

CYBERSECURITY TRENDS 2023:

Securing our hybrid lives



Digital Security
Progress. Protected.

TABLE OF CONTENTS



INTRODUCTION

3



1 HYBRID WORK: Turning business platforms into preferred social spaces

4 – 5



2 HYBRID COMMERCE: Blurring the lines between business and pleasure

6 – 8



3 HYBRID PLAY: Leveling the playing field in online video gaming and beyond

9 – 11



CONCLUSION

12

INTRODUCTION

Living a hybrid life, counting benefits and costs



James Shepperd
ESET Security Editor

ESET's predicted trend for 2023 is that the changes in human behavior online, expressed in both professional and personal lives, will further blur the line between the physical world and our engineered virtual worlds. As security professionals, we are confronting the implications of these changes across the IT ecosystem, especially from cloud-powered apps to which we all increasingly entrust our enjoyment, professional success, privacy, and security.

However we got here (certainly helped along through COVID-19 lockdowns), we're here now! And where is that exactly? Likely, even now we are logged in to our preferred cloud-powered environment. We are talking about large-scale, cloud-enabled digital environments like Discord, Slack, and Microsoft Teams. We could in-

clude many social apps like Facebook, WhatsApp, LinkedIn, and Tinder, or even games like Fortnite and VALORANT. There are too many to count, but all forecast one reality: millions of IT users forging their hybrid lives and recasting our definitions of security and privacy.

This super bloom of cloud-powered environments has brought unimagined opportunities to create, collaborate, buy, sell, and play. Going beyond the scope of previous cloud-based technologies, which first freed users from limitations associated with hardware costs and long intervals between updates, today's cloud-based environments bring transformative hybrid opportunities. And while we have gone all in on what the cloud can do for us, unforeseen dangers await.

HYBRID LIVES POWERED BY THE CLOUD AND SECURED BY...?

Along with great opportunities, the immersive multi-featured cloud-powered environments we've adopted for work, play, education, data storage, and connected lifestyles have also opened up pathways for cybercrime. The scale of these always up-to-date platforms, with millions of users logged in concurrently from desktop, mobile, and Internet of Things (IoT) devices, has a hand in creating a massive, shared threat surface.

With some cloud-powered environments even offering the rawest of material – free server space – all have the potential to help create, house, and share vast amounts of personal data and intellectual property, even to millions of fellow users. Herein, this wealth of human expression is simultaneously a wealth of data tempting everyone from average joes to entrepreneurs to seasoned cybercriminals.

HYBRID WORK: TURNING BUSINESS PLATFORMS INTO PREFERRED SOCIAL SPACES

Hybrid work and hybrid play now merge into hybrid living, but where is the line between the two? Is there one?



Alžbeta Koval'ová

ESET Security Writer

That the pandemic brought a new normal to businesses, educational institutions, and our everyday lives is an understatement. Many interactions, whether work-related or personal, moved online or at least gained a virtual mirror. This virtual migration began alongside the pandemic when most people and businesses first turned to tried-and-tested communications solutions, such as Microsoft Teams, Slack, and Zoom, which merged rich communication functions with collaboration and productivity tools to help compensate for lost in-person work.

Together with Skype and Skype for Business, all were known entities before our “new normal”; however, the shift to hybrid work, study, and play saw these platforms explode in popularity. As cloud-based solutions, shared access and files, parallel workflows, instant messaging, and more were all easily accessible. But all ups have their downs.

Anything that becomes widely popular also becomes attractive to attackers. This holds true of cloud-based platforms too. Cloud-based cyberattacks accounted for [20% of all cyberattacks in 2020](#). Because the popularity of cloud-powered services isn't wavering, neither is the interest of attackers. Let's look at three platforms mentioned above to identify a trend: apps designed for work but transformed by popular demand into a social communication platform.

SECURING THE CONVENIENCE OF HYBRID LIFE

Microsoft Teams, launched in 2017, is now the fastest-growing Microsoft app and go-to communications tool. [Teams has seen explosive growth](#) from early in the pandemic. The annual number of Teams users nearly doubled between 2020 and 2021, and in 2022, users numbered 270 million, most of whom are of working age (35-54 years old). The choice of many, Teams has moved beyond its intended business setting and is now commonly used in education and has gained a role in people's personal lives.

Microsoft Teams is a convenient option among communication apps, but it is not without risks. In [2021](#), a vulnerability was discovered in Teams that allowed malicious insiders to steal emails, Teams messages, and OneDrive and SharePoint files. More recently, in [August 2022](#), a post-exploitation opportunity was discovered due to Teams storing access tokens in plaintext on disk, thus making them easier to steal should an attacker somehow first manage to compromise a victimized computer. For some, weaknesses like these indicate that cloud-based solutions are [more susceptible to attacks](#) than on-premises solutions and thus need a special layer of cloud-based protection.

Another cloud-based solution for videoconferencing that has become a household name in recent years is Zoom. This peer-to-peer software platform saw a [massive boom](#) during the pandemic as people began working, socializing, and attending events online. Zoom seemed to be the perfect option, as it didn't require having an account to attend an event. It also has a free version with limited functionalities.

Of course, Zoom's wide use brought with it the attention of security professionals and ill-intentioned actors alike. The platform has [come under the spotlight](#) a number of times since 2020, including for privacy and security issues that were not of its own making. In one widely publicized issue, the former UK Prime Minister Boris Johnson came under fire for inadvertently [revealing a Zoom meeting ID](#) for a Cabinet meeting, which raised concerns about the meetings being exposed to a heightened risk of eavesdropping and attacks known as Zoombombing.

Also early into the pandemic, hackers gathered more than [500,000 Zoom usernames and passwords](#) via an attack known as credential stuffing before putting the logins up for grabs on the dark web. Another type of issue involved security vulnerabilities, including one that affected the Zoom app for macOS and could have given hackers [root access to macOS](#) desktops. Fast forward to early 2022, and [Google's Project Zero team](#) revealed a buffer overflow and an info leak vulnerability in Zoom that, before it was remedied, could have allowed threat actors to monitor Zoom meetings. Some of these issues were followed by reports of phishing and other social engineering attacks, which are known for being [the top vector](#) for malware delivery.

INHERITING THE RISKS OF SUCCESS – A PATTERN

Similarly, the abovementioned productivity app, Slack, which claims to reduce the need for emails by 32% and meetings by 27%, is also a victim of its success. This instant messaging platform allows users to make voice calls and video chats, and send messages and media files in private chats or as part of a community (workspace). This app reports over 12 million daily users while being compatible with all major operating systems. According to one estimate, an average user is on the app for at least [10 hours a week](#). Slack is used by more than 100,000 organizations worldwide and offers a paid tier called Slack Connect that includes a secure messaging feature used by over 10,000 organizations.

However, Slack comes with its fair share of vulnerabilities and risks to users too. A more [recent vulnerability](#) was reported in 2019. It allowed attackers to exploit a vulnerability in Slack Desktop for Windows to alter where files sent through a Slack channel are downloaded, ultimately allowing them to inject malware into the files or steal them. This, of course, is not the first security issue, as major flaws were found as early as [2015](#).

One of Slack's more obvious downsides seems to be its open communities feature, allowing large groups of people to connect. Like email, Slack has become a perfect vector for phishing and spam.

HYBRID COMMERCE: BLURRING THE LINES BETWEEN BUSINESS AND PLEASURE

It is now acceptable to find a job on a dating app!



André Lameiras
ESET Security Writer

Although many enterprises and small and medium businesses (SMBs) take advantage of solutions such as Slack or Microsoft Teams for collaborative work, these platforms are still trying to figure out better ways to create meaningful interactions between staff members. While these companies prioritize workflow, there's also a growing need to reinforce social connections through a virtual company culture that enhances engagement and a feeling of belonging among workers, both with those who work remotely and those who work in hybrid mode. These virtual hallways are, in many ways, a needed replacement for in-between discussions that typically happen by the copier or in the office corridors.

"SOCIAL" PAST ITS PEAK?

In Q4 2021, well into the pandemic, Facebook saw its user numbers [drop for the first time in 18 years](#) – losing approximately half a million users. Though since rebounding, did this episode signal that traditional social media platforms are past their apex?

Since [the internet went “social” on the wave of Web 2.0](#), around 2004, social networks started mimicking the everyday interactions of life: lists of friends with whom we could share photos, thoughts, and other multimedia content. But while in real life you can meet one group of friends one day and another the day after, on social media they were encouraged to mix. Suddenly, it became acceptable for work colleagues to send friend requests and, very quickly, it became awkward not to accept. Google tried to solve this by launching Google+, a social network that would divide the people you connect with into different circles, just like in real life. But the idea didn't have much success.

Meanwhile, the internet got so used to Facebook that, by 2015, the platform had [reached 1.44 billion users](#) and acquired Instagram and WhatsApp. It quickly became the “new normal” for work colleagues to message each other about work during and after work hours, connecting employees in a way that never existed before. While this could be a positive – for example, enhancing company culture – it didn't take long for employees to start discussing “the right to disconnect”; after all, no one wanted to receive texts about work at dinnertime or to share vacation pictures with their bosses. And in the office, managers didn't want employees to lose time with social interactions. But it was too late.

DEMOCRATIZING BUSINESS TOOLS

Simultaneously, people were also starting small businesses on Facebook, initially taking advantage of “buy and sell” groups and, from 2016, using the platform's new Marketplace. Freelancers started using personal pages to promote their work, teachers shared class notes, and small bookshops promoted their new arrivals. Everything was possible without even having an official business account with pro features and complex analytics; it was anyone's game.

By the end of 2020, it was already so common to do business via these social media platforms that Facebook launched the Facebook Business Suite app to allow small businesses to manage their content, messages, and analytics for Facebook and Instagram in one place. And since November 2022, all Facebook users can “re-purpose” their personal profile into “professional mode”,

a new capability designed to support new content creators by giving them access to analytics and monetization programs, including the possibility of receiving money directly from fans.

WORK TRICKLING INTO OUR SOCIAL LIVES

Running a successful business may demand an “always on” status, but to be “always on” is more than just sitting at your PC in the office. Clearly our work is no longer confined there. Our work is in our pockets, on our phones, and just next to our personal pictures. This concentration of data, data processing and creation tools (your camera included), and communication tools, all in one, is a big shift in how we organize our lives. Any app developer worth their salt knows this.

Telegram, a cloud-based instant messaging service with over 700 million active users worldwide and with apps for all devices, is also becoming an increasingly capable mobile workspace. The app allows for the creation of groups and channels (like on Slack or Teams), file sharing up to 4GB, and folders that prompt users to use their existing accounts to create a dedicated space just for workflow, right there between the family and gaming chats. It persistently pings users with notifications from work, even during a vacation, if not turned off.

Even if some users benefit from the nascent legislation on [the right to disconnect](#), everyone is affected by the data policies of their favored cloud-provided service. While this should be a concern for both personal and work data, at minimum, companies should use apps that encrypt data and collect only minimal data, and preferably use apps that [store all messages and media locally](#) on the user's device.

In parallel, there are a host of other messaging apps being repurposed for business that several million people use: dating apps. Surprisingly, these too are used for professional networking, finding new clients, hiring, and job hunting. In 2020, at the start of the pandemic, the dating app Bumble created the “Community Grants” profile, which looks just like [a regular user's profile](#). By swiping right on it, users are matched and requested to nominate a local SMB in need of financial support due to

the lockdowns. Bumble pledges to choose 200 businesses and award them up to a USD\$5,000 grant. While its primary focus is dating, [Bumble also offers a Bizz mode](#) that facilitates meetings between professionals.

THE RISKS OF MIXING PROFESSIONAL AND PERSONAL LIVES

Mixing business with your social life is a growing trend. Tinder, for example, offers the possibility to run ads, and many [freelancers](#) and SMB owners take advantage of their personal profiles to get new customers to swipe right. If a customer becomes a date, even better! Being an entrepreneur seems to be a trending characteristic. According to a [Shopify survey published last year](#), from April 2020 to July 2021, Tinder registered a 25% increase in mentions of users' entrepreneurial experiences in their bio, which seems to be a characteristic appreciated by 71% of the app's users.

While these apps do not allow commercial activities, a conversation with someone self-described as a gym addict can easily lead to being sold a personal trainer service; a wine exporter can try to sell a few bottles; a coffee shop owner will be thrilled to connect with someone over a coffee.

But while this could be seen as a creative solution, it can create real problems. Blurring use cases for apps across the personal and professional can have serious consequences. Falling for a phishing scam on WhatsApp can prompt the download of malware that steals both personal and work messages. Dating app scammers and criminals might abuse someone's aim to network and sell in order to acquire information about a business. Even in an office environment, sharing information online that is intended for friends but that colleagues might access – such as pictures on Facebook or your presence on mobile apps such as Grindr or Happn – might end up with unwanted attention or be used for stalking, [doxing](#) or professional gain.

But there's more. Just recently, Meta [disciplined or fired](#) more than two dozen workers for allegedly misusing internal systems to hijack users' accounts, in some cases in exchange for thousands of dollars. While this might

not be a widespread problem, nothing guarantees that this is not happening at other companies. And even if the target might be a personal account, work details exchanged using that account is icing on the cake once in criminal hands.

Indeed, some employees might be more interesting targets than others, depending on how much data they have access to. And that can be an important factor when imposing more restrictive measures on staff with higher exposure. But this can also be misleading, as every employee in a company is connected, and it might be easier to steal information from someone who is not perceived as an obvious target.

Back to that overlap between professional and personal. As we go through cultural changes around how we communicate, work, and live, we can't ignore how our online and offline lives have merged, creating new risks that must be avoided by establishing clear rules.

If businesses expect employees to be available anytime, they must be prepared to end [Bring Your Own Device](#) policies to ensure a clear division between personal and private life. This means giving employees dedicated work devices – not just laptops, but smartphones as well. Companies ensure that both they and their employees know the consequences of using the same device for both work and private life.

Other priorities stand out too. Companies should stop providing configuration profiles that employees can install on their personal iOS devices to access their work email and other work platforms. On top of this, it is essential to implement clear password rules to discourage employees from using the same password for personal and work accounts and require multifactor authentication. The future is full of amazing technologies, collaboration tools, and more humanized online social experiences, but they will continue to blur the thin line that divides different spheres of life.

HYBRID PLAY: LEVELING THE PLAYING FIELD IN ONLINE VIDEO GAMING AND BEYOND

Does VALORANT's approach to cheating signal a turning point in how we deal with the continued hacks afflicting our hybrid world of work and play?



Rene Holt
ESET Security Writer

FIRST SOCIAL APPS, NOW GAMING?

So far, we can see how the growth of cloud-powered apps like Telegram and Teams has created mega communities out of their users. Many of these apps have opened the door to personal self-expression and the types of risk-taking notorious on social media platforms. Oversharing, connecting with strangers, clickbait, and phishing are now part and parcel of our work, and social and gaming lives; the lines are far too blurred in our hybrid lives for the risks to disappear.

But what about the free server space in the cloud, where millions of gamers, educators, and [students](#) are participating in a brave new world of digital possibility and risk? In Discord's now well-established platform, we find a kind of "natural selection" manipulated by moderators and bots, and an "evolution" happening in real time as communities adapt to new members' expectations for performance, fun, profitability, gameplay, fairness, and security.

What is Discord?

Born as a communication platform for the gamer community, Discord offers any community a cloud server with text and voice channels, along with screen sharing and file upload capabilities. Each community can set its own rules for and moderate how members interact with each other. Discord even offers developers a programming interface for creating bots and webhooks. Because of its rich collaboration features, threat actors have increasingly been abusing Discord for malware distribution, data exfiltration, and Command and Control (C&C) communication.

To highlight the changes taking place in the gaming space, let's look at what the members of one of Discord's largest gaming communities have been up to in their hybrid lives – sharing their passion for VALORANT while fighting against the tide of cheating spreading across the gaming landscape.

VALORANT: GAINING POPULARITY IN A HYBRID WORLD

For some businesses, 2020 brought lockdowns that triggered a renewed look at the cloud as a transformation needed for business continuity. But for others, like Riot Games, who had already been using the cloud as the core enabler for their business model, plans rolled ahead with Riot Games releasing VALORANT, a free-to-play online multiplayer first-person shooter. Two years later, around 700,000 fans are playing this game daily, and a million have joined the official VALORANT Discord server – making it the most popular server since August 2022.

Does the rapid growth of VALORANT's popularity indicate uniquely attractive gameplay? If yes, how has VALORANT approached the perennial problem of cheating? Finally, how will this approach affect other parts of our hybrid, cloud-enabled world, and is there a link?

THE GAMEPLAY ATTRACTION

VALORANT is attractive because it demands accountability. If a player dodges the queue, goes Away From Keyboard (AFK), or commits friendly fire, the game may impose a penalty of a timeout or a loss of points. Repeated offenses merit increasing penalties.

The game also demands fairness. Players can go up against each other in Competitive matches only if they are of similar rank and skill. Smurfing, where experienced players go on a killing spree of amateurs to boost their stats, is limited by requiring Account Level 20 to play competitively.

Finally, VALORANT promotes skill and teamwork. As novices, players hone their aim, the different Agents' special abilities, and their familiarity with the game maps. But as more experienced players, who each have a similarly high level of aim, teamwork and strategy become increasingly critical to winning matches.

PROTECTING THE GAME WITH ANTI-CHEAT SOFTWARE

All of this effort to promote fair, competitive gameplay is safeguarded by requiring players to run the anti-cheat software Vanguard at the same time as VALORANT. Vanguard uses a kernel-mode driver to identify vulnerable drivers on the gamer's computer and either block them from running or prevent VALORANT from running. Since this driver runs when the computer boots up, it can detect attempts to load cheats prior to starting the game. Vanguard also has a user-mode client application that monitors gameplay for the use of cheats such as aimbots.

Cheating is also handled by the security features built into VALORANT. For example, the game uses a Fog of War system to prevent wallhacks, where cheaters see opponents through walls. The punishment for cheating could go as far as a hardware ban of the cheater's computer.

The discussions around this aggressive approach to the tech's implementation and how players feel about the implications to the independent function of their PCs have been active. Although some may criticize anti-cheat software as spyware, putting the Vanguard client application under the microscope of a detection and response tool like [ESET Inspect](#) reveals a different picture. The ESET Inspect console only flags Vanguard injecting a thread into the virtual address space of the VALORANT process, thus giving Vanguard a deep look into VALORANT. Considering the purpose of anti-cheat software, this is an entirely unsuspecting action.

Figure 1 shows `vgc.exe`, the Vanguard client executable, triggering a `CodeInjection` event affecting `valorant.exe`, the game executable.

Ultimately, the attractiveness of VALORANT lies in its focus on skill development, teamwork, and strategy to win matches – a focus that is secured by its strong approach against cheating and sabotage.

RIPPLING EFFECTS IN A HYBRID WORLD

The shift from playing games offline to an age of online multiplayer games and esports has dragged in the curse

of cheating. Cheats are the plague of the esports world, just as malware is of the internet. Indeed, the relationship runs deeper because the development of cheats requires the same tools and know-how used by vulnerability researchers and malware developers. Some even consider cheat development as [the gateway drug to malware development](#).

This places anti-cheat software in a comparable role to security software and, indeed, in the same role of confronting some of the same exploitation techniques used by malware authors. Tackling the problem of cheats thus has strong parallels with tackling the problem of malware, requiring the identification and monitoring of the techniques used to gain an illicit advantage or control over another.

As we progress in a world transformed by the continued cloudification of traditionally offline activities, holding cheaters and hackers accountable will be critical to securing that progress. Only in this way can the excitement of the game, or whatever hybrid activity we participate in, keep its unalloyed appeal.

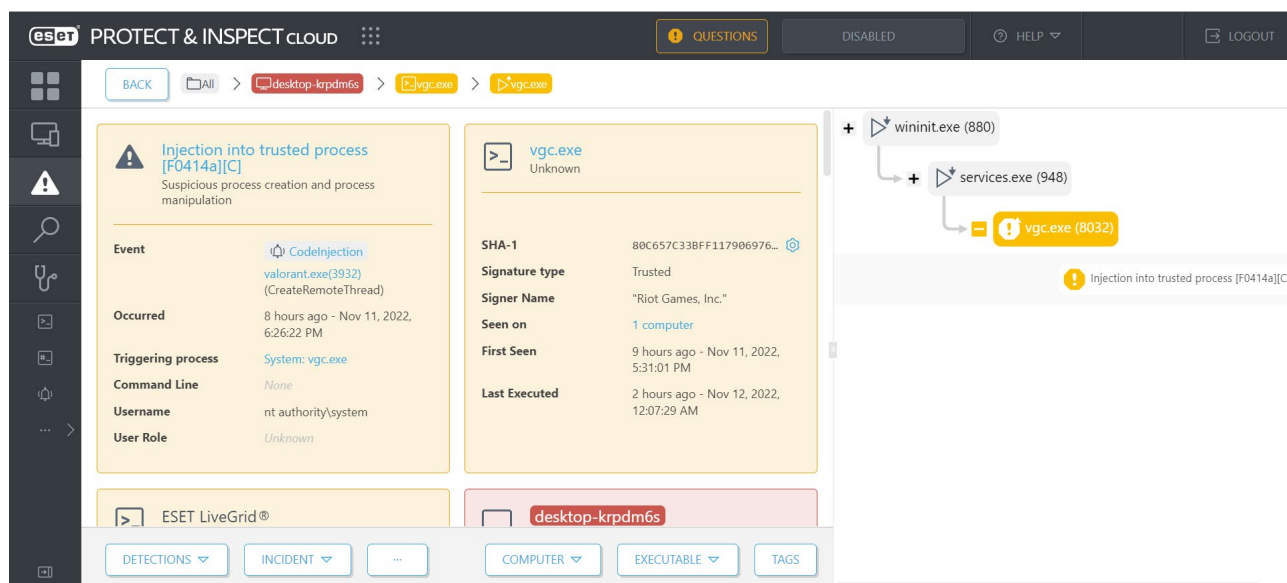


Figure 1. ESET Inspect reveals Vanguard injecting a thread into the VALORANT process

CONCLUSION

With multiple cloud-powered apps in both our hands and pockets, we have crossed a threshold – one that is taking us to a new dimension of how we work, socialize, and play. However, we are not just passive spectators caught up in a web of virtual environments, but active participants who create our own communities and influence the shapes of others. Escaping this hybrid life is almost unimaginable, perhaps leaving only one option: striking forth boldly ... but with caution.

After all, we've seen the slew of security issues affecting business apps like Teams, Zoom, and Slack. Even though remedied, we should not think these types of issues have been tidied up and are of no further concern. The hybrid workplace we live in is imbued with the power of metamorphosis. What began as work apps have transformed into social communication platforms, meaning that a whole new vector for security and privacy risks has penetrated this landscape.

With the move of business into the social sphere, these platforms have their work cut out. But they are not alone in this task. They represent one force competing inside a melting pot of platforms. Popular communication apps like Facebook, Telegram, and Bumble are another force. Originally social apps but, again, imbued with the power of metamorphosis. We see them being repurposed for business users, bringing both success and new cyber risks in their wake.

All these cloud-powered apps, platforms, and environments have created mega communities out of their users, with one of the largest being gamers. And where are the gamers? Well, probably on Discord servers for their favorite games. But just as the cyberbattle against hacks threatening our hybrid lives persists, so does the battle against cheating in games. It is a phenomenon looking at itself in the mirror.

Can the gaming community's response to cheating be instructive for our own hybrid world? Using anti-cheat software is one approach, but are there broader implications to in-game surveillance by algorithms that monitor behavior, relationships, and playing patterns? The same question is potentially applicable beyond gaming, regardless of the cloud-powered environment we might belong too.

By running through these popular cloud-powered apps, platforms, environments, and games, we hope to have shown how deeply we have become entrenched in our hybrid lives. Although fusion can improve our human and social experience, it is a reminder that well-defined limits can help ensure we continue to enjoy the benefits via a continued focus on privacy and security, just like we do in the physical world.



Digital Security
Progress. Protected.