CYBERSECURITY TRENDS 2021:

Staying secure in uncertain times

TABLE OF CONTENTS

INTRODUCTION

The COVID-19 pandemic has dealt a shock to the 'system', thrusting many of us into a spiral of worry and giving the permanence of change a whole new meaning. With 2020 ending soon, one of the big questions on everybody's lips is: how might 2021 play out?

2020 has been a year like no other in living memory, as hardly any facets of our lives have been spared the effects of the worst public health crisis in decades. The COVID-19 pandemic has upended our day-to-day, exposed our collective fragility and vastly heightened our sense of uncertainty. The paradigm change will no doubt have profound and long-lasting effects, including those that we cannot yet foresee.

Some of the seismic shifts sparked or accelerated by the pandemic involve our embrace of technology as the global emergency has helped push some of the previously offline "touchpoints" into the online realm. Indeed, by increasing our reliance on connectivity and kicking digital transformation into overdrive, the crisis may have even given us a bit of a sneak peek into the near future, perhaps even after the pandemic.

This begs the question of what may be in store in 2021, including when it comes to threats and risks lurking in the digital realm. It's well established by now that cybercriminals were quick to adapt to the new reality, seizing the unique opportunities that the general anxiety and the inevitably pell-mell rush to remote work brought. As we're about to step into the new year, we need to pause and think about how the cybersecurity threat landscape has evolved and how cyber-risks may be further reshaped and exacerbated going forward. Looking back at, and cautiously extrapolating from, recent events and trends remains the best way to get a sense of the future.

One aspect of our lives that has changed beyond recognition in 2020 has to do with our working habits. In a way, the shift may have been long in the making, with the pandemic vastly accelerating and intensifying pre-existing trends. However, businesses and the newly distributed workforce were ill-prepared to contend with the cyber-risks that the almost overnight switch to the new normal had brought on or escalated. In the opening chapter, Jake Moore looks at this shift, as well as at how organizations, especially those that won't go back to the old ways, and their workforce can stay safe. Just as importantly, he wonders what the near future holds for working patterns and whether we'll go back to the pre-pandemic office life any time soon.

It would be remiss of us not to consider at least some of the most pressing threats posed by malware, with Tony Anscombe looking specifically at how ransomware attacks have evolved. This threat has been going strong for years now; however, more and more ransomware operators are further tightening the screw on their victims by combining extortion with data exfiltration, as well as with threats to publish, sell or auction off the stolen data if no payment is made. Tony also looks at an increase in ransom demands as another trend that's been evident of late, before looking at the broader picture and noting how the shifts are a way for cyberextortionists to maximize the ROI of their attacks. How will the situation play out in 2021, perhaps even with implications for the very definition of 'ransomware'?

With threat actors continuing to deploy a range of increasingly complex and often innovative ways to ensnare their victims, Camilo Gutiérrez looks at one particularly evasive tactic that, while not entirely new, has gained traction over the past few years. Living-off-the-land attacks co-opt legitimate applications on the targeted system and minimize the forensic footprint, all the while maximizing the stealth and effectiveness of the incursions. As a result, they can be difficult to detect and prevent, serving as a powerful reminder for organizations to assess their preparedness to fend off these attacks.

That technology permeates almost every facet of our lives was, naturally, made even more evident during a year when all things digital shaped our days more than ever before. As we yearn for technology-enabled convenience, the Internet of Things has been a thing for years, including when it comes to the use of technology for sexual wellbeing. Adult toys certainly haven't escaped the smart revolution; indeed, after the pandemic struck, sales of smart sex tech surged. What has perhaps commanded less attention, however, is the privacy and cybersecurity implications of these devices. Denise Giusto and Cecilia Pastorino show that this tech is a potential hotbed of privacy and security concerns that may ultimately expose some of the users' most sensitive data to cybercriminals.

To be sure, many long-standing problems will not be going anywhere as the world will strive to come back from the depths of the pandemic. Nevertheless, if there is a silver lining in the dark cloud cast by COVID-19, it's that there are also valuable lessons to be learned from the calamity. Among them, it reminds us to be prepared to face and respond to adversity and that arming ourselves with knowledge is a powerful first step towards 'inoculation' against various kinds of threats.

1

THE FUTURE OF WORK: EMBRACING A NEW REALITY

2020 was the year when businesses transitioned to remote working, but who really helped take these companies through accelerated digitalization? Was it the CEO, the CTO or more truthfully, was it COVID-19? And what will work look like after the pandemic?

Jake Moore
ESET Security Specialist

Since governments around the world implemented COVID-19 lockdowns, the world of work has changed dramatically in ways most people could not have envisioned. The result? *Mass implementation of remote working* that has seen a heavier reliance on technology than ever before, together with a resultant disruption of many businesses' technology infrastructures. Central IT systems have been substituted with a network of disparate individuals, all with a greater responsibility for their own technology use and cybersecurity needs. Not only does a fractured security system leave companies vulnerable, but employees' confidence in handling cybersecurity is also a serious risk.

At a time when businesses are relying on resilience, malicious actors are continually exploiting the security vulnerabilities that accompany remote working. Of course, there are ways to make our new environments more secure. Simple measures can be put in place to help reduce the chance of a cyberattack – but going from one or two offices to dozens, even hundreds of home offices, usually comes with a price.

WHAT COVID-19 HAS TAUGHT US

The pandemic not only taught us how working from home is possible, but also how companies can create and enforce policies in a matter of weeks. Relocating entire workforces would usually take months of planning, endless consultations and then more planning before being signed off by multiple parties. But when faced with being told by your government that you are no longer allowed into your offices (where possible), it is fascinating how quickly these changes can come into effect – and even hit the ground running when push comes to shove.

Some questions, however, still loom: How can we protect the remote workforce? Is working from home as safe as in the office? Will we ever go back to the office life of 2019?

In order to be resilient against cyberattacks, many companies have strong policies and risk assessments in place. Many will also have protection to withstand the vast majority of threats that any normal business would expect. However, it is unlikely that any organization in the world was entirely prepared for this huge and rapid shift in working when COVID-19 hit the world. The physical office walls act as one big firewall and any abnormal inquiry into the network can often be easily highlighted. But when everyone in the organization is now connecting to a network from outside the safety blanket of the usual perimeter, the chief information security officer (CISO) and other invested parties may face some daunting tasks, to say the least.

Remote working in some form or another is clearly here to stay for the long haul, but to efficiently operate it requires excellent management, as well as security at the core. To help businesses run smoothly with minimal disruption, they need to ensure the management and security practices play an equal role, which in turn protect their staff and the business. Some organizations were thrown off course when they were instructed to house their staff at home, but others embraced it and even discovered a more productive shift (ESET included!).

Training can go a long way in protecting staff and this works best when it is delivered often and in small doses. This can be, for example, via quick reminders in products around the importance of *virtual private networks (VPNs)* and on the awareness of phishing emails to keep people vigilant yet without frustrating or frightening them.

BEFORE VS. AFTER

Prior to COVID-19, cyberattacks were already on the increase, and the pandemic and resulting lockdown has only heightened this risk. From *phishing scams to COVID-19-related malware*, cybercriminals have pounced on the innate vulnerabilities of dispersed workforces and their IT systems in order to find those cracks to exploit.

Remote working has brought flexibility, but it has also dramatically altered business processes and systems in order to cater to a distributed workforce. Employee access to IT departments, and vice versa, has changed. Collaboration and teamwork are facilitated virtually, and a lack of face-to-face communication can hinder direct channels of communication. Some of the baseline security measures taken for granted in the office must be compensated for at home, such as requiring home workers to use multi-factor authentication or a VPN to access internal networks. Reminding workers to enable automatic updates and check the security of their own Wi-Fi networks is also crucial as the first line of defense against cybercriminals. Ideally, the remote workforce will always also be using company-issued devices and remain fully vigilant to these constant and persistent threats.

The overnight shift in our culture of remote working has been critical to many organizations in proving that it works as will it continue to work. However, we must never become complacent. We soon miss those discussions at the water cooler or at lunch where we discuss the latest phishing scam or other practical security tips that often help people to make the right choices.

FUTURE-PROOFING YOUR ORGANIZATION

Fully digital companies were clearly better suited and set up to move their workforce home, but not all companies were so fortunate. It should be remembered that thousands of companies require their employees to work from home but if security is at the heart of a company's organizational policy, then there is no reason why the majority of the world's businesses cannot continue to securely and safely work away from the office.

But what if there is a vaccine? Will everything just return to normal? I don't think so. We have all learned that working remotely can benefit organizations and can be transitioned securely. I don't think, however, that we will work remotely five days a week. What we have found that as it works, we will continue to work from home when it suits us … which will no doubt benefit our health and well-being.

Personally, I have found this shift to home working improves my family life tremendously. I have never spent so much time with my young children, and they have commented multiple times how nice it is to have me at home more often. The rigmarole of the Monday-Friday 9-5 is gone forever, and we must document COVID-19 for this *rapid speeding-up of the process* that would have likely taken years to come into effect, if at all. More employees around the world will naturally and effortlessly migrate to what works for them and their businesses, which in turn makes a better environment for us all. The fact it can be taken seriously and securely enables it.

Regardless of what the future will bring, two things are certain – the way we work has been permanently altered and cyberattacks are not going away. The COVID-19 pandemic has only accelerated the implementation of technology across all facets of life, and as more and more of our working and home lives become digitized, cybersecurity will remain the lynchpin of business safety.

Cyberattacks are a persistent threat to organizations, and businesses must build resilient teams and IT systems to avoid the financial and reputational consequences of such an attack. An understanding of the workforce can play a key part in any business's cybersecurity strategy, both enhancing the effectiveness of training and encouraging employees to be more invested in their own self-awareness and skills. Understanding that the human element of cybersecurity is just as important as the technical is the first step in building holistic protocols that account for individual strengths and blind spots.

2

RANSOMWARE WITH A TWIST: PAY UP OR YOUR DATA GETS LEAKED

With ransomware attackers increasing their ransom demands and seeking greater leverage to coerce businesses into paying up, the stakes are clearly rising for the victims. What will next year look like on the ransomware scene?

Tony Anscombe
ESET Chief Security Evangelist

One thing I predict needs to change in 2021 is the dictionary definition of *"ransomware"*:

> *"Ransomware is illegal computer software that stops a computer from working or prevents the user from getting information until they have paid some money."*
>
> *(Collins English Dictionary)*

Why should the definition change?

The 1980's are remembered for many things: mixtapes, shoulder pads, the Rubik's Cube and the Live Aid concert to name a few, but few would associate the decade with ransomware. In 1989, the *AIDS Trojan was born*, infecting devices through a floppy disk, and hiding directories and encrypting the names and extensions of files stored on the hard disk. The user was then presented with a message to renew their license to resolve the issue by sending $189 to a post office box in Panama. Thirty-one years later, with several twists and turns in its evolution, the term "ransomware" is a commonly used term across the world.

Ransomware today is prominently associated with encryption of files and data and locking access until a fee is paid and a decryption method provided – at least you hope that's all it is. During its evolution, ransomware has taken various forms, including locking the entire device without encrypting anything and displaying a message requiring payment to regain access; as well as locking the screen, displaying pornographic pictures and demanding payment through premium-rate SMS to regain access and stop the images from being displayed.

The market share of Microsoft Windows creates a natural target environment for cybercriminals wanting to extract cash from their victims. However, it's important to note other platforms are not immune, with examples of ransomware attacks on Apple's OS X and on Google's Android operating systems.

TIGHTENING THE SCREW

Exfiltration combined with extortion may not be a new technique, but it is certainly a growing trend. Attacks take the form of bad actors exfiltrating a copy of sensitive data to their own environment and then encrypting and locking access to the data on the victims' servers. The sensitive data is then placed under threat of being published and sold or auctioned off if no ransom is paid. This technique is typically a long-play scenario on the part of the attacker, since they need to gain network access, identify the sensitive data and then exfiltrate a copy to their own environment.

Consider, for a moment, the incursion from the point of view of the cybercriminal: companies are becoming smarter, deploying technologies that thwart attacks, create resilient backup and restore processes and are demonstrating less pertinacity to hand over the cash. The bad actors need a "Plan B" to be able to monetize their effort and build resilience into the attack, rather than being reliant on a single form of threat: infect and encrypt. By adding "take a copy" to the mix, they build in resilience and a unique selling point in order to close the deal with their "customer" – the victim.

The Maze team is one such cybercriminal group that has been making their name with exfiltration and extortion attacks. At the end 2019, the group published details of data they claimed to have stolen from Southwire, a US based cable manufacturer, that refused to pay the $6m ransom. They then continued their nasty activity by publishing a list of companies that refused to cooperate and threatened publication of sensitive papers and data. In March 2020, as the world was awash with chaos as the COVID-19 pandemic took grip, the Maze group reportedly tweeted that due to the global crisis they would offer a discount to all companies not cooperating and would refrain from attacking medical organizations until the situation improved.

The long-play scenario of exfiltration and extortion requires the bad actors to possess a different skill set and a certain amount of patience. While many ransomware attacks have been about denying access, either by locking or encrypting, this growing trend of taking a copy requires the attackers to infiltrate a network and to move around undetected so that sensitive data can be identified and then copied. It is no longer about a simple phishing link or attachment in an email that an unsuspecting employee or consumer opens and unwittingly unleashes a ransomware attack. There still needs to be an initial point of entry, using techniques to exploit remote desktop protocol (RDP), brute-forcing their way in through credential-stuffing attacks or by the more traditional phishing and social engineering mechanisms.

Once in the network, it's a matter of remaining undetected, gathering information and collecting additional credentials and passwords to ensure that even if the initial route in closes, that access is retained. The groundwork and intelligence to map a network and understand what is valuable takes time and requires skilled resources to achieve the ultimate aim of identifying the company's digital crown jewels that would, if breached, locked or published cause the company the maximum disruption. It's only after the data has been stealthily removed that the bad actor can move to the more traditional deployment of ransomware. Through existing privileged access, the bad actor may have even taken the opportunity to disable protection software to ensure a successful attack.

THE CHANGING DEMANDS

The additional skill set and time required need to be funded and this can be seen with the changing demands being made by cybercriminals. In 2018 the city of Atlanta suffered a traditional-style ransomware attack. Key infrastructure servers were encrypted and the bad actors demanded $51,000 for a decryption method. Atlanta did the right thing – they refused to pay and rebuilt their systems, which reportedly cost them $9.5 million.

The last 18 months have seen the demands increase, unfortunately not with normal inflation. Lake City and Riviera Beach City in Florida *paid $500,000 and $600,000*, respectively. Lion, an Australian beverage company, refused to pay a $1 million demand and the University of California San Francisco had a demand for $3 million and paid $1.1 million. In a little over two years, the demands made on Atlanta seem miniscule, but there is definitely an unwanted increase in the amount being demanded – a trend that is very likely to continue.

The demand for payment in bitcoins is not the only metric that demonstrates that this is a changing landscape. Coalition, a cyber insurance company that serves 25,000 small and midsize businesses in north America recently *published a report* summarizing claims for the first half of 2020, which of course includes the start of the pandemic. The report stats "the average severity of claims reported by coalition policyholders increased by 65% from 2019 to 2020, in large part driven by the rising costs of ransomware." The report further details that 41% of all claims are ransomware and states that "more recently a number of ransomware groups are now stealing an organization's data prior to encrypting it, and then threatening to publicly expose the stolen data if a ransom is not paid." The independent data in the Coalition report provides a different perspective and confirms the change in the modus operandi used by cybercriminals and the increase in the amounts being demanded.

THE STAKES GO UP

Fast forward to August 2020, and yet another data breach story: Blackbaud, a cloud services company that provides fundraising software to organizations across the world, *announced they had successfully fended off a ransomware attack*. In cooperation with a digital forensics expert and law enforcement, the Blackbaud cybersecurity team had stopped the cybercriminal from encrypting data and locking them out of their own systems. However, the attacker quickly invoked a Plan B, offering, for a fee, to delete the sensitive customer data they had exfiltrated from the Blackbaud systems prior to being successfully removed by the cybersecurity team.

Blackbaud, shockingly, paid an undisclosed sum to the extortionist on condition that proof of deletion was provided. The resilience of having a Plan B paid dividends for the cybercriminal, despite the heroic efforts of the teams that thwarted the attack. Had the attack been limited to the more traditional compromise-and-encrypt scenario, we might never have even heard about the breach. Nevertheless, as the data copied (stolen) included personally identifiable information of individuals, the company was obligated in some locations by privacy legislation to inform customers and regulators that a data breach had occurred.

Thwarted attacks or diligent backup and restore processes may no longer be enough to fend off a committed cybercriminal who's demanding a ransom payment. The success in monetizing due to a change of technique – despite being more resource-intensive and requiring patience – offers cybercriminals an increased chance of a return on investment (ROI) – yes, it's a "business" judged on ROI. In the Blackbaud scenario, the ransomware attack neither deployed malicious software nor locked access to systems or data, another evolution of the term "ransomware". This is a trend that, unfortunately, I am sure we will witness more of in 2021.

3

BEYOND PREVENTION: KEEPING UP WITH THE SHIFTING SANDS OF CYBERTHREATS

Threat actors always look for ways to make their attacks harder to detect and thwart, including by co-opting a system's legitimate tools for nefarious ends. How can cyber defenders keep up?

Camilo Gutiérrez Amaya
ESET Senior Security Researcher

Ever since the concept of "computer virus" *appeared more than 30 years ago*, cybersecurity threats haven't stopped evolving; indeed, according to the *Global Risks Report 2020* of the World Economic Forum, cyber threats are among the top risks for humanity over the next ten years. Add to that the COVID-19 pandemic, which on top of all its dire consequences, has also increased the risks of suffering a security incident. This was confirmed by the uptick in attack attempts earlier this year as observed by multiple organizations, including the *United Nations* and the United Kingdom's *National Cyber Security Centre* (NCSC).

Against this background, we have witnessed in recent years how cybercriminal groups have turned to the use of increasingly complex techniques to deploy increasingly targeted attacks. Some time ago, the security community began to talk about "fileless malware" attacks, which piggyback on the operating system's own tools and processes and leverage them for malicious ends. In other words, the incursions co-opt pre-installed applications without the need to drop additional executables on the victim's system. Such executables were nicknamed LOLBaS ("Living Off the Land Binaries and Scripts") and since the end of 2017 the term began to be used to refer to evasive

techniques where attackers leverage binary executables that are already pre-installed on a system. Since these attacks can be difficult to detect, adversaries adopt these techniques in order to maximize the stealth and effectiveness of their attacks.

WHERE IT ALL STARTED

It is important to note that the use of these techniques is not something new. We saw how some malware families began to abuse these characteristics way back in 2001, when the *Code Red worm* appeared. In recent years, however, these techniques have gained more traction, having been employed in various cyberespionage campaigns and by various malicious actors, mainly to hit high-profile targets such as government entities. This was the case with *Operation In(ter)ception*, which involved attacks against military and aerospace companies in Europe and the Middle East, as well as with the *Evilnum* group and its attacks on the financial sector.

Many of the tactics, techniques and procedures (TTP) leveraged by these groups are outlined in the MITRE ATT&CK® framework. The best-documented TTPs include, arguably, those leveraged by *APT34*, also known as Lazarus Group, which made a name for itself in cybercrime with incursions such as the *attack on Sony Pictures in 2014*, through the *attacks against an online casino in Central America* in 2017 and lately due to *attacks targeting financial institutions* in Europe. As ESET researchers have found, the *Invisimole group* also bases its operations on the use of "living off the land" techniques with a complete set of tools to carry out cyberespionage campaigns. The incursions take advantage, for example, of vulnerable applications such as *Total Video Player* or *speedfan.sys*, in addition to legitimate components like *rundll32* and *wmiapiexec*, in order to remain under the radar.

That said, even a quick search in the MITRE ATT&CK® framework about the malicious use of binaries such as *certutil*, *esentutl* or *regsvr32*, to name just a few, turns up a large number of threat actors using these techniques. Even a cursory look at groups that use these three binaries reveals more than 100 different threat actors, including some of the world's most notorious APT groups, such as Turla, Machete, Fancy Bear and Cobalt Group.

In light of all the above, then, it can be reasonably expected that 2021 will be a year in which incidents leveraging these techniques will have a greater impact, with sectors such as critical infrastructure or the financial sector possibly being the most targeted.

UNDERSTANDING THE ATTACK MODELS TO BOLSTER YOUR DEFENSES

Courtesy of their use of legitimate programs, one of the main distinguishing features of these attacks is that they significantly reduce traces of criminal activity, as the malicious actions are loaded and executed from the computer's memory without affecting the file system. Consequently, these attacks generate little-to-no forensic artifacts that cyber defenders can analyze.

This may, of course, hamper the detection and, by extension, prevention of these attacks. The attacks are also particularly effective when an organization's security is geared towards whitelist-based detection technologies or when it lacks heuristics that provide advanced detection capabilities.

Since these attacks seek to evade most security solutions and thwart forensic analysis, another main feature underpinning these techniques is stealth. Attackers rely on a system's native tools such as PowerShell and WMI (Windows Management Instrumentation), which are designed to facilitate the automation of tasks and the management of operating system settings.

Attackers also often use these methods to achieve persistence, privilege escalation and even data exfiltration, whereas initial access is still commonly associated with exploiting vulnerabilities or social engineering campaigns. Therefore, there's a need to consider also other security management strategies that go beyond prevention technologies and center on detection and incident response.

SECURITY CHALLENGES FOR COMPANIES

The key part of an organization's approach to fending off fileless malware in 2021 involves strengthening internal processes and procedures that allow integrating technologies and people in order to monitor the entire lifecycle of a threat, from the moment an attacker seeks initial access into a system all the way until achieving data exfiltration or some other type of nefarious action. As a result, it is essential to consider several layers of technologies that allow visibility before, during and after an attack.

These types of capabilities are achieved with technologies such as endpoint detection and response (EDR), which enhance the defenders' visibility into what is happening within a network. In tandem with detection technologies, EDR can increase an organization's capacity to detect suspicious activities and stop behaviors seen as dangerous, all the while making it possible to investigate potential incidents that can be part of a larger attack and to isolate devices that could be compromised.

Fileless threats have been evolving rapidly and it is expected that in 2021 these methods will be used in increasingly complex and larger-scale attacks. This situation highlights the need for security teams to develop processes leveraging tools and technologies that not only prevent malicious code from compromising computer systems, but that also have detection and response capabilities – even before these attacks fulfill their mission. Pandemic-induced changes have accelerated the digital transformation in 2020, but the upcoming year ushers in new challenges for organizations, which should continue to adopt technologies that allow them to expand their visibility into, and monitoring of, anomalous behavior. Hence, it is vital for organizations to be equipped with the appropriate technical tools and a team of trained people who help detect incidents early and respond to them swiftly.

4

BAD VIBES: SECURITY FLAWS IN SMART SEX TOYS

How secure are sex toys? Are vendors doing enough to protect people's data and privacy? And why is security so critical when it comes to adult toys?

Cecilia Pastorino
ESET Security Researcher

Denise Giusto Bilić
ESET Security Researcher

It won't be news to anyone that Internet of Things (IoT) devices have vulnerabilities. ESET has found serious flaws in *multiple smart home hubs* and *smart cameras*. Also, *ESET researchers recently uncovered KRØØK*, a serious vulnerability that affected encryption of more than a billion Wi-Fi devices. Although IoT devices have been subject to countless security breaches leading to the exposure of people's login details, financial information, and geographical location there are few kinds of data with more potential to harm a user, if published, than those relating to their sexual behavior.

With new models of smart toys for adults entering the market all the time, we might imagine that progress is being made in strengthening the mechanisms to ensure good practices in the processing of user information. However, many researches have shown that we are a long way from being able to use smart sex toys without exposing ourselves to the risk of a cyberattack. Now these findings are more relevant than ever as we are seeing a rapid *rise in sex toy sales* as a consequence of social distancing measures related to COVID-19.

So how secure are adult toys now and what lies ahead? Have the necessary precautions been taken to protect people's data and privacy? Why is security so critical when it comes to sex toys?

HOW SECURITY COMES INTO PLAY

As one can imagine, the information processed by smart sex toys is extremely sensitive: names, sexual preferences and orientations, list of sexual partners, information about device usage, intimate photos and videos – all these pieces of information can result in disastrous consequences if they fall into the wrong hands.

Who could be interested in this type of information? Many countries have laws that expressly *prohibit citizens from engaging in certain sexual practices*. What would happen if local authorities launched an oppressive campaign based on the forceful expropriation of data from the companies that process them, or the exploitation of bugs or weaknesses in sex devices as a way to identify, locate, and persecute gays, adulterers or anyone else belonging to a minority or social group on grounds of their sexual choices? In addition, sex toys are not exempt from the possibility of being compromised by cyberattackers. New forms of *sextortion* appear on the radar if we consider the intimate material accessible through the apps that control these devices.

As well as concerns about data confidentiality, we must consider the possibility that vulnerabilities in the app could allow malware to be installed on the phone, or firmware to be changed in the toys. These situations could lead to DoS (Denial of Service) attacks that block any commands from being delivered, such as what happened with a *smart male chastity cage that has recently been proved vulnerable* to being exploited by attackers who could lock them in masse, potentially trapping thousands of users. A device could also be weaponized to carry out malicious actions and propagate malware, or even be deliberately modified to cause physical harm to the user, such as by overheating and exploding.

Alongside this, we cannot talk about the implications of an attack on a sexual device without also reassessing the significance of sexual abuse in the context of the digital transformation that society is going through. What are the consequences of someone being able to take control of a sexual device without consent? Could that be described as an act of sexual assault? The notion of cybercrime takes on a different appearance if we look at it from the perspective of invasion of privacy, abuse of power, and lack of consent for a sex act. Consent obtained through fraud is no consent at all, and this legislative gap in current laws will need to be resolved in order to ensure the sexual, physical, and psychological safety of users in the digital arena.

ATTACK SURFACE OF A SMART SEX TOY

In terms of their architecture, most of these devices can be controlled via Bluetooth Low Energy (BLE) from an app installed on a smartphone. In this way, the sex toys act as sensors, which only collect data and send it to the app to be processed. The app is then responsible for setting any options on the device and controlling the user's authentication process. To do so, it connects through Wi-Fi to a server in the cloud, which stores the person's account information. In some cases, the app also acts as an intermediary between various users seeking to use features like chat, videoconferencing and file transfers, or if they want to give control of their device to remote users by sharing tokens with them.

Some vendors offer users the possibility to connect to their devices by installing software on their computers and using a special BLE dongle. You can also use the BLE API in certain browsers to connect to the sex toys using a web app. The numerous ways in which you can connect to the devices provide more flexibility, but also increase the attack surface.

So what could go wrong? This architecture presents several weak spots that could be used to compromise the security of the data being processed: intercepting the local communication between the controlling app and the device, between the app and the cloud, between the remote phone and the cloud, or directly attacking the backend. Of course, not all attacks take place over network connections and some malicious scenarios could be launched using malware previously installed on the phone or by exploiting bugs in the operating system.

Many security researchers (*[1]*, *[2]*, *[3]*, *[4]*, among others) have proven that these devices contain security flaws that could threaten the security of the data stored as well as the user's safety. The loopholes ranged from poor authentication procedures to devices that constantly publicize their presence, allowing anyone to connect to them.

In 2016, two researchers presented a talk entitled "*Hacking the Internet of Vibrating Things.*" They showed how information such as intensity, patterns, temperature and user habits were collected by the *We-Connect* application and sent back to the servers with no anonymization at all. Last year, a researcher showed *how easy it could be for an attacker to hack a butt plug* controlled over BLE. It was also the first proof of concept where a smart sex device could be weaponized and used to harm the person using it.

This year, the ESET Latin America research team presented at DEF CON IoT Village *new research regarding insecure smart sex toys*. The investigation was based on two devices: a wearable device called Jive, manufactured by We-Vibe, and the Max male masturbator from Lovense.

We found that both devices had vulnerabilities in the implementation of BLE communications, allowing attackers to intercept the data being sent and remotely control the devices through BLE MitM (man-in-the-middle) attacks. This implies that anyone could use a simple Bluetooth scanner to locate and control these smart sex toys in their vicinity, similar to what researcher Alex Lomas did back in 2017 while *walking the streets of Berlin and discovering sex toys*. This vulnerability is very common in IoT devices since most of the models that are available in the market do not implement secure paring, which allows anyone to connect and control them.

Regarding the *Lovense Remote* app, we found some controversial design choices that may threaten the confidentiality of intimate images sent by users. There was no end-to-end encryption, screen captures were not disabled, the "delete" option in the chat did not actually erase messages from the remote phone, and users could download and forward content from others without a warning. Also, malicious users could find out the email addresses associated with any given username and vice versa. These findings constitute serious privacy concerns, especially in an app specifically designed to share sexual content.

The app lets users grant remote control of their devices via a URL, which includes a 4-digit token. We also encountered security issues with this token that would allow attackers to hijack random remote devices without consent.

In the *We-Connect* app, we realized that sensitive metadata was not being stripped from files before they were sent, which means that users may have been inadvertently sending information about their devices and their exact geolocation when sexting with another users. This could be very dangerous, since many users grant control of their devices to complete strangers by sharing their tokens online, both as a personal preference or as part of a "cam girl/boy" service.

BEST PRACTICES TO AVOID RISKS

Smart sex toys are gaining popularity as part of the concept of "sexnology," a combination of sex and technology. These practices may well be here to stay, but we must not forget the potential threats to users' privacy and intimacy.

To minimize the risks associated with the use of smart sex devices, we recommend keeping in mind the following advice:

1. Some apps offer the possibility to control devices locally via BLE without creating a user account. If you are not planning on letting other users control your device remotely over the internet, look for one of these devices.

2. As much as possible, avoid sharing photos or videos in which you can be identified and do not post remote control tokens on the Internet.

3. Avoid registering for sex apps using an official name or email address that could identify you.

4. Always read the terms and conditions of apps and websites for which you register.

5. Use smart sex toys in a protected environment and avoid using them in public places or areas with people passing through (like hotels).

6. Downloading the apps and trying out their features before buying the device can give you an overview of how secure the product is. Use search engines to find out if the model you are thinking of buying has had vulnerabilities in the past.

7. Always protect the mobile devices you use to control these gadgets, keep them updated and have a security solution installed on them.

8. Protect the home Wi-Fi network you use for the connection with strong passwords, securely encrypted algorithms and regular updating of the router's firmware.

WHAT'S NEXT?

The era of smart sex toys is just beginning. The latest advances in the industry include *models with VR (Virtual Reality) capabilities* and AI-powered sex robots that include cameras, microphones and voice analysis capabilities based on artificial intelligence techniques. The *use of these robots as replacements for sex workers in brothels* is already a reality.

These sex toys are only a small expression of sexuality in the digital world, an area that we could argue also includes dating apps and other devices such as *"virtual girlfriends"*, the technological manifestation of a bigger sociological phenomenon that is transforming our society as IoT devices keep seeping into our lives.

As has been proven time and time again, secure development and *public awareness* will be key to ensuring the protection of sensitive data, while we empower users to become smart consumers who are able to *demand better practices from vendors* in order to maintain control of their digital intimacy in the years to come.

CONCLUSION

Even when the tide begins to turn and we resume a measure of pre-pandemic life, we shouldn't let our guards down. Complacency, they say, is the enemy of progress. It also happens to be an enemy of security.

When the COVID-19 pandemic struck, much of normal life ground to a screeching halt and a new reality set in. Even the Earth itself suddenly became quieter and *moved less* as we hunkered down, carving out working spaces in our homes and learning to cope with being cooped up. The lockdowns and other aspects of what has come to be called the new normal brought about changes in our collective habits and even shifts in our perceptions of time and place.

With the world in the throes of the worst crisis in decades, we've had to come to grips with heightened uncertainty about health, relationships, finances and the future. The pandemic and its ripple effects have taught us a slew of science terms and caused many of us to reinvent ourselves. Even more importantly, however, the pandemic has taught us some important life lessons, bringing into sharp relief what is important and what isn't.

As stay-at-home orders were put in place, our lives shifted into the online realm and the digital transformation was pushed into overdrive. Technology is helping us maintain some social and emotional wellbeing and support the public health response to the pandemic. Working patterns were also upended as many companies scrambled to keep their operations running by taking their business online and pivoting to a remote workforce almost overnight. The internet has become almost our sole window into the world.

These realities, however, also conspired to create a near-perfect storm of cyber-risks. Organizations and the newly distributed workforce had to swim (or sink) in the largely uncharted waters of remote work, often unwittingly revealing chinks in their armors. Cybercriminals were quick to adjust their tactics to take advantage of the expanding attack surface and the target-rich environment, including by capitalizing on people's fear of the virus.

The trend of going all-in on remote work also helped uncover and address some privacy and security issues in platforms that after a surge in popularity attracted a wave of scrutiny. These developments, in turn, helped make it abundantly clear that the security side of things needs to be a top priority for everybody, a fact made all the more salient as technology was instrumental in dealing with the widespread social disruption.

Then there's also a long list of familiar threats, such as ransomware, that didn't go anywhere this year. Rather the contrary, they continued to evolve, which is what they normally do, and hit the victims harder than ever before. Our review of the recent major developments on the ransomware scene, showed how the stakes are going up for the victims, as well as that these attacks are a persistent reality that will, as cliché as it sounds, continue to evolve.

It's that time of year when we pause to look back at themes that defined the year that's ending, as well as reflect on what lies ahead for us. While this process has a ring of familiarity to it, a lot feels – and is – different this time. Still, we need to look ahead, including into the post-pandemic future. And even when the tide begins to turn and we resume a measure of normal life, we shouldn't let our guards down, be it offline or online. Complacency, they say, is the enemy of progress. It also happens to be an enemy of security.

CYBERSECURITY
EXPERTS ON YOUR SIDE