BLACKCLOAK™

SPECIAL REPORT

Execs are under siege as hackers target the video game industry

www.blackcloak.io

In February, the Polish video game company CD Projekt revealed that it had become the victim of a ransomware attack in which the cybercriminals claimed to have accessed the source code for the video games Cyberpunk 2077, Witcher 3, Gwent and an unreleased version of Witcher 3.

CD Projekt refused to pay the ransom and within days the hackers auctioned off the source code as well as other sensitive company information stolen during the attack. It was reported (but never confirmed) that the starting price for the auction was $1 million, with a buy-it-now price of $7 million.

The CD Projekt hack was just the latest example of an alarming trend in which attackers are taking aim at the video game industry, which has exploded in popularity during the pandemic as people stuck at home have turned to video games for entertainment.

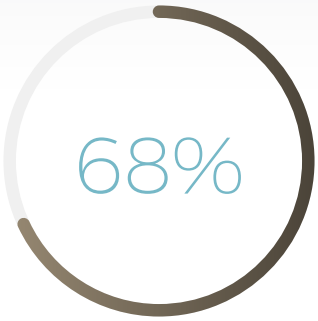
Even more worrisome, the specific target of these attacks appears to be C-Level executives. According to the Verizon Data Breach Investigation Report (DBIR), C-Suite executives were 12 times more likely to be targeted in cyberattacks than other employees in the organization. The report also found that 71% of C-Suite cyber attacks were financially motivated, with attackers looking to make money from company or employee data, intellectual property or ransomware.

A recent report confirmed that the gaming industry is not only one of the fastest growing targets for hackers, but also one of the most profitable. Hackers launched 12 billion credential stuffing attacks on gaming websites during a 17-month period between November 2017 and March 2019, according to Akamai's State of the Internet/Security Web Attacks and Gaming Abuse report. By comparison, there were 55 billion attacks launched against all industries combined. Out of the 10.6 billion web application attacks against Akamai customers between July 2018 and June 2020, more than 152 million were directed toward the gaming industry.

BlackCloak conducted its own independent research and discovered some troubling security-related concerns. By digging into publicly available information, we were able to discern the corporate email addresses of video game company executives and members of the leadership teams. This led to the capture of personal email addresses for these same executives.

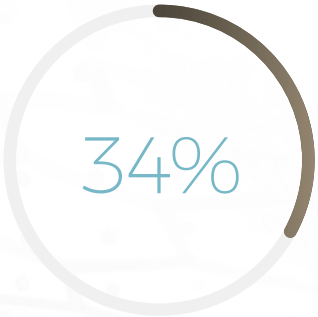
From there, our cybersecurity analysts were able to draw the following conclusions based on a **review of 15 of the Top 20 video game companies in the world**, which are responsible for 90% of the world's most famous games.

OF EXECUTIVES HAD EXPOSED PASSWORDS IN CLEAR TEXT ON THE DARK WEB.



OF THESE PASSWORDS WERE ASSOCIATED WITH THEIR PERSONAL EMAIL ADDRESSES.

WERE ATTRIBUTED TO THEIR WORK EMAIL ADDRESSES.



OF EXECUTIVES REUSED THE SAME PASSWORD OR ROOTS OF THE SAME PASSWORD MULTIPLE TIMES.

The key takeaway from the research is that the leadership teams at video game companies are vulnerable to cyberattacks which could potentially put their entire company at risk. CISOs need to understand that there is no longer a line of demarcation between work and personal lives online. Protecting the company can no longer be limited to the metaphorical four walls of the corporate office.

Enterprise grade security tools such as VPNs, endpoint protection, firewalls, and anti-virus software are fine for company-owned assets, but they fail to protect executives when they are using their personal devices and personal email accounts. Security needs to be extended to home networks, to all devices used by family members on the Wi-Fi network, and to all locations used by the family, including secondary homes.

WHY HACKERS ARE TARGETING VIDEO GAME COMPANIES →

WHY HACKERS ARE TARGETING VIDEO GAME COMPANIES

The vast amounts of intellectual property, mixture of financial transaction information, and reputational risks make video game companies a prime target for hackers.

For example, the number one player in the video game industry is Sony, with **$25 billion in video game revenue** from its PlayStation franchise. Sony is also a major player in the movie, music, and consumer electronics industries.

Probably the most infamous hack of all time occurred in 2014, when North Korean agents attacked Sony, stole and leaked confidential data, and tried to blackmail the company into not releasing a film called The Interview, a comedy about an assassination plot involving North Korean leader Kim Jong-un.

The largest global vendor of video game software is Tencent, the Chinese technology conglomerate. And Microsoft is the fourth largest player in video games; its Xbox business generated **$12 billion in revenue last year**. In other words, these are big targets.

One of the reasons that video game companies are a popular target for cybercriminals is that they don't fall under the same regulatory requirements as, say, financial institutions or healthcare companies, which are mandated to deploy strict security measures to protect customer data. A start-up video game company rushing to develop a game might not make security as high a priority as a bank or hospital.

On the user side, video game players are oftentimes guilty of re-using the same password across multiple sites. Once attackers are able to either buy or hack a user's login credentials, they can launch attacks against video game companies, as well as gain access to the end user's bank accounts and credit card information.

And another wrinkle is that clever video game players often try to 'hack' the game itself in order to give themselves an advantage over the gamers that they're competing against. From there, it's a short hop to actually hacking the network that the device and game are operating on. In fact, the UK's National Crime Agency recently reported that 82% of teens and young adults recruited by online criminals had developed their cybercrime skills through video gaming.

SUCCESSFUL ATTACKS AGAINST VIDEO GAME COMPANIES ARE INCREASINGS →

SUCCESSFUL ATTACKS AGAINST VIDEO GAME COMPANIES ARE INCREASING

When the pandemic hit and everyone was required to stay at home, video games usage spiked, and hackers took notice, launching a barrage of new attacks.

Last April, an **anonymous hacker leaked the usernames and passwords (around 1 GB of data) of close to 23 million players** of Webkinz World, a children's game by the Canadian firm, Ganz. The hacker reportedly gained access using a SQL injection vulnerability.

Nintendo, the third largest video game company, announced last June that **300,000 customer accounts had been broken into**. Hackers gained access to Nintendo Network ID accounts of customers who used the same password on both their Nintendo and Nintendo Network accounts. Hackers could have spent money at the My Nintendo store or the Nintendo eShop using virtual funds or money from a linked PayPal account. Also, personal customer information such as birthdate or email address might also have been exposed.

In September, the U.S. Justice Department charged five Chinese hackers and two Malaysian tech executives with a six-year campaign aimed at hacking multiple video game companies. The hackers gained access to more than 100 entities, including social networks, telecommunications providers, universities and non-profit organizations using **a combination of spear phishing, brute force attacks and supply chain attacks.**

> "We see this as unfortunately a new area which hackers are exploiting."
>
> — *Acting US Attorney Michael Sherwin.*

In December, a 21-year-old California man was sentenced to three years in prison for a 2016 phishing attack on Nintendo. The man broke into Nintendo's internal networks and leaked information on the Nintendo Switch before its launch.

And in January, Capcom, the Japanese video game developer, announced that it was still assessing the extent of the damage from a November ransomware attack. The company initially said **as many as 350,000 accounts may have been compromised, but it increased that estimate to 390,000 people**. Capcom confirmed that sales reports, financial information, game development documents and other information related to business partners was taken during the attack.

> "We are living in the golden age of online gaming. PlayStation5, Xbox X, new powerful GPUs, AX routers and other recent dedicated developments for gamers show us how much the tech-world focuses on providing the best, most flawless gaming experience. Online gaming has seen tremendous growth over the past years, and during the pandemic a record number have turned to it for escapism, entertainment and social interaction. However, it is also in high gear for hackers and cybercriminals who look to wreak havoc."
>
> — *Eden Amitai, Cyber Security Evangelist at Radware*

HOW THE ATTACKS WORK →

HOW THE ATTACKS WORK

To execute attacks against video game companies, cybercriminals first try to obtain access to games and gaming services by using lists and tools with username and password combinations purchased on the Dark Web. Here are some of the other methods used by cybercriminals:

Credential stuffing: In credential stuffing attacks, criminals will often try credentials from old data breaches as a way to compromise new accounts that may reuse existing username and password combinations.

Phishing: Another approach is phishing campaigns in which attackers set up malicious but convincing emails and websites related to a game or gaming platforms. The objective is to trick gamers into signing in with and revealing their login credentials.

SQL Injection: In a SQL Injection attack, hackers use online forms to inject specific code that can then compromise the database behind the form. Another common tactic is Local File Inclusion (LFI), through which attackers use web applications to gain access to files stored on the server. Cybercriminals typically hit mobile and web-based games with SQL and LFI attacks as a way to capture usernames, passwords, and account information.

Distributed Denial of Service (DDoS): Between July 2019 and June 2020, more than 3,000 of the 5,600 DDoS attacks seen by Akamai were aimed at the gaming industry. Such attacks skyrocket at times when users are more likely to be home, such as during holidays or school vacations. Even more concerning, 55% of respondents to the Akamai survey who called themselves "frequent players" said that one of their accounts had been compromised at some point.

"The fine line between virtual fighting and real world attacks is gone," said Steve Ragan, Akamai security researcher and author of the State of the Internet/Security report. "Criminals are launching relentless waves of attacks against games and players alike in order to compromise accounts, steal and profit from personal information and in-game assets, and gain competitive advantages. It's vital that gamers, game publishers, and game services work in concert to combat these malicious activities through a combination of technology, vigilance, and good security hygiene."

A RISK TO THE EXECUTIVE IS A RISK TO THE COMPANY →

A RISK TO THE EXECUTIVE IS A RISK TO THE COMPANY

Why try to attack the fortified security defenses of the corporate enterprise when you can hit the soft target of an executive's personal devices or home office? That's the calculation that hackers are making when they target the senior leadership teams of video game companies.

The blurring of lines between business and personal usage of electronic devices has been going on for a while, but it has been exacerbated by the pandemic and has created elevated security risks when it comes to senior leaders who have access to highly confidential information and to a wide range of IT systems.

They may find themselves sharing an Internet connection or devices with other family members who might be doing homework, using collaboration tools to keep in touch with friends or family members, or engaging in entertainment either via a streaming service or a video game. In this scenario, an attack on any device or application can give the attacker a way into the corporate network or to breach data and intellectual property.

When we audited the home networks of our C-Suite clients, the results were even more frightening:

1 in 5

Home Wi-Fi Networks

was not secure because it still used the default password. These wide-open home networks allow adversaries to see into the cameras, home automation and IoT devices.

3 in 5

Personal Devices

lacked basic anti-virus software

1 in 4

Devices

was actually infected with active malware, including viruses, trojans or worms designed to steal data.

WHAT CISOS SHOULD DO →

WHAT CISOs SHOULD DO

It is always a good idea for CISOs to apply the latest security tools and policies on corporate networks and devices. But as the personal and professional lives of executives merge, it becomes increasingly difficult for CISOs to apply traditional enterprise security best practices without infringing on the executive's need for privacy.

It's a tricky balancing act. CISOs already have enough on their plate without trying to figure out how to protect every smartphone, personal email account, video game player, and other electronic device connected to the home WiFi. It's also mission critical that the CISO protect personal information, passwords and other data that can be sold on the Dark Web and used by criminals to launch attacks against the company.

One way to address this weak spot in enterprise security is to implement a digital executive protection program. CISOs should consider implementing a solution that focuses exclusively on protecting corporate executives in a way that respects their privacy but also applies the latest security techniques in a non-obtrusive but holistic way. A concierge-style security service can conduct penetration testing, regular scans of home networks, and security monitoring of cell phones, tablets and computers to protect against a costly data breach or ransomware attack aimed at the C-suite, senior leadership team, and key personnel with responsibility for intellectual property.

BLACKCLOAK™

Protect Your Company by Protecting Your Executives.™ With BlackCloak's Concierge Cybersecurity & Privacy Platform™, you can mitigate the risks of financial, reputational, and intellectual property loss that may occur through executives targeted on personal devices and home networks and across personal accounts.

Get peace of mind that your company is being secured against threats coming through executives without having to invade their personal lives. Learn more at blackcloak.io

CONTACT US

sales@blackcloak.io

blackcloak.io

company/blackcloak

@BlackCloakCyber