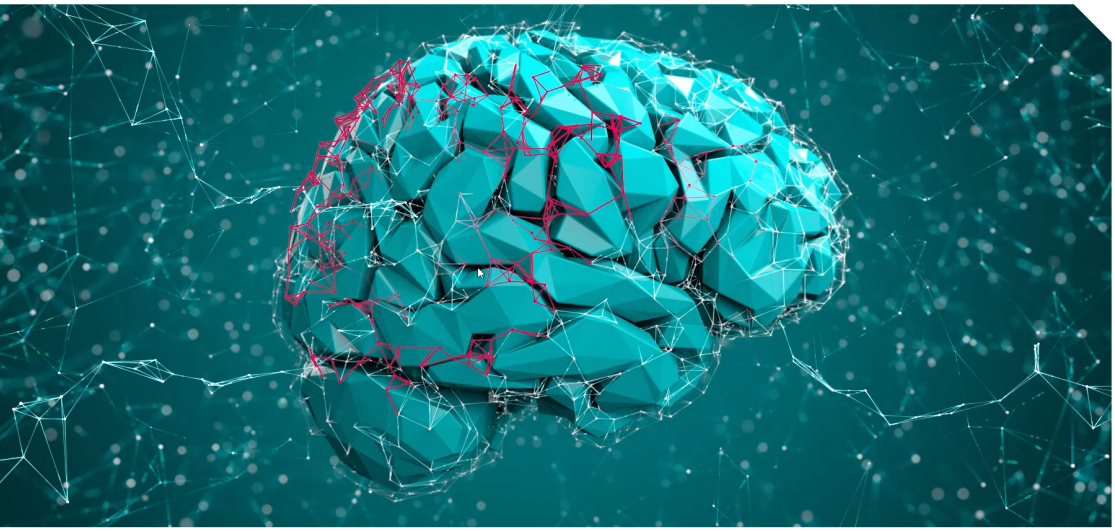
4. Don't underestimate the usefulness of backup media that aren't rewriteable/reusable. If you can't modify what's been written there, then neither can ransomware. Check every so often that your backup/recovery operation is (still) working properly and that your media (read-only, write-disabled, or write-enabled) are still readable (and that write-enabled media aren't routinely writeable). And back up your backups.

5. I'm certainly not going to say that you should rely on backups instead of using security software, but bear in mind that removing active ransomware with security software that detects

Back up everything that matters to you, often, by keeping at least some backups offline – to media that aren't routinely exposed to corruption by ransomware and other malware – in a physically secure location.

ransomware is by no means the same as recovering data: removing the ransomware and then deciding to pay up means that the data may no longer be recoverable even with the cooperation of the criminals, because the decryption mechanism is part of the malware. On the other hand, you certainly don't want to restore your data to a system on which the ransomware is still active. Fortunately, safe backups can save your data if/when something malicious slips past your security software.

mechanism for paying the ransom didn't really work to the attacker's advantage. (Of course, in 1989 Dr. Popp didn't have the advantage of access to cryptocurrency or the Dark Web, or easy ways to use Western Union [the 419 scammer's favorite] or to monetize nude photographs.) The attack itself was 'classic' ransomware, in that it deprived the victim of his or her data. Later, DoS and DDoS attacks deprived companies of the ability to benefit from the services they provided: while customers were deprived of those services, it was the



And the future?

"Don't make predictions about computing that can be checked in your lifetime" – wise words from Daniel Delbert McCracken. Still, we can risk some extrapolation from the recent evolution of ransomware in order to offer some cautious thoughts about its future evolution.

Targeting

The AIDS Trojan was pretty specific in its targeting. Even then, not many people were interested in the minutiae of AIDS research, distribution of the Trojan by floppy disk was relatively expensive, and the provider who was expected to pay. However, as the non-corporate, individual use of the internet has exploded, the attack surface and the range of potential targets have also widened. Which probably has an influence on the promiscuous distribution of most modern ransomware.

Non-targeting

While the media and security product marketers tend to get excited when a highly visible or high-value victim is disclosed – healthcare sites, academic institutions, telephony service providers, ISPs – it's inappropriate to assume that these institutions are always being specifically targeted. Since we don't always know what

vector of compromise was used by a specific campaign, we can't say 'It never happens!'. But it looks as if ransomware gangs are doing quite nicely out of payments made by large institutions compromised via lateral attacks from employees who have been successfully attacked when using their work accounts. The UK's NHS Digital, for example, denies that healthcare is being specifically targeted – a view I happen to share, in general – while acknowledging that healthcare sites have 'often fallen victim'.

Could this change?

At the moment, there still seem to be organizations that are prepared to spend relatively large sums in ransom payment. In some cases, this is a reasonable 'backup strategy', acknowledging that it's sensible to keep a (ransom)war(e) chest topped up in case technical defences fail. In other cases, companies may be hoping that paying up will be more cost-effective than building up complex additional defences that cannot always be fully effective. That in itself may attract targeting of companies perceived to be a soft touch or especially able to pay (financial organizations, casinos). The increased volume of wiper attacks and ransomware attacks where payment does not result in recovery may mitigate this unhealthy trend, but companies that are still perceived as unlikely to harden their defences to the best of their abilities might then be more specifically targeted. It is, after all, likely that a successful attack on a large organization will pay better and more promptly than widespread attacks on random computer users and email addresses.

Data versus Devices

Looking at attacks on smartphones and other mobile devices, these tend to be less focused on data and more on denying the use of the device and the services it facilitates. That's bad enough where the alternative to paying the ransom may be to lose settings and other data, especially as more people use mobile devices in preference to personal computers and even laptops, so that a wider range of data might be threatened. As the Internet of Unnecessarily Networked Things becomes less avoidable, the attack surface increases, with networked devices and sensors embedded into unexpected items and contexts: from routers to fridges to smart meters, from TVs to toys, from power stations to petrol stations and pacemakers. As everything gets 'smarter', the number of services that might be disrupted by malware (whether or not a ransom is demanded) becomes greater. In previous years we've discussed the possibilities of what my colleague Stephen Cobb calls the Ransomware of Things. There are fewer in-the-wild examples to date of such threats than you might expect, given the attention they attract. That could easily change, though, especially if more conventional ransomware becomes less effective as a means of making a quick buck. Though I'm not sure that's going to happen for a while...

On the other hand, there's not much indication that Internet of Things security is keeping pace with IoT growth. We are already seeing plenty of hacker interest in the monetization of IoT insecurity. It's not as simple as the media sometimes assume to write and distribute malware that will affect a wide range of IoT devices and beyond, so there's no cause for panic, but we shouldn't underestimate the digital underworld's tenacity and ability to come up with surprising twists.

* Apologies to the shade of Henry Newbolt who wrote Vitai Lampada, from which I've misquoted: https://en.wikipedia.org/wiki/Henry_Newbolt.

Looking at attacks on smartphones and other mobile devices, these tend to be less focused on data and more on denying the use of the device and the services it facilitates.

2

Critical infrastructure attacks on the rise

- Critical Infrastructure hacks keep increasing
- ESET case study: Industroyer & Black Energy
- Supply-chain attacks
- Why this could happen in your country too?

AUTHOR

Stephen Cobb
ESET Senior Security Researcher

Critical infrastructure attacks on the rise

Cyberthreats to critical infrastructure jumped into the headlines in 2017, starting with a Reuters report in January that a recent power outage in Ukraine "was a cyber-attack". In last year's Trends report we said that we expected infrastructure attacks to "continue to generate headlines and disrupt lives in 2017". Sadly, we were right, and unfortunately, I have to say that the same trend is likely to continue in 2018 for reasons outlined in this update. It should be noted that critical infrastructure is more than just the power grid and includes the defense and healthcare sectors, critical manufacturing and food production, water, and transportation.

Turn it off and on again

Let's look at how things have progressed over time. In late December of 2015, cyberattacks on Ukrainian power companies resulted in electricity service being turned off for several hours to hundreds of thousands of homes in that part of the world. The first article published by ESET researchers in 2016 (on this incident) was Anton Cherepanov's analysis of Black Energy, the malicious code used in that cyberattack. That specific malware did not directly manipulate Industrial Control System (ICS) devices, but it enabled hackers to penetrate the networks of electricity distribution companies and kill software used by ICS equipment. Press reports then – some with eye-grabbing headlines like "Malware turns off the lights" – did not make that distinction clear.

The attack in late 2016, first reported in January of 2017, was quite different, as ESET researchers Anton Cherepanov and Robert Lipovský reported on WeLiveSecurity. Their analysis described a new piece of malware that is capable of controlling electricity substation switches and circuit breakers directly, in some cases literally turning them off and on again (which can severely disrupt supply at this scale). They dubbed this malware Industroyer and made a very strong case for it being the biggest threat to industrial control systems since Stuxnet. When they presented their malware analysis at Black Hat USA 2017, the room was packed and you could have heard a pin drop.

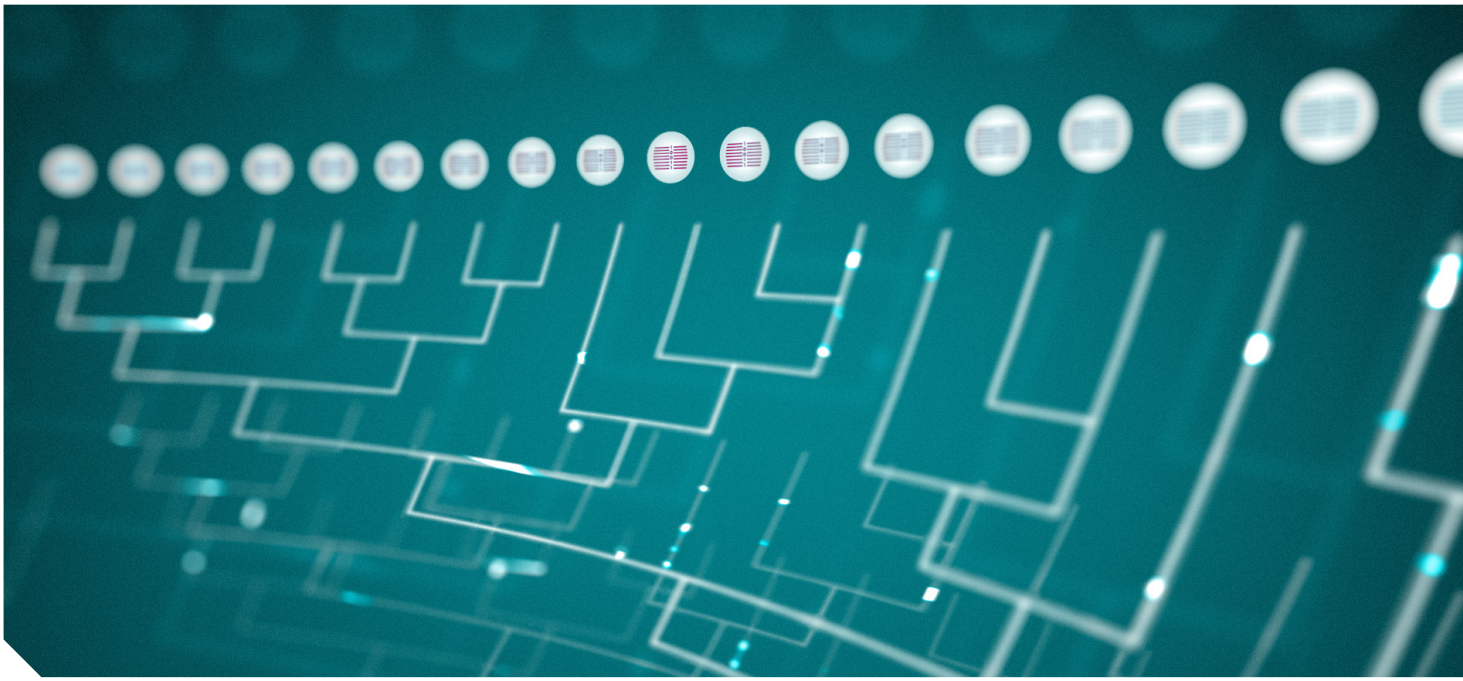
Industroyer's implications for the future of critical infrastructure threats are worrying to say the least, as you can tell from the tone of this interview with Robert Lipovský. The industrial equipment that Industroyer targeted is widely used (well beyond Ukraine – for example in the UK, EU, and the US – and across multiple critical sectors). Furthermore, a lot of ICS equipment still in use today was not designed with internet connectivity in mind, making any retroactive protective measures challenging to implement.

Of course, many of the organizations that currently operate critical infrastructure are working hard to secure it. ESET's research further suggests that any future cyberattack using Industroyer would need to be tailored to specific targets. This may limit eventual outbreaks to well-funded attackers and impede widespread campaigns aimed at turning out the lights, crippling transportation, or halting critical manufacturing. However, it is not unusual for such conditions to change

The industrial equipment that Industroyer targeted is widely used well beyond Ukraine – for example in the UK, EU, and the US – and across multiple critical sectors.

over time as attack code is refined and intelligence is gathered. In other words, the ability to carry out cyberattacks on the power grid will tend to increase through 2018 unless blocked by preemptive measures, like system upgrades, early detection of network probing, and drastic improvement in phishing detection and avoidance.

While producing cost savings, the newer approach introduces further weaknesses into the supply chain, such as chips with hard-to-patch vulnerabilities, and code re-use that introduces software vulnerabilities. Examples in 2017 are the Devil's Ivy flaw found in over 200 different models of security camera made by Axis Communications, and the BlueBorne



Infrastructure and supply chain

Unfortunately, simply upgrading old ICS equipment with gear that was designed with internet connectivity in mind will not automatically improve security. That is because, as Stephen Ridley, founder and CTO of Senrio (a company focused on the security of connected devices) points out: industrial devices are shifting from application-specific integrated circuits (ASIC) to a generic and cheaper System-on-Chip (SoC) architecture for which code libraries are readily available.

vulnerabilities that impacted several billion devices across the most popular platforms: Windows, Linux, iOS and Android. Forecas ts are that more such examples will still be discovered in 2017, and beyond 2018.

A different type of supply chain problem made headlines in 2017, in part because it affected the entertainment industry. While arguably not critical infrastructure, this sector learned some lessons in 2017 that are of value to the truly critical parts of the economy. The attempted extortion of Netflix over the "Orange is the New Black"

TV series, and the unrelated digital theft of the latest installment of the Pirates of the Caribbean movie franchise both point to worrying aspects of supply chain security.

While many large companies appear to be taking cybersecurity much more seriously these days, with security teams getting both the budget and the C-level backing required to do a good job, many smaller businesses supplying goods and services to larger organizations are struggling. That makes them an attractive target if, for example, they happen to have a blockbuster sitting on their post-production audio processing systems, which happen to be connected to their office network, and whose users have not been trained to recognize phishing emails.

2017 confirmed that security weaknesses at those smaller suppliers were shown to be an effective means to compromise large targets such as major motion picture producers. After several high profile cases made the news, I put together some advice on supply chain security, which is also relevant to organizations involved in critical infrastructure. After all, attackers may find it hard to hack into the network of a large utility company directly, but what if they hack the company that supplies janitorial services instead?

In the old days, we used to worry about the "evil janitor attack" in which an ethically challenged but computer-savvy janitor might obtain unauthorized network access while taking a break from cleaning offices on the night shift. While that threat has not entirely disappeared, it has been joined by the threat of a cyber-insecure janitorial supply firm connecting to power plant systems via a vendor services portal (for example) that is poorly segregated from the ICS network.
The implication? Critical infrastructure organizations need to keep improving their security in 2018, reducing the effectiveness of phishing attacks (still amongst the most prevalent attack vectors), segregating and controlling network access, reviewing and testing both old and new hardware and software, and doing digital due diligence on suppliers. They also need to watch for and react to the kind of network probing and surveillance that may presage a full-on cyberattack.

Attackers may find it hard to hack into the network of a large utility company directly, but what if they hack the company that supplies janitorial services instead.

3

Doing time for cybercrime: Police and malware research join forces

- Takedowns, prison and how ESET combats criminal activity
- Case Study: How Windigo research helped to put an attacker behind bars
- Why should we care?

AUTHOR

Alexis Dorais-Joncas
ESET Senior Security Researcher

Doing time for cybercrime: Police and malware research join forces

The primary purpose of malware analysis is to determine how a given piece of malware works, extract IOCs (Indicators of Compromise) and determine potential countermeasures. This work is almost purely technical in nature: it focuses on binary files and their properties. Results from malware analysis are crucial for organisations to allow them to defend against an outbreak or to remediate a live infiltration. They are also crucial for security software vendors, enabling them to build better detections and protective measures for their customers.

But sometimes other types of questions need answers. Is this file related to that other one? How is the C&C (Command & Control) infrastructure built, and how does the communication protocol work? How does the botnet monetize its activities: pay-per-install, spam, traffic redirection?

Answering questions like these is what malware research is all about. It allows for better understanding of the big picture behind a single malware sample, to connect the dots and to understand what's going on.

Of course, this also helps security software, aka AV vendors design better protection. But information stemming from malware research can also be useful to law enforcement in the fight against cybercrime. How so? Let's see, with a few examples of work done by ESET that have helped disrupt malicious operations.

Disruption campaign against Dorkbot

In 2015, ESET was invited to join Microsoft's Coordinated Malware Eradication campaign (CME) against the Win32/Dorkbot malware family. Dorkbot was a kit, available for sale in underground forums, that infected over one million PCs spanning multiple, independent botnets. The objective of this CME campaign was to massively disrupt as many of those botnets as possible by taking down the related C&C infrastructures simultaneously.

In support of this operation, ESET malware researchers automated the process of extracting C&C information from Dorkbot binaries. We applied this process to our flow of both existing and new Dorkbot samples. We then manually sanitized the results by removing known sinkholes and clean domains/IPs to mitigate the risk of taking down legitimate resources. Microsoft merged that information with their own data to create an exhaustive list of all the active C&C nodes to target. This complete list was then relayed to law enforcement agencies all around the world, such as the Canadian Radio-television and Telecommunications Commission (CRTC), the Department of Homeland Security's United States Computer Emergency Readiness Team (DHS/US CERT), Europol, the Federal Bureau of Investigation (FBI), Interpol, and the Royal Canadian Mounted Police (RCMP). On disruption day, warrants and takedown notices were executed in a coordinated maneuver.

Since then, we have seen a sharp decline in Dorkbot activity worldwide, indicating that the CME campaign succeeded.

Dorkbot was a kit, available for sale in underground forums, that infected over one million PCs spanning multiple, independent botnets.

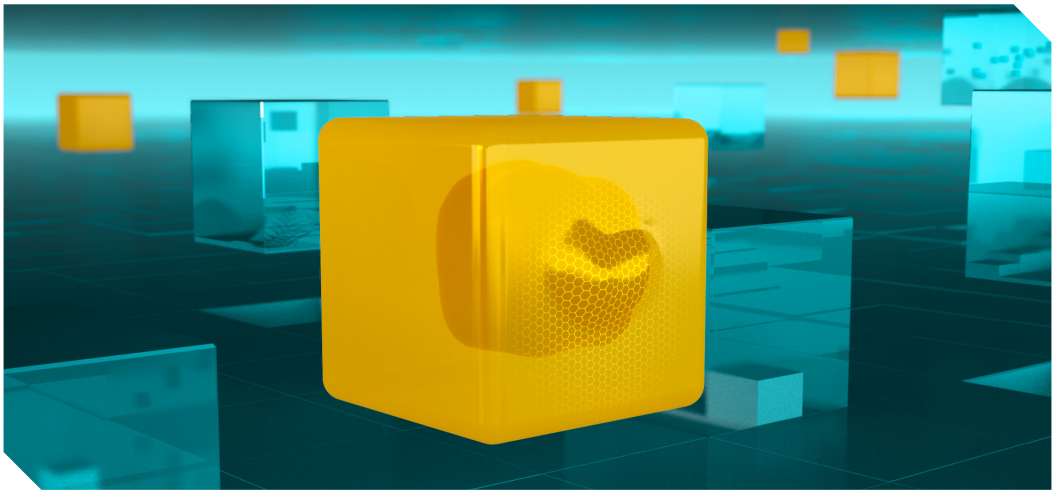
Windigo and the Ebury botnet

ESET first published an exhaustive technical analysis of what we dubbed Operation Windigo in 2014. Briefly, Windigo was supported by a credential-stealing backdoor that infected tens of thousands of Linux servers, on which one or more additional malicious components were installed and used to monetize the botnet by, for instance, sending spam or redirecting HTTP traffic. After publication, we started collaborating with the FBI on their investigation into the cybercriminals behind Operation Windigo.

Our contribution was to share technical information stemming from our malware research, such as infected IPs, information taken from the spam messages sent by the botnet, and other relevant and publicly-available information such as domain registry information.

Equipped with that information, the FBI was able to do its part, slowly but surely. In early 2015, a Russian citizen named Maxim Senakh was identified as one of the co-conspirators behind Operation Windigo and formally indicted in the USA. Senakh was later arrested by Finnish authorities at the Russian border as he was returning to Russia from a vacation, and then extradited to the U.S. in February 2016. Senakh ended up pleading guilty to conspiracy to commit wire fraud being in violation of the Computer Fraud and Abuse Act. He was sentenced to 46 months in prison.

More details on this story are available in this blogpost https://www.welivesecurity.com/2017/10/30/esets-research-fbi-windigo-maxim-senakh/.



Why should we care?

Spending time and energy to make the life of cybercriminals harder is worth it. We believe it's one of the best ways to help prevent cybercrime activity and to make the internet a safer place. We also think it is the Right Thing To Do.

There are various theories behind classic crime prevention and we will certainly not pretend to be criminologists. However, there is neat mapping between what we do to combat cybercrime and the theory of "situational crime prevention", which is defined as:

Situational crime prevention is based upon the premise that crime is often opportunistic and aims to modify contextual factors to limit the opportunities for offenders to engage in criminal behaviour."

Situational crime prevention techniques can be grouped into various broad categories, three of which are connected to what we do.

1. *Increasing the effort involved in offending*
   Executing coordinated disruption campaigns, such as the one directed against Dorkbot, forces the attackers to regroup and pivot to new strategies and techniques, such as creating new malware or changing communication protocols, clearly increasing the effort needed to maintain an ongoing criminal operation.

2. *Reducing the rewards that come from committing a crime*
   (A corollary to 1.) is that disrupting malicious operations necessarily increases the cost of committing the crime, reducing the net profit proportionally.

3. *Increasing the risk associated with offending*

Providing technical information to law enforcement officers helps them steer their investigations in the proper direction and build stronger cases. More cybercriminal investigations with increased cooperation from malware researchers will lead to more arrests and convictions, hence increasing the risk to cybercriminals that they will be caught.

Some people think the reason so few cybercrimes go punished is that it is easy to perform criminal activities on the internet anonymously, without much chance of being traced. It is actually pretty much the opposite: maintaining perfect operational security (OPSEC) consistently is pretty hard. Think about all that has to be done in order to exploit a malicious operation: launch infection campaigns, monitor the status of the botnet, update the malicious components, register domain names or hosting services, monetize the operation itself, and so on. In order to perform the perfect cybercrime, each and every step must be executed perfectly, all the time. Cybercriminals are humans and humans make mistakes. All it takes is one bad day where an attacker connects to the wrong server before enabling a VPN or TOR connection and a giant arrow pointing back to him or her will be stored in a log file somewhere, waiting for somebody to find it.

Some people also give up going after cybercriminals because even when identified, cybercriminals remain out of reach. Maybe they live in a jurisdiction that has no effective laws against cybercrime, or that has no mutual extradition treaty with the countries investigating them? But there again, humans make mistakes. All it might take to be caught is for a known cybercriminal to leave his country to take some vacation time abroad.

2017 has been marked by a large number of arrests in various cybercrime operations, as outlined in Stephen Cobb's excellent summary. As major law enforcement entities gain experience in working with private entities such as ESET to track cybercriminals, we can predict with some confidence that 2018 will bring more and more successful investigations that will contribute to making the internet a safer place for everyone. Except for cybercriminals.

In order to perform the perfect cybercrime, each and every step must be executed perfectly, all the time. Cybercriminals are humans and humans make mistakes.

4

Democracy hack: Can electoral processes be protected?

- Electronic voting & internet voting
- Hacktivism and attacks during electoral campaigns
- How security can change a country direction

AUTHOR

Camilo Guttierrez
Head of Awareness and Research
ESET Latinoamerica

Democracy hack: Can electoral processes be protected?

The past two years have seen electoral contests taken place in several countries long regarded as key players on the global stage. However, the elections raised a whole host of questions, among which the most pressing was whether a cyberattack could influence an electoral process to the extent of causing a shift in the political course of a nation?

To venture a definitive answer to such a question would be a daunting task for anyone, regardless of whether they sat in the chair of a political scientist or cybersecurity researcher. Nonetheless, it has become apparent that the scenario in which we currently find ourselves, poses a number of challenges. There is substantial evidence that the implementation of electronic voting has yielded results that are far from secure, as we will demonstrate here.

Moreover, there are two other crucial factors to which we must draw attention. Firstly, the influence of social networks on public opinion, especially in respect to pushing a political agenda, particularly the way in which they support hacktivism; and lastly, the need to include national cybersecurity issues as part of the political agenda.

Insecure electronic voting systems

It was only a matter of time before information technology would be incorporated into the electoral process, especially given the reasons why certain countries (such as Argentina, Brazil, Germany and the United States) decided to introduce a limited implementation of electronic voting, in some extent: to put an end to fraud, to standardize and speed up the counting process, and to supplement rather than replace the paper ballot system. We can all agree that technology advances inexorably, but perhaps efforts should be aimed toward implementing more control mechanisms rather than favoring an approach that actually adds new points of failure without removing any of the risks.

Just as unscrupulous campaign officials, activists and other key players have found ways to commit fraud over the years by exploiting the electoral system itself, soon cybercriminals will discover ways to capitalize on the digital system, particularly if they are armed with sponsorship of some kind.

Back in 2006, Finnish computer programmer and co-founder of ROMmon, Harri Hursti had already demonstrated in the well-known documentary Hacking Democracy, how the Diebold voting system in Leon County, Florida, could be easily and completely compromised just by using a memory card.

Just like that, he was able to change all of the votes without being detected. Nonetheless, this same software – that with just a few adjustments, a new name and a change of ownership – continues to be used in the United States to record and count tally votes.

Fast forward 10 years and very little has changed, other than the fact that additional evidence has been revealed.

Brazil's electronic ballot box has been mired in controversy since 2012, when it was discovered that it was possible to crack voting secrecy completely. After years of substantiated allegations of vulnerabilities, the Superior Electoral Court will go back to implementing paper ballots (in a hybrid format) for just 5% of ballot boxes to be used for elections in 2018. Meanwhile, electronic ballot procedures in both Argentina and Germany have been shown to be flawed as well.

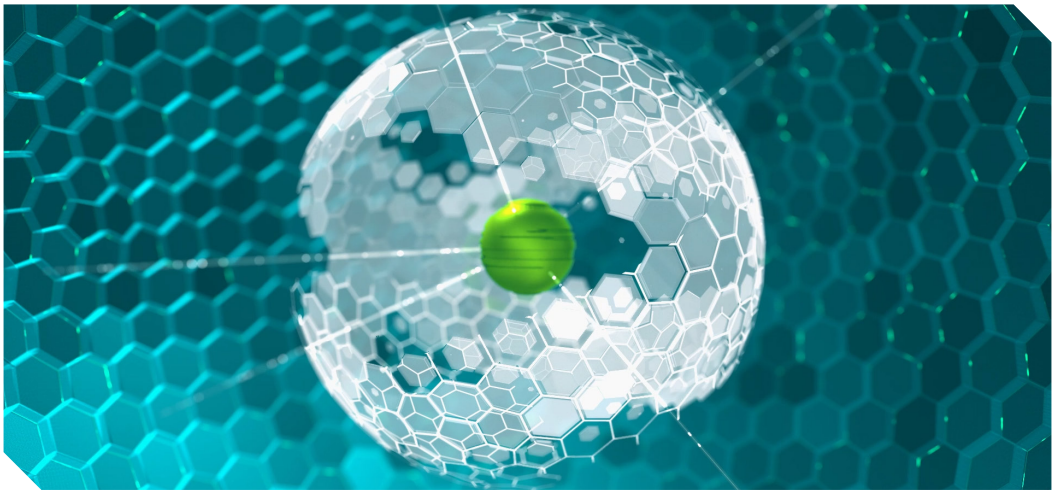
The preponderance of evidence to date, strongly suggest that we cannot rely solely on technology for something as significant to our lives as the electoral process; it must only be used as a complementary tool. If the idea is to mitigate any and all forms of fraud, thus boosting faith in both the results and our democracies, we must consider hybrid systems with both paper and electronic ballot records.

Hacktivism that can change public opinion

Social media has become the new frontier of the political stage and used by political campaigns to reach increasingly large numbers of people. As we now know, these same networks have also been used to undermine electoral campaigns by spewing falsehoods, and promoting fake news reports, not to mention widespread attacks on reputation aimed at public figures.

A number of these attacks use computer threats such as bots or other form of malware, which could be mitigated with adequate security management protocols in place. Otherwise, what might appear to be the indication of a trend may actually be the manifestation of a group of attackers.

While such an attack might help to manipulate or skew popular opinion, it does not signal doomsday for democracy.



However, it does pose some critical cybersecurity challenges in order to ensure that the voice of the populace is truly represented in the elections.

The "Defending Digital Democracy" program, announced earlier in July, is backed and endorsed by companies like Facebook and Google, which suggests how highly they rate the importance of securing these types of mechanisms.

Social media has also been used to undermine electoral campaigns by spewing falsehoods, and promoting fake news reports, not to mention widespread attacks on reputation aimed at public figures.

If the parties involved don't take matters into their own hands, these kinds of incidents will continue to happen well into the future.

National cybersecurity

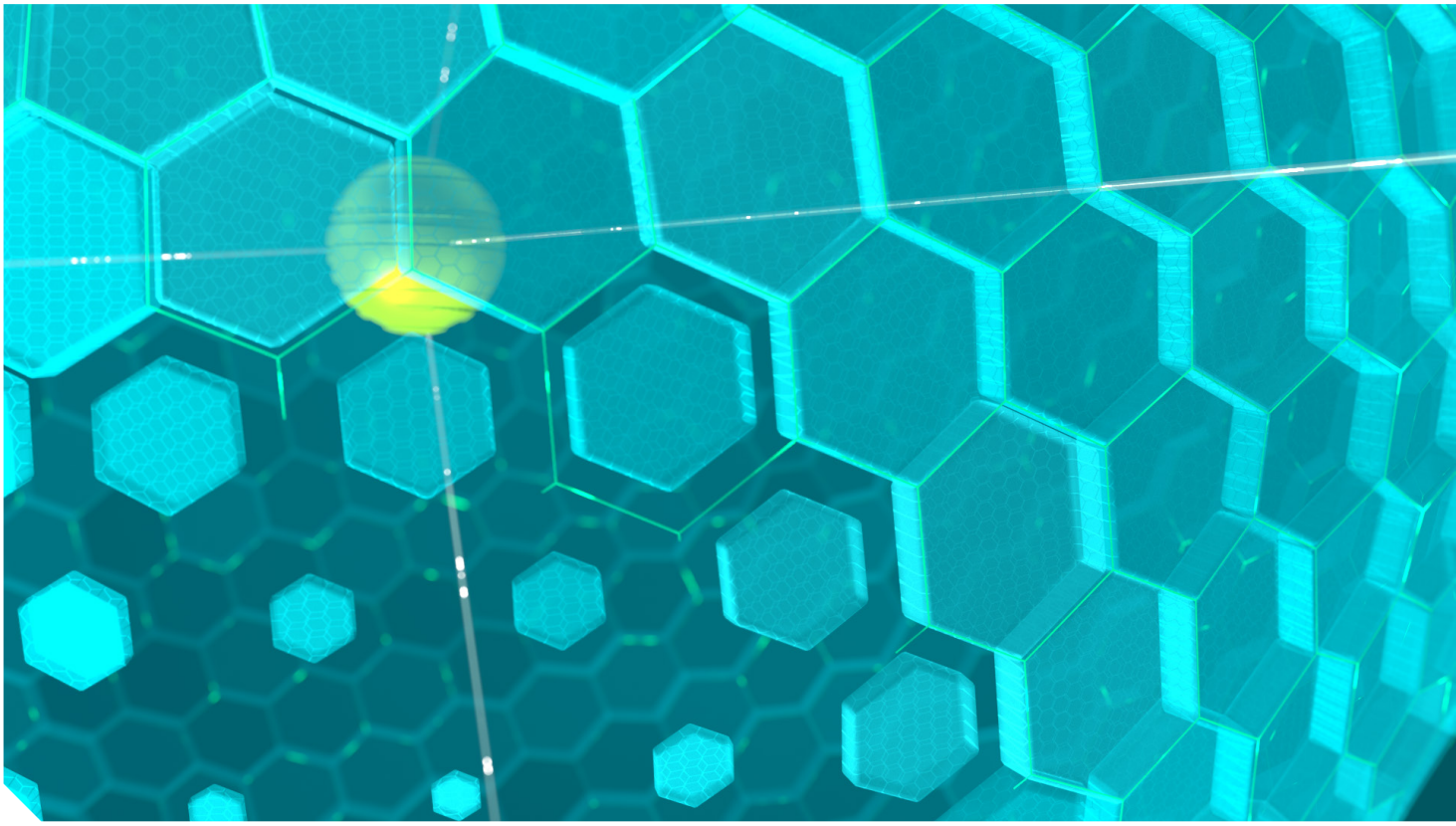
If technology is a major part of our lives, then the governments must be tasked with the responsibility of ensuring that users interact with technology as safely as possible, by implementing national cybersecurity programs engaging with key players, such as CISOs and auditors.

And if public officers, such as court authorities or voting commission officials, must make decisions regarding the implementation of certain technologies, then they should undergo cybersecurity training appropriate to the situation, to help them make the most suitable choices.

There is no doubt that new risks come with every new advancement, but if we want to use technology to improve our lives, then we must prevent it from creating greater problems overall than benefits. All aspects of an electoral system must be regarded as part of every country's critical infrastructure (and be safeguarded as such).

The challenges are laid out before us. Now is the time to engage in preventive measures that focus on the digital security of information, and all those involved must contribute to solutions that guarantee the proper implementation of democratic processes.

There is no doubt that new risks come with every new advancement, but if we want to use technology to improve our lives, then we must prevent it from creating greater problems overall than benefits.



5

Personal data in the new age of technology and legislation

- How IoT is taking us to a 'public' world in terms of personal data
- Social media profiling and users always more used as the 'product'
- Users behaviors used in AV industry related to free AVs

AUTHOR

Tony Anscombe
ESET Global Security Evangelist and Industry Partnerships Ambassador

Personal data in the new age of technology and legislation

Privacy is, or should be, a fundamental human right. Nowadays, the understanding of what the term privacy means for the end user inclines towards data privacy or information privacy. This deviation makes maintaining the desired data-neutral position for the end user increasingly complex. On one hand, there are extremely technology-driven privacy enthusiasts who cultivate zero digital footprint anywhere, on the other – in real life, the vast majority of end users leave a footprint everywhere; giving cybercriminals a web-scape full of sensitive data that looks like a sandy beach on a busy day.

Data is driving the next revolution in technology and feeding the vast artificial intelligence (AI) systems being built. The question is: when any sensitive data enters one of the webs, how many machine-driven decision-making processes will be able to enforce the right to erasure and the right to be forgotten and will the companies collecting this data understand where and how it is being used by their AI systems?

While the majority of endusers understand that they are giving their data to social networks or to companies through forms and applications, there are many other providers and services whose data-collecting may not be so transparent.

Free software and services

As consumers expect to enjoy software at no cost, or very low cost, some vendors have taken the decision to enter the data-collection and data-sharing business. Providers of free software only have a few methods by which to monetize their products and the least intrusive, at least from the perspective of what the end user actually sees, could be the collection and sale of data to third parties.

In the past year we have seen trusted security vendors deciding to offer free anti-virus products. While they may not have openly declared their intentions as to how the monetization of their new, free products will work, we can expect to see some of them use indirect monetization methods such as data collection.

The trend of offering of free antimalware products and the likely monetization of them through indirect means, seems to have accelerated after Microsoft began offering Windows Defender Antivirus as a free default option. Naturally, as a percentage of users shift to the Microsoft by default option, there is less opportunity for existing vendors to sell software, hence the appetite for alternate monetization via offering their own free software rather than direct competition.

The free or low-cost cybersecurity software will continue trending over the next year. This will increase risks connected with data privacy, as free software usually lacks traditional monetization methods, and instead, introduces complex disclosure statements that are in part designed to obscure intent as to what data is being collected and whether it can be sold. This is evidenced by the

many companies offering lengthy and unreadable privacy policies that are only comprehensible to lawyers.

Thus, with any free product it is important that a user understands how the company is making money: for example a mobile game may show adverts, or upsell levels of the game. If it is not obvious how the company makes money then it is highly likely your data and privacy are the method of monetization.

Internet of Things

While free products and apps are all-knowing about our online habits, the adoption of Internet of Things (IoT) devices means that even more sensitive data is now available for collection and exploitation.

As you drive home from work, your phone is transmitting traffic conditions to share with other drivers, hopefully allowing you to make intelligent detours or driving decisions to get you home earlier. The connected thermostat at home is communicating with your phone, relaying your location and the time of day. Currently, you are homeward bound. As you enter the suburban street where you live, the garage door opens automatically, using your proximity to make a decision. The lights come on and your current choice of music transfers from the car to your home automatically. IoT devices are designed to work together, simplifying our existence.

And every device can tell a story via the data it collects. Combining those various data streams, any attacker will be able to paint a full picture of your life: where we work, where we eat, when we go to the gym, what cinema we visit, where we shop and so on. The combination of this data and advances in machine learning and artificial intelligence could mean that we start becoming puppets of technology as it increasingly makes decisions for all of us.

Analysts at Gartner predict that in 2018 there will be 11.2bn connected devices in the world, rising to 20.4bn by 2020. The rise of the machines is coming, beware! Every time a device asks to be connected we need to educate the end user to read the privacy policy and to make informed decisions about whether or not to accept the data collection terms as set out in the privacy policy.

Legislation

Starting in May 2018, the European Commission's General Data Protection Regulation, a directive that gives citizens more power over how their information is processed and used, comes into effect. The legislation affects any company processing or collecting the data of a European Union citizen, regardless of where the company is based.

Non-compliance could result in large fines, but there is no clear answer as to how these fines will be imposed on companies outside of the EU. The Commission may feel that it needs to make an example of a company located outside of its territorial borders, and, potentially, very soon after the May 25th implementation date. Without such an example of enforcement many international companies may take the risk of non-compliance, so we might see the European Commission step up and take action in 2018.

Privacy in the US took a backward step in 2017 when the new administration repealed pending legislation that restricted internet service providers (ISPs) from collecting customer data without permission. While

Every device can tell a story via the data it collects. Combining those various data streams, any attacker will be able to paint a full picture of your life.

some ISPs have made a voluntary pledge not to allow third-party marketing, that does not mean they will not use such data for their own commercial gain.

The depth of data collected from our online habits could easily allow profiles to be constructed, showing what may be considered extremely personal interests, drawing on information that we don't realize someone is collecting.

Customer profiles could become the target of hackers and we have seen individual data breaches of data sites, stores and others sites. Stealing data that is generated by watching everything we do online could be the ultimate prize to a cybercriminal, offering the opportunity to blackmail users based on their online habits.

The ability to manipulate huge amounts of data as described above and then to use it for something meaningful is a relatively new option for many software and service providers, as the associated storage and processing costs have dropped massively. The 'big data' ecosystem now means that many more companies have the ability to collect, correlate and sell their data.

The ease with which companies can collect data and sell it, our willingness to accept the default settings, and our avoidance of actually reading a privacy policy, means that our identity, way of life and personal data are becoming a corporate asset.

I hope that 2018 brings about greater user awareness, but realistically I suspect it will see greater amounts of data collected with little awareness on the part of the user. With every device that gets connected without informed decision or choice, our privacy is eroded further, until at some point privacy will be something that only our ancestors enjoyed.

Every time a device asks to be connected we need to educate the end user to read the privacy policy and to make informed decisions about whether or not to accept the data collection terms as set out in the privacy policy.

CONCLUSION

Conclusion

Following an analysis of the progression of ransomware and ongoing attacks on critical infrastructure, highlighted in the previous chapters, it becomes clear that cyberattacks will continue to expand in scope and volume over the coming year. However, we must not lose sight of the fact that these complex scenarios are just one aspect of cybercrime as a whole and not necessarily the most significant. Even though sophisticated cyberattacks might attract more attention, they only represent a small fraction of the cyber threats we analyze in our malware labs on a daily basis.

The truth is that the most successful threats we see are the simplest; usually distributed through malicious attacks using spam, phishing, and direct download campaigns that could be mitigated just by increasing cyber awareness among end users. The problem is that the resources needed to make the public cyber aware have yet to be allocated.

Events from 2017 have shown that technological advancements and their accelerated rate of adoption by end users globally, have brought a number of previously unthinkable scenarios within the realm of possibility.

Apart from the specific characteristics of each event, the single common denominator in every single one of these situations is sensitive and private information. Regardless of whether it belongs to a corporation, the government, or to individual users who may believe their data is of little significance, nowadays information is a valuable commodity across all echelons. It can be used as currency to access applications and free content, such as when online businesses monetize it, in exchange for user profiles — while government agencies use it to keep records and manage their operations.

In most cases, the harvesting of this sensitive and private information is a transparent and legitimate activity; often described under "terms and conditions" that very few people take the time to read. But what happens when there are many parties involved in protecting this information? The risks grow as the number and complexity of processes in which something could go wrong multiplies.

An end user's personal information may be compromised by a specific incident (such as a malware infection or a phishing campaign); or through a system-wide breach at the company level; or even through a cyberattack affecting a government agency or financial institution.

So why hasn't anyone insisted that all the parties involved do their fair share so that cybersecurity measures are properly enforced on all fronts? The task isn't solely reserved for cybersecurity companies to handle or eliminate, that would be the same as asking doctors to eradicate disease, or for the police to put an end to all crime.

Digital scams and threats to information security will continue to exist as long as there are people in society willing to

harm others simply because they have the opportunity to do so, or seek to profit dishonestly.

Now is the time for users at every level, and ultimately, the public as a whole, to understand that cybersecurity not only depends on the providers they choose to safeguard it, but also on themselves and the fact that there is still a lot more work to be done.

The first step is to understand the value of information in this day and age, and the reasons why every player in this game of digital living needs it to fulfill his or her objectives. It is not possible to protect something without first understanding what it is, and knowing why we need to protect it.

Understanding these threats and building awareness about how to mitigate them is critical to protecting the confidentiality, integrity and availability of information of various stakeholders in our society, the same information that has become the basis for a number of activities (both lawful and otherwise).

The outlook appears to be quite promising: ever since WannaCryptor (WannaCry) took the world by surprise, awareness of cybersecurity has achieved a greater presence across various industries and has repeatedly made headlines.

Attacks on the social media accounts of celebrities and soccer clubs, such as Real Madrid and Barcelona, as well as the internal systems of high-profile companies, such as HBO, Disney and Equifax, have also affected the thinking of the general public, many of whom are just beginning to understand what is going on.

We hope that Trends 2018 will help shed some light, for readers, on the key problems that have to be addressed in order to make progress toward a safer future.

ENJOY SAFER TECHNOLOGY™