Darknet Threat Actors Are Not Playing Games with the Gaming Industry

ke-la.com/darknet-threat-actors-are-not-playing-games-with-the-gaming-industry/

January 4, 2021

The gaming industry should really thank Covid-19: People are stuck at home, seeking indoor hobbies, and giving online gaming a chance. With the rise of gamers and purchases, the online gaming industry is estimated to reach $196 billion in revenue by 2022. However, the growing success of this industry also calls attention to cybercriminals scouting out their new targets – and what better target could cybercriminals ask for than an industry that's up and coming and may not be prioritizing their security precautions as much as their industry advancement and profit. So, though this industry isn't valued at the trillions of dollars that the financial industry may be valued at, it still checks off boxes for two key factors that many profit-driven cyber criminals tend to seek: increase profits and minimize the complexity of the process in order to do so.

- In order to assess the threat landscape of the gaming industry in light of Covid-19, we explored the risks that are potentially threatening employees and internal resources of the leaders of this industry.[1] We've included some of this blog's major key takeaways below:
- KELA observed **multiple instances of supply and demand for initial network access of gaming companies** (especially their resources designed for developers).
- KELA found nearly **1 million compromised accounts pertaining to gaming clients and employees, with 50% of them offered for sale during 2020.**
- KELA detected **more than 500,000 leaked credentials** pertaining to employees of the leading companies in the gaming sector.
- The gaming industry is growing, in turn increasing the number of threats against it. By **proactively monitoring darknet communities**, organizations in this industry can **collect real-time valuable intelligence in order to help gain an external viewpoint on their organizations' attack surfaces and mitigate cyber threats**.

Terms

Before diving into some threats targeting the gaming sector and the implications they may have, let's first review three commonly used terms throughout this blog post:

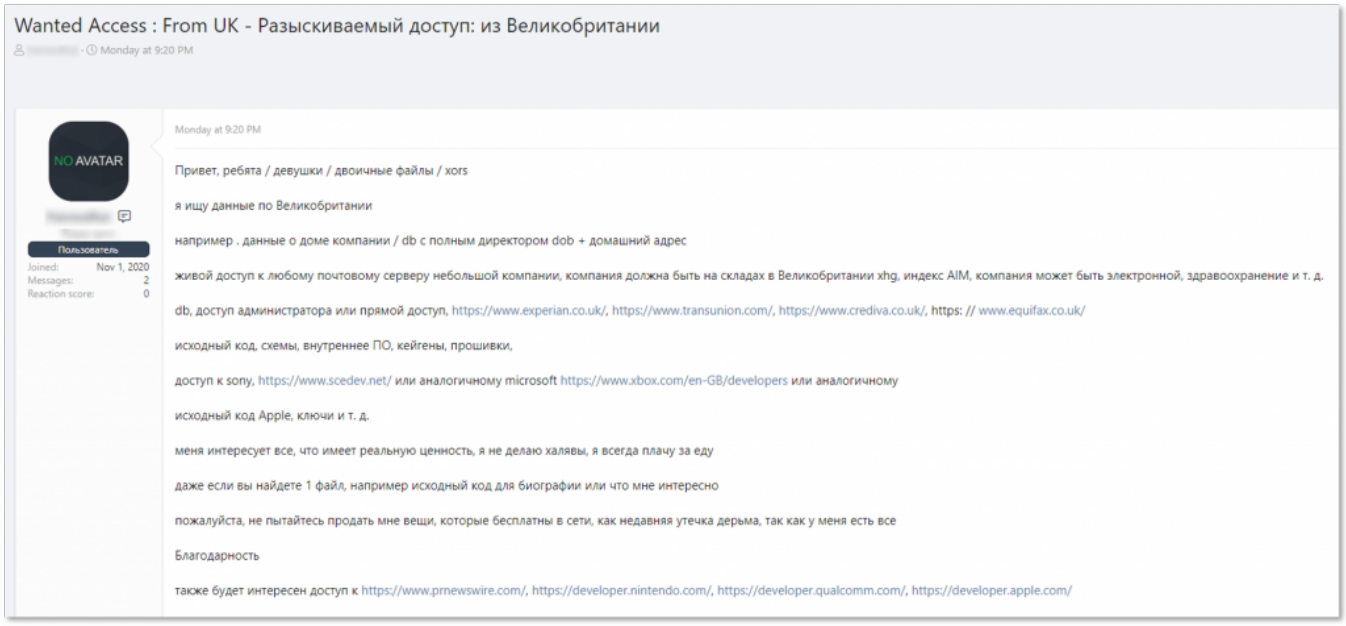
- **Initial Network Access** – A broad term referring to remote access to a computer in a compromised organization. Threat actors selling these accesses are referred to as *initial access brokers* – threat actors linking opportunistic campaigns with targeted attackers, namely ransomware operators.
- **Compromised Accounts** – Credentials, cookie sessions and additional technical fingerprints which are offered for sale on automated underground marketplaces such as Genesis and more. These accounts are breached and stolen from victims' computers generally via infections by banking trojans or other stealers. Such accounts can grant access to tools and software used in a targeted environment, such as RDP, VPN solutions, and more. They could be leveraged by a sophisticated actor to gain initial network access to the relevant corporate's network.
- **Leaked Credentials** – Credentials from various breached databases constantly traded and circulating in the underground. Mostly, these databases include private and corporate email addresses and associated passwords, including plaintext ones. This data can enable attackers to access the company's resources and provide further malicious activity, such as account takeover attacks, social engineering, phishing and malware spreading campaigns.

All these threats, altogether or separately, can be used in an attack chain aimed to compromise organizations.

Supply and Demand: Threat Actors Specifically Looking for Access to Gaming Companies

For the past two months, we've observed several different actors looking for access to networks of gaming companies.

A perfect example highlighting the demand for initial network access to gaming companies is seen in a listing by a Russian-speaking actor who was looking to purchase multiple types of accesses and databases. This actor specifically stated that he was interested in access to developers' networks of Xbox (Microsoft), Nintendo, Qualcomm, and Apple.

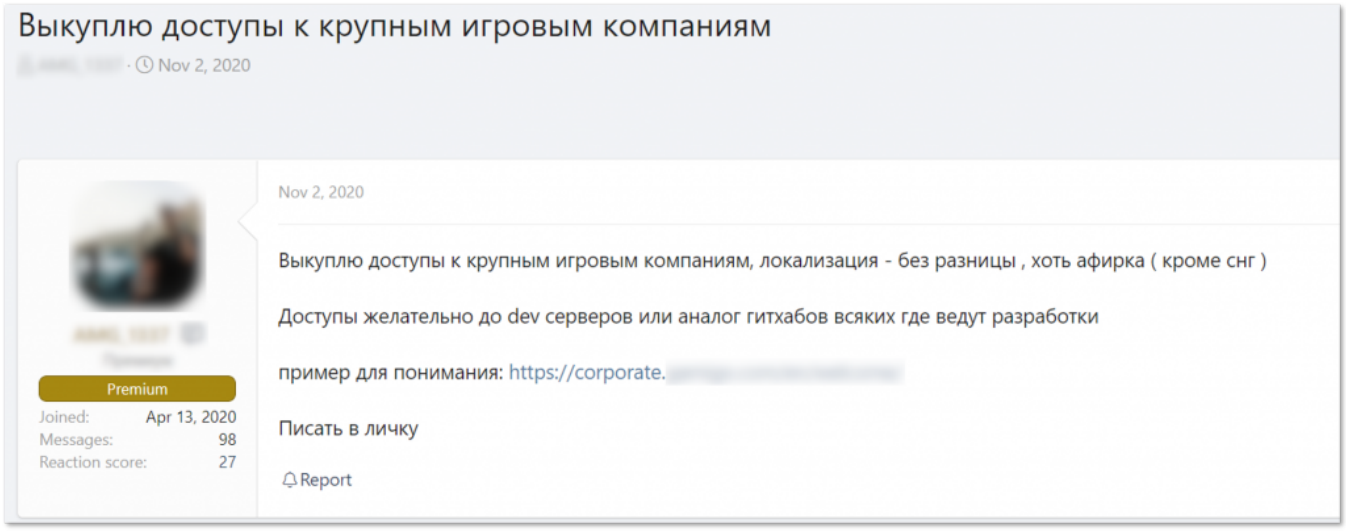


A threat actor stating he is interested in access to developers' resources of gaming companies in a format "developer.COMPANY.com" or similar links

---

Another example, from December 18, shows a threat actor selling data related to a major Japanese video game developer, which has recently been disclosed as Koei Tecmo. The listing included FTP credentials – in this instance it does not necessarily indicate a network access, rather it provides an access point into the company's environment. The sample of data posted by the actor included email addresses, which KELA confirmed were indeed leaked from the company's server in March 2020 and later offered on Cit0day – a service that operated hacked databases and provided access to information for a subscription fee. Just a few days after the original listing, the threat actor decided to release all of Koei Tecmo's data for free on the same forum that he published the original listing on.

Another instance showed a member of a Russian-speaking underground forum stating that he is ready to buy access to big gaming companies anywhere in the world. He claimed he was specifically interested in access to servers or repositories used for development. **Such accesses, as we'll describe later, are frequently offered for sale in different underground markets.**

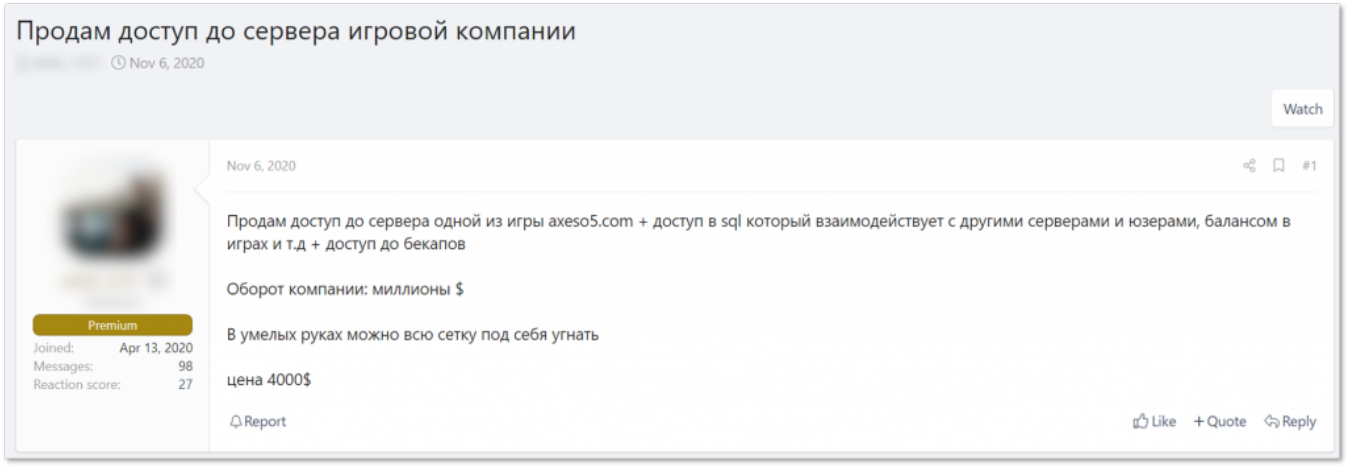


A threat actor seeking for access to "developments servers to GitHub analogues where they keep their code" of gaming companies

---

Interestingly, four days later the same actor offered access to a server of a publisher of online games in Latin America. It's possible that these are two unrelated events: the actor was looking for accesses to developers' resources and separately worked on breaching the Latin American publisher whose access he soon offered for sale. However, it can also be true that he managed to buy some kind of access and

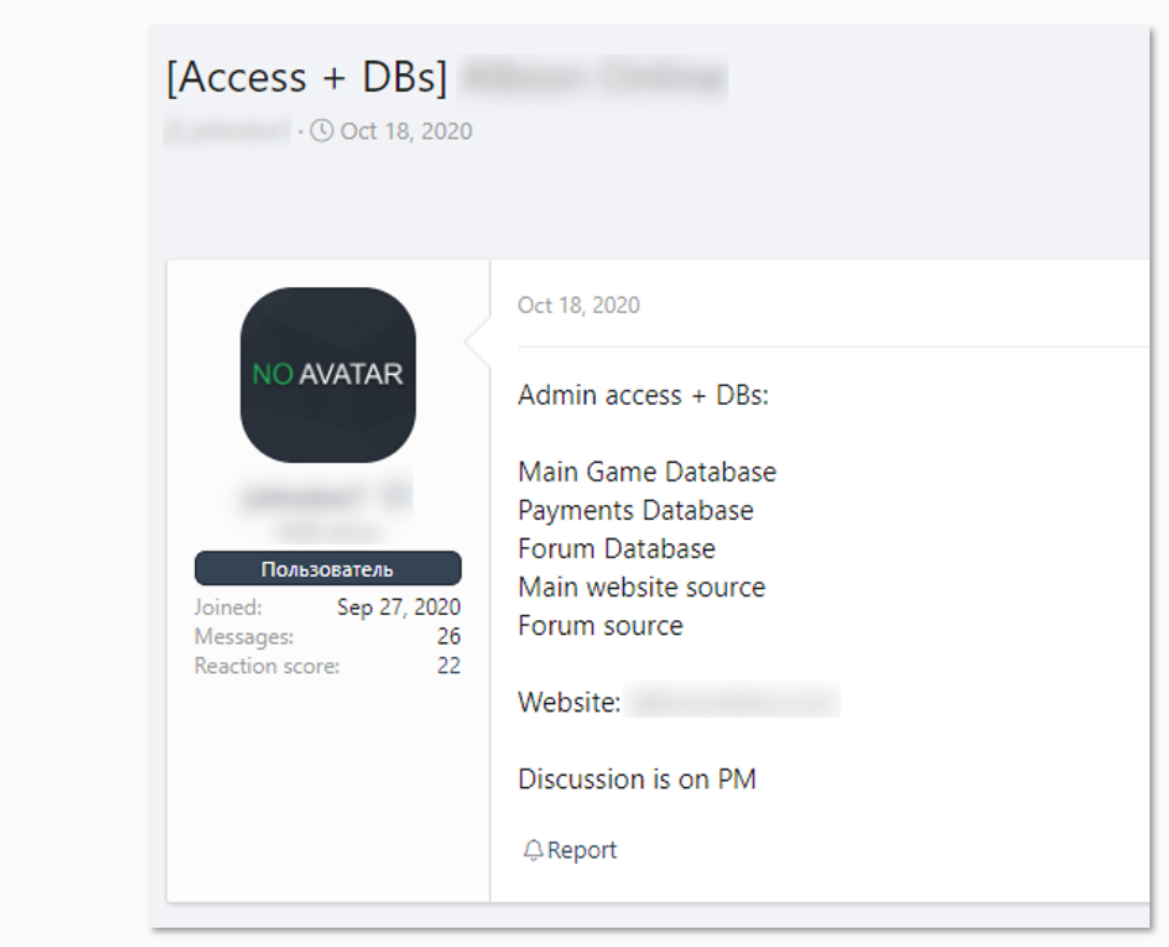
transformed it into the server access offered for sale. Regardless of the connection of events, or the lack thereof, these two instances (as well as the others mentioned above) showcase the fact that threat actors are actively interested in targeting organizations in the gaming sector.



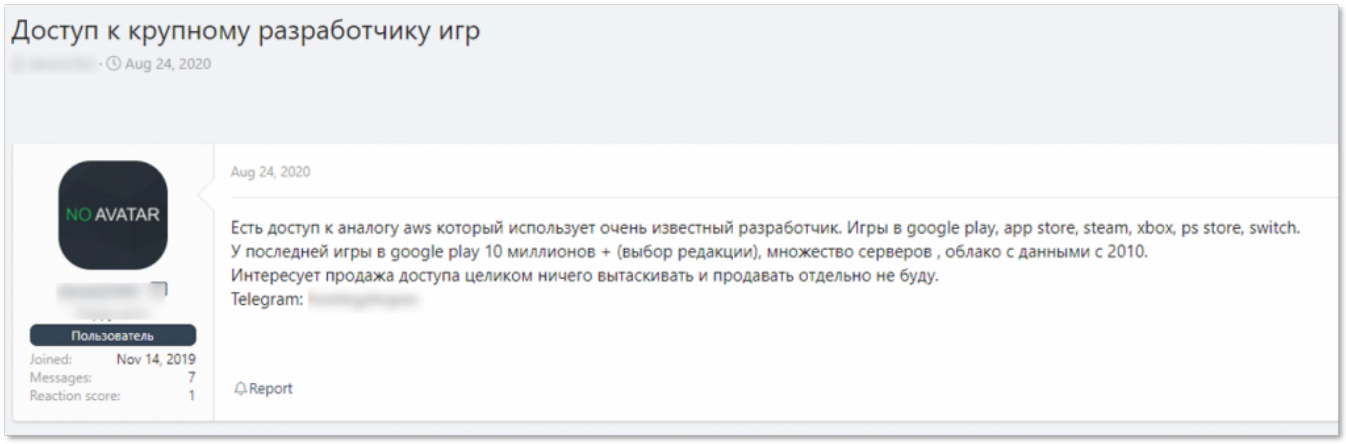
The threat actor, previously looking to buy access to gaming companies, is himself offering access to a gaming company's server

---

Some other offers that we observed by initial access brokers include access of an unknown type to an online game of a German developer and access to a cloud storage solution ("analogue of AWS") used by a major game developer.



Access to an online game of a Germany-based developer



Access to cloud storage solution of a "major game developer"

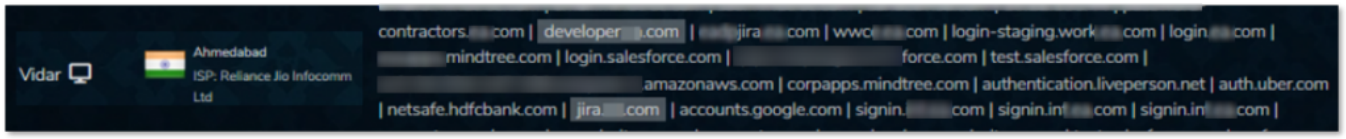
In private communication with the threat actor that offered access to the cloud storage solution, he claimed that the offer is no longer relevant, but alternatively offered something else – access to the network of a major Japanese game developer. Seeing that this was offered only in private conversation with the threat actor, we can assume that the number of threats is greater than actually presented.

Supply: Compromised Accounts

Compromised accounts originate from infected computers (also known as *bots*), usually infected with banking trojans or infostealers. These bots are sold in automated shops, where new listings are added daily, essentially making it very easy for threat actors to attain access to a variety of resources. As one can imagine, a victim's computer might have access to different services such as corporates' portals, employees' internal resources and platforms, social media accounts, kids' school portals, bank accounts, and much more. These markets essentially assist threat actors to attain access to desired services with the click of a button and at a price of a couple of dollars per bot.

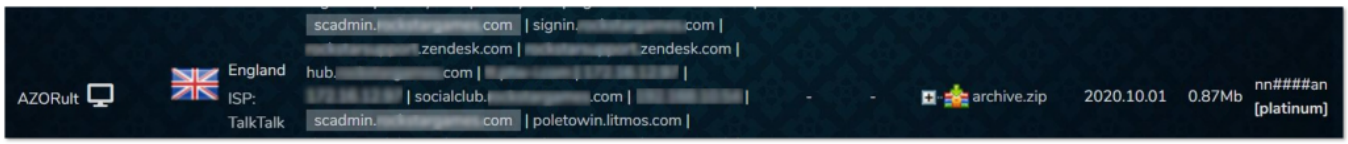
KELA has been monitoring the major underground markets of this type for over 2.5 years and **has tracked nearly 1 million compromised accounts of employee- and client-facing resources of the 25 major gaming companies in question – with half of them being listed for sale in 2020 alone.**

It's important to note that we detected compromised accounts to internal resources of nearly every company in question. These resources are meant to be used by employees, for example – Admin panels, VPNs, Jira instances, FTPs, SSOs, dev-related environments, and the list goes on and on. As seen in the examples below, with a payment of just a couple of dollars a potential attacker can have access to the core areas of a company's network.



Developer-related and Jira credentials collected from the information stealer Vidar, which could indicate some internal resources of a leading gaming company are being compromised

---



Admin-related credentials collected from the information stealer AZORult, which might indicate some internal resources of a leading gaming company are being compromised.

VPN and SSO from Vidar, which might indicate some compromised internal resources of a leading gaming company.

For the past three months, we've observed four ransomware incidents impacting gaming companies – three of which were publicly reported. In addition, it's possible that another major gaming developer was attacked, as Sodinokibi (REvil) stated in their interview.

Credentials to internal resources of recently attacked companies – such as VPN, website management portals, admin, Jira and more – were put up for sale and hence were available for any potential attacker prior to the cyberattacks that occurred. We also detected an infected computer (bot) which had credential logs to plenty of sensitive accounts that could be accessed by attackers upon purchase: SSO, Kibana, Jira, adminconnect, service-now, Slack, VPN, password-manager and poweradmin of the company – all on a single bot – which strongly suggests that it's used by an employee of the company with administrator rights. **This highly valuable bot was available for sale for less than $10**.

Though we cannot directly correlate an attack on one of these victims to a bot that was listed in this market, this incident still highlights the risk that stands when an organization's sensitive resources are available for malicious use with an investment of just a couple of dollars.

Scenario: How Cybercriminals Could Play Around with Compromised Accounts to Execute a Cyber Attack

To understand the risk, let's review a quick scenario of a possible c**yberattack that can lead to ransomware infection once a compromised account is offered on the underground automated shops**:

Going back a few years, a threat actor would have to spend some time in the reconnaissance phase, carefully choosing victims and using multiple tools to get access to a valuable, functioning RDP server belonging to a corporation. Nowadays, an actor needs to only enter underground marketplaces and purchase a bot containing RDP credentials (another possible way – access one of the many remote access markets and acquire multiple RDP corporate servers for a few hundred dollars).

Next, the potential attacker needs to explore them and proceed with ones that look "interesting" – meaning they enable access to a network of a large company with significant revenue (and probably from a sector willing to pay ransom – government organizations, for instance, usually do not negotiate with ransomware operators). Finally, the actor will attempt to escalate privileges or install further tools in order to gain initial access.

From that stage on, once there's initial access to a specific company, the attacker will usually choose one of two directions:

- Using the initial access to deploy ransomware on the company's network on their own.
- Selling it to ransomware affiliates, who will deploy the ransomware themselves as part of a more organized crime.

However, deploying ransomware is only one of the many different cyberattacks that these cybercriminals may attempt. This access could also enable them to initiate other offense such as corporate espionage, fraud, and other methods that could cause victims to incur severe financial losses.

Supply: Leaked Credentials

When looking at an exposure of a company, unfortunately, employees continue to remain as the main entry point, driving us to also analyze the sample companies' leaked credentials stemming from 3rd party breaches. As of December 2020, we've **observed more than 500,000 leaked credentials pertaining to the employees of the 25 major gaming companies in question.** many cases, such credentials are available for free in the underground ecosystem, creating another opportunity for attackers to utilize for further attacks that could lead to profits.

We found that these credentials also include high-profile email addresses such as senior employees and email addresses which are generally a significant channel in the company – invoice, purchasing, admin, HR-related emails, support and marketing are only some of the examples we noticed.

It's worth highlighting that KELA's caching capabilities allows visibility into additional context of leaked credentials, such as associated passwords to a certain email address, previous leaks of a specific email address and more. As part of our regular review, we unfortunately still come across a great deal of re-use of passwords, as can be examined in the example below:

EMAIL	DOMAIN	PASSWORD TYPE	PASSWORD	SOURCE TYPE	SOURCE	POSTED DATE
.com		Plaintext	DRAGAN		teplocat.net database dump	May, 31st 2020
.com		Plaintext	DRAGAN		toanhoc247.edu.vn database dump	May, 31st 2020
.com		Plaintext	DRAGAN		sr-asia.org database dump	May, 24th 2020
.com		Plaintext	DRAGAN		revesdepoupees.com database dump	Sep, 1st 2019
.com		Plaintext	DRAGAN		jwsports.co.kr database dump	Sep, 1st 2019
.com		Plaintext	DRAGAN		tastock.com database dump	Aug, 19th 2019
.com		Plaintext	DRAGAN		Willowsmusic.com database dump	Jul, 14th 2019
.com		Plaintext	DRAGAN		Electricaudios.com database dump	Jun, 30th 2019
.com		Plaintext	DRAGAN		dxmy.4noses.org database dump	Jun, 30th 2019
.com		Plaintext	DRAGAN		Collection #2	Jun, 24th 2019
.com		Plaintext	DRAGAN		network.duranduranmusic.com databa...	Jun, 16th 2019
.com		Plaintext	DRAGAN		oksweetheart.section101.com databa...	Jun, 9th 2019
.com		Plaintext	DRAGAN		wwe.lyndseyjones.com database dump	Apr, 28th 2019
.com		Plaintext	DRAGAN		georgewara.com database dump	Apr, 22nd 2019
.com		Plaintext	DRAGAN		fournoses.net database dump	Apr, 22nd 2019
.com		Plaintext	DRAGAN		creeptones.net database dump	Apr, 22nd 2019
.com		Plaintext	DRAGAN		reecesullivan.com database dump	Apr, 22nd 2019
.com		Plaintext	DRAGAN		Collection of 4725 Database Dumps	Jan, 14th 2019

This single (censored) email address was leaked in numerous unique breaches, as well as some of the Collections dumps (referring here to Collection #1-5), and we can still see that once this user signs up with their corporate email address to a 3rd-party platform or website, they are most likely using an identical password across platforms. This exact behavior, which is unfortunately widely and commonly practiced, is really a “human vulnerability” that is continually being leveraged by threat actors, allowing attackers to gain access to services of interest.

Scenario: Leaked Credentials Are Level 1 in the Attack Process

As one of the main attack vectors still stands as phishing (also the vector possibly used against Ubisoft), there’s room to exemplify how **leaked credentials** can be easily “translated” into a more significant attack. *Combolists* (email address: password lists) as well as databases with credentials originating from previous breaches are no news in the Darknet. Once an adversary is going through their reconnaissance phase of looking for their next potential target and puts their hands on an email address of interest, there are a variety of techniques that they may use. For instance:

- An attacker can be seen using social engineering, or phishing attempts specifically tailored to the victim – either based on the place they work in, or on personal details. The aim is, of course, attaining the relevant credentials in order to gain access to services of interest, find an entry point to a targeted network and then escalate privileges and move laterally.
- A threat actor can attempt to perform brute force and dictionary attacks, for which these databases with plain text passwords are highly useful. Once access was gained to a service of interest – the actor will continue to move laterally to eventually deploy ransomware, as we supposed earlier.

Hence, these databases may be highly useful for a potential attacker to perform a variety of attacks. The examples presented above reflect the types of threats KELA is detecting on a daily basis and can be used as an excellent example of why it’s crucial to educate employees and ensure that they understand the various ways that attackers may use to enter the organization’s network.

Training the Targets: What Organizations in the Gaming Sector Should do to Reduce Cyber Threats

The examples laid out in this blog present the ever-growing threats against the gaming sector that can be leverage by threat actors in a cyberattack. Over the years, new sectors will continue to emerge as the main targets for cyber criminals. These new targets are generally becoming popular among cyber criminals due to the simple fact that they are driving large sums of money. For that particular reason, we’ll likely continue seeing new major targets rise, and organizations will need to prepare in accordance.

Organizations in the gaming sector have to act fast as they are the new target that cybercriminals are interested in. This preparation begins with security training to employees, including:

1. Raising awareness to employees about the risks presented above.
2. Enforcing password changes.
3. Implementing unique password use and MFA policies.

The organizations in this sector will also be required to invest in different measures in order to ensure that they are protecting all of their different assets. Most importantly, these organizations should invest in ongoing monitoring of their assets, to get an external viewpoint of their organization as seen by cybercriminals. By monitoring mentions of their assets across the darknet, they will gain the necessary

intelligence in order to help them better assess their exposure and prioritize security operations.

As we've all been observing – attacks and attackers are becoming more sophisticated and customized to the victim. Some attackers try to search for the specific data and information that is relevant to the scope or industry of the victim and reproduce the successful attacks. As the gaming industry continues to grow in revenue, we will likely continue to detect more threats and attacks targeting the online gaming industry. With constant monitoring of their assets' exposure in the darknet, these organizations can proactively detect threats and map out their risk in order to foresee potential weaknesses in their environment.

---

[1] Excluding Google, Apple and Microsoft. We have checked 53 domains which are related to the companies at issue, meaning not only looked into the companies' main domains, but also some of their most popular games.