DARKNET DIARIES

EP 45: XBOX UNDERGROUND (PART 1)

Episode Show Notes

[FULL TRANSCRIPT]

JACK: I kind of want to start the show with you just talking about how the original Xbox got hacked.

BUNNIE: Mm-hm. Sure.

JACK: This is bunnie, or at least bunnie is his hacker handle. Back in 2003 he published a book called Hacking the Xbox just after graduating from MIT.

BUNNIE: Yeah, I was in MIT as a grad student at the time.

JACK: Oh, and just as a random fact here, the term ‘hacker’ actually emerged from the MIT Tech Model Railroad Club in the 1960s and that ethos sort of paved the way for the hacker culture today. They were hacking model railroad sets to make them do things they weren’t intended to do, and bunnie fit right in with this hacker culture at MIT.

BUNNIE: Basically, every toy, every game console I had gotten since childhood, I had always taken apart. If I got tired of playing the game, I would just change the resources in the game and get the highest score or whatever it is. It was more fun to sort of hack the games than it was to

play the game itself, is the bottom line.

JACK: Around this time, the original Xbox came out. Bunnie got ahold of one and found it had high-end computing parts in it.

BUNNIE: When I took it apart, it was very clearly a PC to me on the inside. Being able to run my own code on it, put Linux on it, to make the game do what I want to do, right, was just a natural impulse to me. If you paid whatever, $300 it was at the time for this thing, that's not a small amount of money particularly to a student, and then you're told that you can't use it for what you want to use it for. Like, what if I'm done playing games? I need a computer to write my paper. This is ridiculous. That's the feeling that ran through my blood at the time.

JACK: That's the goal. Bunnie owned an Xbox which had all these parts that a computer would have, and he wanted to use it like a PC.

BUNNIE: It was basically a high-end PC. It should be able to run my word processing software, or I should be able to just tell it to boot to a shell or something like that so I can do what I want with it. It seemed like a reasonable prospect to me.

JACK: He tried to put his own software on it but there was a problem. It wouldn't run.

BUNNIE: The firmware image needed to be signed, encrypted to a key, and the key was not known, obviously, to the people who didn't have it. I couldn't put my own code in there unless I had that key.

JACK: Challenge accepted. Forget about playing the games on the Xbox; the game now was to find this key and somehow make it so he can run his own software.

BUNNIE: Right. A bunch of people were searching for it at the time. I figured they would just crack it open

but they all pointed down to this, what was a hidden key that's read from a location inside of memory that would be mapped out after you booted. The processor would wake up in the morning, it would go to a secret location, get its keys, and then it would brick over the door, turn it into a regular wall so you couldn't find it again. Once you're in the outside space, none of the other exploits could figure out what that key was. It was obviously hidden somewhere in the hardware, this extra-architectural feature of the Xbox. Since I was a hardware guy doing research on hardware at the time, this played into my alley so I started poking around.

JACK: [MUSIC] After a lot of research, bunnie had an educated guess that this key probably travels over a specific wire, or bus. He tried to figure out a way to sniff the data that was going over that bus.

BUNNIE: Simply put, I built a little circuit board that could capture the data going across that bus and log it

to another piece of hardware that we could use for later analysis. Then essentially, as we boot the device, we could watch that secret ROM going to the CPU and then observe the key embedded inside that secret ROM.

JACK: This worked. He captured the data which looked kind of like it could be a key. He tried using the key in different ways to test some code, but it wasn't working. But then he used the key with a certain offset and shazam, the whole thing started being decrypted.

BUNNIE: I had to pinch myself. I couldn't believe it. Then I was like, this can't be. This had to be a mistake in the code. It couldn't be right. Then I just double-checked and double-checked. I was like holy cow, this is it. This is the key. I couldn't believe it. I think it was like four a.m. and my girlfriend was asleep already so I wasn't going to bother her, but I was jumping out of my skin. I couldn't scream and shout so I sent a note into the IRC form that was on at the time, and other

people validated it that it was correct. Then the next day, I saw my PHD advisor and told him about it, and that's when he informed me about the DMCA and all the consequences that could have happened as a result of this. I was like oh my God, I didn't even realize this was a thing. How [00:05:00] could this even possibly be illegal for me trying to run my own code on my own box?

JACK: The DMCA, or Digital Millennium Copyright Act, specifically says it's illegal to disseminate technology in order to circumvent copyright protections. But the excitement of cracking a key on the Xbox was thrilling. Bunnie kept tinkering with it and eventually got the Xbox to run Linux, which was a victory in this little game he set out to play. But now there was this looming issue that this whole thing might be illegal. Bunnie, being a good MIT student, wanted to do the right thing.

BUNNIE: We want to do the whole responsible disclosure thing, like

tell Microsoft about the problem, figure out the right way to present the research, that sort of stuff. For several months it went back and forth with lawyers and whatnot to try to figure out what was the right way to disclose the research without doing it irresponsibly.

JACK: Bunnie and Microsoft came to an agreement. Microsoft said you can publish your report, but…

BUNNIE: Basically, just don't share the key. You can tell how you did it and what the research was and all the methods, but just don't print the exact key. That's reasonable, right?

JACK: Bunnie started writing about how to reverse engineer the Xbox but he had to make a choice on where to stop with all this hacking.

BUNNIE: I kind of wanted to avoid anything that could be perceived as unlawful, particularly because I wanted to go public with it and I wanted to share the results of the

work. You can't really play it both ways; either you go white hat or you go black hat, right? I just solidly decided I was going to go white hat on this one.

JACK: One thing led to another and bunnie ended up writing an entire book on how to hack the Xbox and reverse-engineer it. He ended up actually self-publishing the book and sold it through his own website. Guess what? It became fairly popular.

BUNNIE: Drive up to the post office with this – I had this old Maxima sedan filled floor-to-ceiling with books and envelopes. They're like oh, it's that guy again, that weirdo with the car full of books. They'd bring out a big whatever the rolling cartons are, and I would just dump it all in there.

JACK: This book inspired many hackers to learn how to do this and to take this so much further.

BUNNIE: I think the problem that every

technologist faces that every technology is potentially dual-use. This happened with the atomic bomb. Some people thought they could create an energy source for humanity and other people saw a weapon. I think there is a responsibility the technologists to consider potential ethical ramifications of what they do, but it's also not the place of the technologists to deprive all of humanity because they solely judged that the technology may be used one way or the other.

It's just something you have to be aware of in a disclosure and how you educate people how to use it. We then say oh, man, shouldn't touch fire because fire can lead to burns. It also leads to cooking and heating and staying alive. The question does keep me up a lot at night, but at the end of the day, some people are gonna do what they want to do, right? Who am I to say what's right or wrong? Over time, sometimes things will evolve in a direction you can't control, but I think to each their own at that point in time. There's only so much you can

do to control destiny.

JACK (INTRO): [INTRO MUSIC] These are true stories from the dark side of the internet. I'm Jack Rhysider. This is Darknet Diaries.

SKITZO: Okay, I guess the best thing to start is basically from the beginning.

JACK: Wait, wait, wait, before we get started, what should we call you?

SKITZO: [00:10:00] Skitzo's fine.

JACK: Okay. Skitzo it is. [MUSIC] Skitzo was a member of the Xbox hacking crew called Team Avalaunch. It was big in 2009. Oh, and I should give a warning somewhere at the beginning here; this episode and the next episode, they're explicit in nature. There are a lot of cuss words in these two, and the second one gets dark. We're gonna talk about drugs and depression then, but if you can make it through that, holy cow are you in for an amazing story. It's so

amazing, I can hardly believe any of this, except I do believe it because I spent months fact-checking this as much as possible. But it's still unbelievable.

SKITZO: Jeez, Team Avalaunch is a collective group of hackers and hardware enthusiasts, let's put it that way. The main focus there was Xbox. There were some members that ventured into different areas. You had individuals like Lantus that was really, really great with the emulation side of things. People like Redline, who could do wonders with networking, and then you had some greed and you had some people that took up space for God knows what.

JACK: The original Xbox that came out was amazing. The graphics were stunning, the games were great. Halo was my favorite, of course. The AI of the enemies in that game was just unlike anything I've ever seen before. It was amazing. But after the Xbox was out for a while and that initial sheen sort of wore off, some people didn't like the dashboard that came

with it. The Xbox dashboard is the menu within the Xbox and it lets you pick the games you want to play, log into Xbox Live, look at your settings, that kind of stuff. The stock dashboard just wasn't enough for this group of hackers, so they got together to try to make a better dashboard. They wrote the software themselves and then got the Xbox to play it.

This wasn't easy to do, to hack the Xbox into playing your own homemade software, but eventually they got it. The dashboard that Team Avalaunch made was pretty popular among the people who liked modding their Xbox. Another thing this group tried to do is play other games on the Xbox like Nintendo games and PlayStation games. You know what? They were doing it. They were hacking the Xbox to play all kinds of games the Xbox was not supposed to play. But really, if we take out our moral compass here, changing the dashboard and running emulators on your Xbox might be just entering the yellow area of hacking. Yeah, it's against the terms of service and might be illegal, but it's not really that

big of a deal for someone like Microsoft to crack down on, investigate, or hire some lawyers to go after you.

SKITZO: It was, you know, you want to do this with your Xbox, you're gonna do this with your Xbox. But it was never a malicious attack on anything. It was a hobby.

JACK: Team Avalaunch tinkered and toyed with getting the Xbox to do all kinds of things. When the Xbox 360 came out in 2005, they were all over that, too.

SKITZO: That's more or less where I come in. During that time of the OG Xbox scene, I was more into the Sony and Dreamcast scene. It wasn't only until the 360 scene; that's where I came in with Team Avalaunch.

JACK: The Xbox 360 architecture was more secure than the original Xbox. Remember how bunnie was able to sniff that key off of one of the busses on the Xbox? Well, the 360 made it so

the key never left the chip that it was on, making it impossible to do what bunnie did. All new methods for getting custom software to run on the Xbox had to be done. Team Avalaunch figured this out and built a custom dashboard for the 360. A few things were released publically for other people to also do, but a lot of hacking was just kept secret within the group and wasn't publically shared.

SKITZO: I mean, obviously we ruffled feathers but we weren't there to play pirated games. I mean, obviously ultimately when the majority of people that will do this want to do that, I was more than happy playing CPS3 games and Super Nintendo games, and XBMC on my OG Xbox than I was more concerned about playing a pirated game.

JACK: You kinda get the feel of what Team Avalaunch is up to, right? They're figuring out how to mod the Xbox, take it apart, make it do things it's not supposed to do. One of the members of Team Avalaunch was named Rowdy Van Cleave. He was thirty-eight

years old, living in California.

SKITZO: Howdy got…

JACK: Hold on. I call him Rowdy. You call him Howdy.

SKITZO: I call him Howdy.

JACK: Okay, but he goes by both?

SKITZO: He goes by both. Howdy was at the right place at the right time. [MUSIC] Howdy had a friend who had access to a recycling facility.

JACK: This is an electronics recycling facility. Computers often contain a lot of toxic components and need to be disposed of properly. Rowdy heard there were Xbox DVD drives for sale at this facility, cheap. He went down there [00:15:00] to take a look. While he was down there, he found a couple of Xbox 360 motherboards, but these looked different than what Rowdy knew an Xbox 360 motherboard looked like. He took

a few of these motherboards home and popped one into his Xbox 360 and booted it up. The words that Rowdy said next were ‘holy shit, this is a freaking dev motherboard.’ The Xbox 360 dev motherboards were used by programmers themselves to make video games for the Xbox.

You could only get one after Microsoft vigorously screened you to be a legitimate developer. It enabled a lot more features on the Xbox and gave them extra access to do things. Under no circumstance did Microsoft ever want these in the hands of consumers, much less Xbox hackers. They called these ‘dev kits’ and they looked, acted, and worked just like a regular Xbox 360, but with a ton more features. Rowdy knew this and to him, this was a jackpot of a find. He went back to the facility to look for more and couldn’t believe what he saw.

SKITZO: There were thousands and thousands and thousands of kits. Here, I’ll put it to you in this way; I had a kit that was covered in mud. That’s how the kit went to this

facility. It was covered in mud. I called it the Joe Dirt Kit. I never cleaned it ‘cause I found it hilarious. I was like, what the hell did Microsoft do to these kits for it to be covered in mud?

JACK: You can imagine a fairly popular and long-running Xbox hacking group stumbling upon a find like this. It’s like finding actual treasure. Rowdy was finding complete Xboxes there, too.

SKITZO: These are complete kits set to be destroyed.

JACK: Do you have any idea where these were coming from?

SKITZO: Microsoft. I want to say probably 100% of these kits were meant to die.

JACK: When he says ‘meant to die’ he means recycled, destroyed, discontinued, because maybe Microsoft didn’t have a need for these anymore, or these were returned ones, or

defective or something, but Microsoft just didn't need them anymore and wanted them gone. [MUSIC] Rowdy grabbed all that he could and started passing them out to everyone in Team Avalaunch. People didn't take just one; you took one just to take apart, and then you grabbed another to try modding it, and then you grabbed another to see what it was capable of on Xbox Live and stuff. There were so many kits going around that it was so easy to get multiples of them. It sort of became a business for Rowdy. Not that he really wanted to get rich off it, but he wanted to put the kits in the hands of Xbox hackers that he knew and trusted.

SKITZO: During that time, I got introduced into it. Like hey, why don't you have a quick peek at what's going on here?

JACK: Now Skitzo is stoked on getting his hands on one of these. The Xbox 360 dev kit is exactly the same as a regular Xbox, just with all kinds of developer options enabled. One of the most amazing things about

owning a dev kit was the ability to access PartnerNet.

SKITZO: Basically, it’s the developer version of Xbox Live. All kits had a, air quotes, ‘credit card’ so you could make any profile and just jump on PartnerNet and you could, if need be, purchase Xbox Live points at that time. But 90% of the time, developers who put their games up for testers to get ahold of it, or to demo, and you download it. It acted exactly as retail Xbox Live did at that time.

JACK: Through PartnerNet, you could potentially see and play unreleased games or unreleased patches, or unreleased add-ons for games, or unreleased maps. It was amazing for this hacker crew to all have the first peek at all this stuff. It was like the wild west for them. While playing games on it was fun and lasted a while, the hot new game was now to hack the dev kits and to see what you could get them to do.

SKITZO: The goal was basically hey,

how can we run code on this and what can we do to it? That was the ultimate goal; can we get an emulator running on it? Can we get MAME on this thing? Can we get anything to XBMC, things of that nature? What's the architect behind it? What are the limits? The network presence that Microsoft took at this time was far more advanced than what the original Xbox had, with respect to connecting on Xbox Live and things like that. How was hard drive structure and the encryption? How did Hyper-V work? It was that Pandora's box of like – to your point, how excited were you, it wasn't necessarily exciting getting the system but getting under the hood that made it fun.

JACK: This was very exciting times for Skitzo, Rowdy, and everyone on Team Avalaunch. They knew that this was something the public was never [00:20:00] meant to see and here they were, a whole team of people, hacking away at it.

SKITZO: The public should never have this. It's the gateway into all the

millions of millions of dollars and manpower that you spent on securing your system. Why don't you tape your house key to your front door when you get home? You're pulling the curtain behind the console, right? With the right tools you can get into the console. You can see how things load. You can do timed attacks on it. You can do a number of different things to the console, have an easier time doing it than retail that's locked up.

JACK: Around this time, Halo 3 was about to be released and those who pre-ordered it got access to the beta version a few months before the release. With these DEV kits, Skitzo and the team could play the public beta version of Halo 3. Nothing really special here, but the beta only lasted a short while, just to test it, and then the game was not playable for a few months until the official release. But Team Avalaunch, using their dev kits, figured out a way to keep playing Halo 3 long after the public beta was closed.

SKITZO: [MUSIC] We were able to run

that on PartnerNet and we were on the server that Bungee had set up and we would play. Bungee was trying to take the server down, and Bungee had a custom welcome screen for us because we kept a dev kit running called Halo 3 Dummy. Halo 3 Dummy kept that server alive so we could get in and play while after the air quotes, ‘beta time’ expired on Partners.

JACK: They did so much more with these dev kits, grabbing stuff from Xbox Live and moving it to dev so that they could play it as developers. Like, you could enable things like double experience points or load up special loot. It’s like you could be a GM in many games, and they played a lot of beta games and unreleased stuff. It was great times.

SKITZO: [XBOX SOUNDS] It was amazing, astonishing, to look back at all this stuff.

JACK: [HALO MUSIC] Rowdy kept getting more kits to send to people, and mostly these kits would only be

put in the hands of people in Team Avalaunch. He wanted to keep this secret and underground.

SKITZO: But for a while it was very close-knit. It was a family. We were a family and I know that term is used a lot but all good things must come to an end. We had greed that started happening with the one guy who kept getting the kits and was always just for us, just for us, and next thing you know, shit's starting to flood the market and every jackass out there with five hundred bucks is getting a fucked-up kit. The kits are getting into the hands of people that shouldn't have had it, and you had garbage cans of human beings getting closer to the scene. Then you had the new bloods that came in and it was just, fuck it. Just go.

JACK: Let's talk about these new bloods. First, let's meet Dylan. Hello, can you hear me?

DYLAN: Yeah, can you hear me?

JACK: Yeah, I hear you.

DYLAN: Perfect.

JACK: This is Dylan, right?

DYLAN: Yeah, Dylan.

JACK: Dylan was young. In 2010, Dylan was only 14 years old. This is kind of what he meant by new bloods, right? These are young kids just getting in the Xbox hacker scene. Because Skitzo and Rowdy were much older and had been in the scene for many years at this point, they were like veterans. But now young kids like Dylan are showing up, and back then, Dylan's hacker name was Dae, D-A-E.

SKITZO: Dae came around and he really didn't give a fuck. He truly did not care.

JACK: Okay, Dylan, what is one of your first hacks?

DYLAN: I got suspended twice during high school for actually getting into computer networks I probably shouldn't have gotten into.

JACK: Whoa.

DYLAN: I think it was the thrill of knowing what's behind doors that kind of got me into it.

JACK: Look at this recipe; a young kid, doesn't care much about the rules, loves video games and the Xbox, loves hacking, and is hungry to learn more and do something crazy. Combine that with a high level of curiosity, and someone who has always 'on' energy, you get Dylan.

DYLAN: I think back then it was just not knowing what you can and can't do. Just not being told this is wrong doesn't necessarily go past a teenager's mind, [00:25:00] so I think I just liked the thrill of it. It was kind of like a rush, it was like an adrenaline rush every time I got into something, and seeing things that I

shouldn’t have seen. That’s kind of what makes you want to do it even more.

JACK: Dylan was so fascinated with Xboxes, he wanted to learn how to hack it. Yeah, he starts joining Xbox hacker forums and hanging out in the chat rooms, and getting to know who’s who in the scene. There’s another person who showed up in the Xbox hacking scene around this time, too. Is Diane all set up? We ready to go?

DIANE: I just hit record.

SANAD: Yeah, she just hit record so we’re good to go.

JACK: Let’s start out with you telling us your name. What is your name?

SANAD: My name is Sanad Nesheiwat. For some reason on my birth certificate, the doctor’s messed up and put my middle name and first name together. That’s why it says Sanadodeh Nesheiwat. But it’s just

Sanad.

JACK: Sanad grew up playing console games, and loving them.

SANAD: Yeah, I was definitely a hardcore gamer. I had Dreamcast, PlayStations. I've been gaming since I was about eight years old. I didn't really get into that whole hacking thing up until the Dreamcast came out. That's when I really started getting into things.

JACK: Sanad is a hardware guy.

SANAD: Well, I mean, I like taking things apart, figuring out what they do, and trying to modify them in ways that will benefit me.

JACK: When he was younger, he had a soldering iron, oscilloscope, lots of chips, electronic parts everywhere. At one point, I asked him a question about electronics and jeez, he just went off the rail, crazy deep on me. Listen to this.

SANAD: What a BGA station does, is it has heat plates and it shoots up hot air from the bottom and hot air from the top. It allows you to take the chip off and clean out the solder and put brand-new solder balls on it.

JACK: Okay, okay. You get it, right? Sanad is passionate about electronics. He's a hardcore gamer and he loves breaking things just to open them up and see what's inside, and how they work. He loves Dreamcast and Xboxes, and these kind of things. Sanad was deep in the console hacking scene. At one point, he and a friend created a launcher that would run pirated software on the Xbox. But his friends started telling him about the Xbox dev kits that were going around in the scene at the time. His friends said…

SANAD: Hey, you guys can totally use dev kits to make your launcher a lot smoother, and you can debug it in real-time, and so on and so forth. I was like alright, so we put together a PayPal donation account and a bunch of people donated so I was actually able

to get everybody on the team a dev kit through Rowdy. That's when I first got one.

JACK: There was something absolutely magical about being a console hacker in 2010 and getting an Xbox dev kit in the mail. This was something you weren't supposed to have; this was forbidden. Here Sanad is, opening it up, eager to plug it in and play it, like it's a doorway to a magic kingdom. Oh, what fun he could potentially have with this.

SANAD: My first dev kit, I actually bricked within two hours. But luckily, I had made a flash dump of it before even messing with it and I was actually able to revive it.

JACK: Once he got it up and working again, it was amazing.

SANAD: Going on PartnerNet was phenomenal. Imagine going on Xbox Live but everything that you download is betas and it's all free.

JACK: [MUSIC] So many unreleased games were available to play.

SANAD: Correct. For example, when Sonic 4, Episode 1 was going to be released, they had it on PartnerNet almost a year before it came out.

JACK: This was a magical time in Xbox history.

SANAD: Oh, it was great, being able to play stuff before everyone else, that's a rush. It was really, really, really cool at the time. After knowing Rowdy for, I want to say almost a month, he started telling me about this program that Dave had.

JACK: Ah, yes, Dave. He's one of our main characters in this story, so let's talk about him now. He lived in Toronto, in Canada, and was only around sixteen years old at the time. He was finishing up high school and was planning on going to University of Toronto after that. Even though he was young and a new blood to the scene, he was fascinated with video

games ever since he was three years old. He taught himself how to program along the way, and make web pages. Dave was an Xbox hacker and he had been buying dev kits from Rowdy, and doing all sorts of cool stuff with them.

SANAD: What it would do was, it would actually parse the XML file for PartnerNet and allow us to download files that were hidden on PartnerNet.

JACK: It was a little bit more complicated than just parsing an XML file, but what happened was that this allowed this small, tight-knit crew to carve even more content out of PartnerNet, [00:30:00] allowing them to see unreleased maps or extra features not even devs wanted other devs to see. It wasn't enough to just have access to beta content, but now they were starting to get access to pre-beta content. Dave had a way of attracting people to him. He was good at socializing with other hackers and making friends online. Once people started finding out that he had Xbox dev kits, they liked him even more.

David was finding a way to mod Halo 3 and post some of his findings on halomods.com. A guy named Anthony was fascinated with David's post and started chatting him up online.

David started trusting Anthony so he sent him an Xbox dev kit and together they figured out how to do more Halo 3 mods. Like, they would be able to jump higher and alter the way the bullets looked. Anthony was good at reverse-engineering things and he was able to look at machine language and convert it to readable code. Together they made mods that were hilarious and awesome to play. Anthony also helped David download unreleased Halo maps from PartnerNet. They could then screenshot those and pass them around to their friends, showing what new content was coming out soon. Anthony and David grew close and would often chat long into the night, talking about video games and hacking Xboxes. They were finding some really impressive hacks. Then David would post some of these mods online and this would help him rise in popularity and make even more friends.

DYLAN: Okay, so the Xbox scene was pretty big, but the people who actually programmed, for example, or released any programs or did anything, they were quite small and David made a name for himself where he was known for this guy who did the Halo mods. You could change the variables of the game and I think that's what drove me to oh, he's a very good name there. He's got a very good background with programming, he's talented. I guess that's where I had some sort of level of trust, as to say for him.

JACK: Dylan, being young and impressionable, looked up to Dave as some cool hacker guy in the scene. Dylan wanted to be part of the scene. At some point, David found a weird way to make some money off these hacks. Someone found a vulnerability on the Xbox 360s. On the bottom of the Xbox were a strange set of pins known as JTAG. These JTAG pins would allow devs to debug the Xbox to fix problems with it. Well, someone figured out that if you put a mod chip on these JTAG pins, it would enable you to do

various cheats in the game. [MUSIC] Kids all over were getting their Xboxes modded with these JTAG hacks which would allow them to cheat in their Xboxes. This was all fun, but the cheats really didn't work that well on Xbox Live. But David figured out a way.

By using his dev kit to start a game lobby on Xbox Live, people could then use their systems to join and use the cheats. For instance, Dave would start up a Call of Duty online game with his dev kit. This is where people from anywhere in the world could then join together and play the game. But Dave's lobby was set up so people would be able to join it and cheat. Like, walking through walls, jumping higher, or having 100% accuracy. While this was fun to play, Dave was seeing how kids were going crazy over these hacked lobbies that he set up. They loved playing them because if you were the only hacker in the lobby, you had an unfair advantage over everyone else in the game. Dave realized the only way you could do this is through his dev kits making

those hacked lobbies. He decided to start charging people to join these hacked lobbies.

SANAD: It started off on websites like Se7enSins and a whole bunch of sites where a bunch of Call of Duty gamers would hang out and stuff that wanted to actually cheat. They just started advertising on there and they would invite people into infected lobbies and they would charge them a fee for it.

JACK: [MUSIC] We're talking like, $100 for thirty minutes of playing as a hacker. This was working; Dave was pulling in sick cash with this. He thought that it was probably a lot of kids taking their parent's credit cards and using that to play in these games. It was crazy. He was making so much money, it allowed Dave to take his girlfriend out to upscale restaurants and stay at $400 a night hotel rooms. Okay, you saw that your online friends were doing this. Did you ever try making money off of one of these paid lobbies?

SANAD: I did lobbies for one night. I made $1,000 off it and then I was like, I'm not doing this anymore.

JACK: Why would you stop? I mean, that's a pretty nice $1,000 in one night.

SANAD: I mean, the whole thing behind it, it's kids using their parent's credit cards and stuff like that. Kids would literally steal their parent's credit cards just to get their lobbies, just to basically get all their stats up and everything.

JACK: Eventually Microsoft figured out that people were using the [00:35:00] JTAG pins to hack like this and they issued a fix, making the JTAG hack completely unusable. This put an end to Dave's little money-making scheme. Following that, Activision, the makers of Call of Duty, sent a cease and desist letter telling him they're not happy with these little hacks. But Dave just shrugged this off and said, quote, "I mean, it's just video games. It's not like we're

hacking into servers and stealing any information." End quote. But that soon changes. [MUSIC] You know what? Everything that's happened so far is small potatoes compared to what happens next, so stick around 'cause it's gonna get so much better. Things are about to kick into high gear with this team and it all starts with Dylan.

DYLAN: Okay, yeah. I was quite good friends with someone in the scene. He went by the name Gamerfreak1727.

JACK: Dylan was still only like fifteen years old at the time and was online friends with someone named Gamerfreak. Somehow his friend got ahold of a database dump for an online forum to a website that discusses video games. My guess is that his friend or someone else found the vulnerability in that bulletin board and exploited it, and stole the user database but didn't really know what to do with it after that.

DYLAN: One day he gave me this list

and went oh, I don't know if it has any use but maybe you can come up with something out of it.

JACK: This was a list of gamers; their usernames, e-mails, and plain text passwords. This was very fun for Dylan. If he wanted, he could at least log into the forum as anyone on the list. That's cool, but maybe there's something more he can do with this.

DYLAN: I went okay, so who is important on this list?

JACK: He looked down the list of e-mail addresses and saw some of the users had e-mail addresses from Epic Games. Now, Epic was the creator of the hit games Unreal and Gears of War. They're a massive video game company. This caught Dylan's eye.

DYLAN: Let's see if they reuse passwords.

JACK: He found another gaming Wiki and tried to log into the Wiki using

one of the logins from the list he got.

DYLAN: I was able to log into that. That kind of narrowed my list down to how many of these accounts that were employees actually did use these passwords for something else. There I kind of pivoted to okay, let's see if they have a personal account linked to these. I actually stumbled across one IT employee there who actually, I kind of found his Gmail account.

JACK: At this point, Dylan has logged into the Gmail account of one of the IT employees of Epic Games. While in this inbox, he'd look through different e-mails to see if he could find passwords or logins to anything else.

DYLAN: Which actually gave me, I guess, the keys to the castle because that password was what he used for his work e-mail. Admin060606. Being a young teenager, I think it was probably late at night, possibly early morning, 'cause I believe I logged

into his e-mail directly after, his work e-mail, and I went oh my God, this worked. I can't believe I got something out of this. I guess yeah, it was an adrenaline rush.

JACK: Now Dylan has a valid login to someone in the IT department who works at Epic Games and can log into Epic's network with this login.

DYLAN: I go back to Gamerfreak1727 and I say okay, we've got something. [00:40:00] I managed to actually find some passwords that were of use.

JACK: Now him and Gamerfreak do a little mapping to try to figure out what exactly they have access to. They discover this person is actually an IT admin for Epic Games. They found the server to let them VPN into Epic's network. Whoa, this is some big-time access into one of the hottest game-makers out there. Dylan thought this kind of access would earn him a lot of street cred with these Xbox hackers and he wanted to be a part of the scene.

DYLAN: I basically approached David and I said to him, I might have something of value. Would you be willing to team up? To David's surprise, I guess, I don't think he would have normally been approached that way. I don't think someone's just gonna go hey, I've got the keys to this; would you like to take a test drive?

JACK: Dave is curious with what Dylan has to show them. They do a Skype session and Dylan shows David the access he has to Epic's network. Together, they poke around in it.

DYLAN: During a Skype session, we were searching for their things and we found oh, there's all this source code. For him as well, I believe, it was very thrilling to be able to then do it himself and go wow, there's so much we can do here.

JACK: Digging into these directories, they found the source code to Gears of War 3. Whoa, this is

getting serious now.

DYLAN: When we found Gears of War 3, I think that was a really big thrill for us all. It was like, wow.

JACK: The Gears of War 3 was over a year away from being released and here was the source code to it. Dave wanted this but wanted to be safe on taking it from that network. There were big folders and this was gonna take a long time to download. He needed someone who could do it safely and quickly.

SANAD: Dave didn't want to log in because he was scared that his IP would get registered so that's when Dave reached out to me.

JACK: Dave knew Sanad had the perfect way of connecting into Epic's network without getting caught.

SANAD: Okay, so I had a hacked cable modem on Comcast.

JACK: This hacked cable modem gave Sanad 100% free internet, and on top of that, the way it was hacked made it show to Comcast this was an unknown customer so Sanad had full confidence that whatever he did with this modem would not be tracked back to him. Oh, and it was super-fast too, so he was able to download illegal stuff quickly and without any fear.

SANAD: Dave messaged me and he's like hey, this is the deal. Gears of War 3 is definitely on there. This was a year before Gears of War 3 was even due to come out. I was like okay, cool, so I'll just grab Gears of War 3. Then he started telling me about source code and everything being on there. I'm like okay, well, I'll just grab all that, too.

JACK: [MUSIC] Dave gives Sanad the username, password, and IP address to log into. This was a Cisco web VPN portal; basically, it was only for IT staff at Epic to log into through a normal web browser. As soon as you do, you are greeted with a list of folders and computers you can connect

to. It was really quite simple for Sanad to figure out where to go and then to find the folders and source code.

SANAD: There was a lot more than just Gears of War stuff on there. There was Gears of War 1, 2, and 3 stuff. Then they had some unreleased games and unannounced games on there.

JACK: Sanad started downloading the source code for these games. It was late at night but damn, this was way too exciting. There would be no sleeping tonight.

SANAD: Oh no, no, no. I stayed awake. I was watching literally everything download, and the progress on them. The second that Gears of War 3 finished, I put it on my dev kit just to run it for a little bit just to see what it was like. The game was nowhere near fully completed at the time. There was a lot of placeholders and whatnot. There was one part where Marcus was supposed to be looking at a screen with his dad talking and

there’s just a grey box with an X on it. At that point I realized; I’m like, this isn’t gonna be fully playable, but nonetheless, it was still cool.

JACK: This was amazing. This was crazy. Now they’re getting deep. This wasn’t just acting like developers and grabbing developer stuff on Xbox PartnerNet. Now, this group is actively hacking into Epic’s network and stealing source code for pre-released games. Unbelievable.

SANAD: Once I get all that stuff, I had a Blu-Ray burner ‘cause I had a PS3 dev kit. I was like hey, I’ll just burn them all to a Blu-Ray for you and I’ll encrypt them, and I’ll just ship them to you. So that’s what I did. I ended up going to the post office. On the customs form I put down ‘wedding videos.’ In case anybody tries to open it, it’s just some disks that could possibly be [00:45:00] wedding videos, you know what I mean?

JACK: Dave gets his package in the mail. It's marked 'Wedding Videos' and he has a little trouble getting the data off the Blu-Ray disk, but eventually got it. Now he was playing Gears of War 3. So cool. This rough-formed hacker crew was starting to take shape now. David was doing some reverse-engineering himself and organizing people, and bringing them together. Anthony was finding ways to hack Halo 3. Dylan kept getting into Epic's network and finding more stuff, and Sanad was downloading it all and distributing it. David was helping all these people get dev kits and access to unreleased games and content. Playing games a year before its launch date might sound amazing but it's actually a terrible experience.

DYLAN: There was no textures on like, half the things.

JACK: Instead of seeing an enemy you would just see a grey box, or instead of seeing a house you'd see a weird green wall, like it was a green screen or something. But it was still

exciting to have early access to the game like this and see where the developers are at.

DYLAN: I think it was the thrill of it, right? It was hey, this isn't even out. Nobody has this. I think that was the fun in it.

JACK: Of course, some people in this hacking crew would invite their friends over sometimes to play these unreleased games, but they were quiet as to how they got these games. Another new blood showed up on the scene, a twenty-year-old name Justin May. [MUSIC] He wanted to buy an Xbox dev kit from Dave and Dave sold it to him.

SANAD: Justin went by the moniker MTW.

SKITZO: MTW is a scud. He is absolute garbage. He is the guy that wanted to be famous and this is a guy that went to fucking PAX and got arrested.

JACK: Okay, okay, okay, let's back

up here for a second. Justin was living in Wilmington, Delaware at the time and was there in the Xbox hacking scene trying to help out wherever he could. For instance, Rowdy had an obsession with grabbing as much stuff as he could from PartnerNet.

SKITZO: They changed the game's fucking font, for example, title screen font or some shit like that. He would spend all day fucking refreshing Partners, looking for something new.

JACK: Justin was helping Rowdy download this stuff which got him into this circle. Dave was able to get a dev kit to Justin and Justin was becoming part of the scene.

DYLAN: He was majorly involved in a lot of this. A lot of the times, he was actually the one doing things alongside – I was probably using my computer, screen-sharing TeamViewer, whatever we wanted to use at the time. I think I had Team Viewed a lot and I just gave him access and went go for

it.

JACK: But the crew noticed a strange coincidence with Justin. They'd all been playing Gears of War 3, the game they stole from Epic, and they were keeping it very tight-lipped amongst themselves. But when Justin got access to the game, just a few days after that it showed up on The Pirate Bay for anyone in the world to download. Nobody knows for sure who leaked the game, but this wasn't good. It suggested Justin might have leaked it. Epic saw their unreleased game was out there in the wild and freaked out. Epic called the FBI to open an investigation to try to figure out how this happened. During that time, Dylan and Sanad were in Epic's network, downloading the latest builds of Gears of War 3, and still poking around. Dylan was still in the inbox of that IT employee that he hacked, looking at e-mails, reading them, and one day he came across a chilling one.

DYLAN: Yeah, we saw oh, shit, they've got the FBI involved.

JACK: [MUSIC] Epic was working with the FBI to see how Gears of War 3 got leaked. E-mails were going back and forth between the IT admins and the FBI, and Dylan and Sanad were reading those e-mails because they were in the IT admin's inbox.

SANAD: They were talking to each other and the FBI agent was like oh, I don't see any intrusions. I just see some malware from South Africa or something like that. I'm like okay, so they're not onto us so let's stop while we're ahead. I mean, I was definitely a little freaked out. I told Dylan, once we saw that, I was like look, they don't know that we're in there. Let's just kind of stop logging in and let's let things die down.

SKITZO: It was an unspoken rule with all of us which was don't poke the bear because you don't want to draw any unnecessary attention.

JACK: Around this time, the Penny Arcade Expo, or PAX, took place in

Boston. At this video game conference, you could play new games, have huge LAN parties, and see the latest stuff from game makers, and hear talks from industry leaders. Of course, members from the Xbox hacking scene were curious to know what was there. Since Justin lived in Delaware, he headed over to PAX and told the gang he'll be there.

SANAD: When that happened [00:50:00] Howdy was at my place. Howdy was staying over at my place.

JACK: Skitzo and Rowdy were on the West Coast so they couldn't see what was going on at PAX, but they knew Justin was there. Rowdy knew Sanad had Justin's phone number.

SANAD: Rowdy was like hey, can you call Justin and I'll talk to him? I was just like, why? He's like I don't want him to know my number. I'm like alright, whatever. I three-way Justin in. Justin doesn't even know I'm on the phone at this point. He just thought it was Rowdy calling him.

Rowdy tells him, he's like look, try to connect to the network wirelessly. If you can't, just don't worry about it. He was like oh, okay, okay, just kind of giving him the BS, like okay, whatever, type of thing.

JACK: Because maybe if you're on the same wireless network as some of these big game-makers, you could get access to something cool, but Justin couldn't really get on that secured wireless. But just imagine Justin there, an Xbox hacker, walking the expo floor, full of video game companies all sharing their latest demos and giving everyone sneak peeks at upcoming releases. He's got to be looking for an opportunity for something to steal or grab to bring back to the boys. Day One goes by and nothing happens. On Day Two of PAX, Justin goes back and he finds a booth of a video game maker demoing a game that isn't out yet. The game was called Breach and they were demoing it on a couple of Xbox dev kits that the game company had. Justin waited around the booth for an opportunity. When one of the employees went to the bathroom, this

left the booth shorthanded which gave Justin a window. He quickly jumped behind the booth and pulled out his laptop.

SANAD: He decided to try to plug a hard-wired Ethernet cable into his laptop and tried to steal a game off of one of the dev kits.

JACK: It was working. The download started and he was pulling the game off the dev kit, right there in front of tons of people at PAX.

SANAD: He got like, fourteen megabytes in and the other employee saw him and started chasing after him.

JACK: [MUSIC] The expo's security quickly saw what was going on and they started chasing him through the expo. The police were then radioed to help too, and together they caught Justin and threw handcuffs on him, and started questioning him.

SANAD: There was a few people there that we knew that said – they were

like, he was saying ‘I know people, I know people. They’re doing bigger things. I know people.’

SKITZO: He gets arrested and I informed Rowdy and I said look, he’s dead. We sever all ties with him. No one talks to him. If you talk to him, very brief. Anything going on? No idea, man. Yeah, oh no, once you got picked up – and I said this to everybody, let’s be smart about this. He got arrested. You know he’s gonna say some shit. Just don’t, don’t risk it.

JACK: This rattled the group of Xbox hackers. Justin knew a lot and potentially was sitting in police or FBI custody. That’s a scary thing to be facing for a twenty-one-year-old hacker. What secrets might he be giving up? How scary were the police to him? In the kind of hacking world these guys were in, trust is all you have with one another. You’re a band of brothers because if one person talks, it could bring down the entire crew. Everyone was wondering if Justin was gonna talk. Would he tell

the FBI or police anything? Was he given any kind of option to give up information to keep him from going to jail? Did the cops try to threaten him with long-term prison times? We don't know. Nobody knows.

SKITZO: Don't get it twisted; I said the motherfucker was a snitch from the start. I told Howdy that, I told shitbag Speedy, that. I told Red that, Lantus. Anyone with ears in the fucking scene, I said do not trust this fuck. You are talking to the Alphabet Boys; you are dead. It's that simple. You know they're gonna say some shit. You know they're gonna scare you with shit. It's their fucking job to do so. You, in turn, are going to be like well, hm, is fucking video games worth this?

JACK: [MUSIC] But I don't think Dylan cared about any of this.

DYLAN: We were teenagers. I don't think we had too much of a sense of risk. Like oh, if we got caught it would be a slap on the wrist, right?

JACK: Skitzo and Sanad weren't teenagers, and they knew the dangers of all this and laid low. But Dylan seemingly took no warning here and just kept poking around in Epic's network. He was still only fifteen now, living in Australia. Maybe that's what made him think that nothing will happen to him. He was totally uncaring that Epic was talking to the FBI and he was uncaring that Justin just got arrested. Dylan went right back into hacking into Epic's network.

DYLAN: Yeah, just stumbling across machines, [00:55:00] I just was pivoting to different servers, all the different servers 'cause they had a ESX kind of host, so they were VMware for everything. So, everything was virtualized. It was easy to know which IPs were servers, which IPs were – it was very [inaudible] work. It made it easier for an attacker as well to kind of go okay, well let's just scan all the servers. Let's see what their host names are. Let's see what's in them. I guess I was just

doing that. It was kind of like a Shodan Safari inside a network. Yeah, I guess what happened was I stumbled across one machine which had an SMB open.

JACK: In this instance, SMB is the remote file-sharing protocol. Basically, Dylan was able to see the files on this computer using a remote shared drive.

DYLAN: Yeah, I was like okay, this is interesting. I kind of went into that machine that was hosting the SMB and I went okay; this machine also has a thumb drive connected to it. That's not normal. Yeah, just lo and behold, was this password list which, you know, Exhibit B. The keys to everything, you name it, was on that list. Everything from the IP, what the server did, what the server name was, the root password, everything.

JACK: Whoa, this is the master password list that the IT department used to access everything. Administrator accounts, root accounts,

the IP addresses, the host names, the passwords. It was all neatly presented on this list. This is like a golden map to everything. This gave him a lot more access into Epic's network. This gave Dylan a huge adrenaline rush to see all this which now gave him new energy to explore more of the network.

DYLAN: Yeah, you're not backing down from that. You can only go further, right?

JACK: It was now a daily ritual for Dylan to log into Epic's network and look around, totally fascinated and curious with what they were doing in there. In fact, at one point, he even got to physically watch what was going on in the office.

DYLAN: As I said, I was doing a lot of ID scans. I went and jumped onto their employee PCs, their conference room PCs. One day it was like okay, I'm gonna jump in a conference room PC and I was like oh, there's a webcam. [MUSIC] I actually watched the sun

come up, and people walking. The door was open and I just watched people walking around. I was like oh, okay. Yeah, it's the thrill, right, it's the thrill that you can see beyond just the internet level of things. You can see the real-life perception of what's going on in that company.

JACK: For the most part, Dylan stayed away from looking into any personal information on anyone's computers, but there was one person that he did take a peek; Cliffy B.

DYLAN: Yeah, the face of Epic at the time. I think that's where it was a bit different, the poster child for hacking. He drove their Lamborghini; he had the Epic Games Lamborghini number plate.

JACK: Cliffy B was the lead designer for some of Epic's most popular games like Unreal and Gears of War. His creative insights were crucial to the success of Epic and he was a bit of a mini-celebrity because of that.

DYLAN: Yeah, we just stumbled across his computer, looked at folders and all of this, and we're like, okay, well, there's pictures. We're not too interested in that. But there was some really odd-naming things like, he had Beach Pics which were very bizarre photos, which I won't go into detail there. Why it's on a work computer, never questioned. But then he had what he called The Lambo Tunes. [MUSIC] These were just his mix tapes, I guess, for his Lambo. There was a lot of K-Pop on there. There was some Mariah Carey even, but you know.

JACK: Dylan continued to log into computer after computer, server after server, to see what each of them did and what they stored. But then something occurred to him; Epic is the creator of Unreal Engine, and if you are a video game creator, chances are you're not going to create a video game from scratch. You're gonna bring in libraries and building blocks that someone else made and the Unreal Engine is a building block for building a 3D, first-person shooter-type game. It handles all the

collisions, movements, health, and objects for you. You just need to program it to make it look however you want.

The Unreal Engine is a massively successful game engine and is used by many huge game companies. Now, to use the Unreal Engine, you had to pay a licensing fee to Epic. It wasn't free. Somewhere in the [01:00:00] Epic Game network would have to be a list of all the game companies that have licensed the Unreal Engine. Probably along with that, are gonna be usernames and passwords to manage their license and account.

DYLAN: I was like, well, where do they store that database? The first thing I thought was okay, it's their Unreal Development Network which was kind of their Wikipedia.

JACK: Remember, Dylan got into Epic's network because an IT admin reused a password from another forum. His theory is that if he could find the username and password list for

these people licensing Unreal Engine, maybe they reuse passwords, too.

DYLAN: All the companies that licensed Unreal Engine, they were using what they called the UDN, which is their Unreal Development Network which I guess was where their support questions came in, where they had Wikipedia on what to do, how to fix things, what's in the latest patches. All different kind of useful information from developers, but obviously they had their e-mails attached to it, they had their passwords attached to it.

JACK: Dylan's theory was that if all these game companies are licensing the Unreal Engine, where's that username and password stored to license it? Somewhere in this Unreal developer network? Maybe. Dylan starts looking all over for the database that would store that username and password. After the break, we'll hear what he found. Stay with us. [MUSIC] Dylan kept poking around the Unreal developer network looking for the database of people who licensed the

Unreal Engine. Sure enough, he found it. He had every e-mail address that licensed it and every hashed password to go with it. Time to crack some passwords.

SANAD: Dave had the best video card out of everybody and him and Dylan realized that it was just the MD5 and salt for the log list for their passwords and usernames. They were able to use Passwords Pro to just de-hash everything.

JACK: They weren't able to crack all the passwords, but some are better than none. They now had a couple of usernames and passwords for other developers from other game studios, not just Epic anymore. People who got cold feet because Justin got arrested are now coming back into the scene because this kind of breathed in new life to it. Dave, Sanad, and a few others, and of course Dylan wanted to see what they could access with these new passwords. Maybe the developers re-used their passwords somewhere else.

DYLAN: If you're a developer for a game company, you're more likely to have access to the Xbox developer network as well, which that was David's field where he was interested in Microsoft itself.

JACK: With this list of licensed Unreal Engine usernames and passwords, they wanted to see if any of them could log into GDNP which is the Xbox Game Developer Network Portal. Basically, if you're going to publish a game to Xbox, you're going to need an account at the GDNP.

SANAD: It uses the same login system as Hotmail. What I found out was for that, if you put in a invalid username, it gave one error but if you put in a username that was existing with the wrong password, it gave a different error. We were able to decipher which GDNP accounts worked from that.

JACK: [MUSIC] Whoa. Now they have a few valid logins to the Xbox game developer network? Obviously, these

developers were not practicing good security and reusing passwords.

SANAD: All of them used their company domain name, so they all used their company e-mails. Then of course, human error, some people like to reuse their password to make life easier for themselves.

DYLAN: Yeah, so we went from there. We were like okay, these usernames and passwords, these all work. Let's reference them. Let's see if [01:05:00] we can get into their other networks.

JACK: Dylan noticed that Xbox developers often used a middleware called Scaleform. This is software that helps game developers create user interfaces and menu systems within video games. He went to Scaleform's website.

DYLAN: They also had a forum itself inside there. That forum I believe was running either – I believe it was PHVBP, just another open-source

bulletin board.

JACK: Dylan started plugging in usernames and passwords, trying to log into Scaleform using the logins from the GDNP he found earlier. Sure enough, he got into Scaleform's forum. Not only did he get in, but when he checked his permissions, he was logged in as an admin to the site.

DYLAN: We had kind of like this admin access and sadly they didn't have permissions set where admins can't dump the user database. We just did backups of the database every day.

JACK: Once they dumped the database, again they ran it through Dave's password cracking computer and were starting to get usernames and passwords for Scaleform users. From there, they got a lot more usernames and passwords. These were connected to e-mail addresses to big gaming studios like Microsoft, bungee, Activision, EA, and Blizzard. What this crew now potentially has is valid logins for developers on these

networks. Scaleform's database was a potential goldmine to this hacking crew. They've already scraped everything out of Epic. They had access to GDNP and Scaleform, but now they're looking at a big list of usernames and passwords for many more companies.

SKITZO: Yeah, that's when I started to really not want to know.

JACK: This is Skitzo again.

SKITZO: At the time I was kind of over it and I saw what was coming. I come from the era when there were some raids taking place in '99 and dodging that fucking bullet, and I didn't want that. It had all the shit of this is not gonna end well for anybody.

JACK: But all these logins not only got Dylan more excited to go deeper, but it brought Sanad back, and David and Anthony were interested, too. Things got crazy after this. They find one of the logins had an e-mail ending in activision.com so they went

to Activision's website and they found a VPN or admin portal or something, and boom, they'd get right in. They're now in Activision's network. [MUSIC] Then they'd find someone who worked at EA on their list of credentials and boom, they'd be able to log into EA's network. Within a very short time they had access to a ton of game developer networks. They were now in the networks for Microsoft, Bungee, Blizzard, EA, Activision, Epic, Zombie Studios.

DYLAN: What about Valve Studios? Steam? We had Steam, even.

SANAD: Me personally, I only messed with Microsoft stuff, Epic stuff, Activision stuff, and Valve stuff, but Dave had access and Dylan had access to way more. They started going to Zombie Studios, Disney, Intel. I kid you not, there was probably a good twenty, maybe twenty-five companies that they had access to.

JACK: Of course, each company that they would gain access to would be a

huge adrenaline rush. They were on fire, getting into one network after another. When they'd get into the video game company's network, all they were looking for were unreleased games that weren't out yet, and what they could download and play before anyone else.

SANAD: My whole thing was no taking money, no selling stuff.

JACK: But see, this is the problem; the more companies they hacked into, the more games they got, and the more amazing it felt. But they were only able to share how amazing this was with their four or five people in this small circle of trusted hacker friends. But this excitement was so hard to contain, that every now and then someone did leak something. When that would happen, this little hacker group started rising in popularity. More and more people wanted to join up. Suddenly, there were two new members of the group.

DYLAN: Austin Alcala, Nathan Leroux.

JACK: Austin was a high school kid from Indiana and Nathan was homeschooled, living in Maryland. Nathan had already done some successful hacks and had a knack for creating in-game gold out of thin air. Austin and Nathan worked together to connect into Zombie Studio's network. It's a game company and they just wanted to look for anything good. They ended up stealing stuff from the US military.

SANAD: Okay, so how they got into that was – it wasn't exactly hacking into the US military; they went into [01:10:00] Zombie Studios, which was contracted to make the Apache Helicopter Flight Simulator for the US military. They had a tunnel between the US military and Zombie Studios, so that's how they were able to get that Apache Helicopter Flight Simulator.

JACK: Austin and Nathan had stolen the source code to the flight simulator for the Apache Helicopters. Unbelievable. Apparently, Zombie Studios had a contract with the

military to create parts for this software. This is a hacking rampage unlike anything I've ever seen. Again, the only reason they're doing it is just for the thrill of it and to play games that just weren't out yet. What a massive hack for such a small motive.

DYLAN: There was nothing we didn't have, or we couldn't pivot to, and I guess that's where it became this big issue. Our team became from maybe four or five people, it became almost a dozen of us.

JACK: Yeah, and picture this; at this time, Dylan is still going to high school.

DYLAN: Yeah, I mean, I was in high school. Pretty low grades, pretty lackluster. I was probably a straight D student, if anything.

JACK: Can you imagine that feeling of excitement when school's out for Dylan? I mean, he's been thinking about what to hack all day and then as

soon as it’s over, boom, he runs home to conduct a massive amount of hacking all night long. Dylan was barely able to pay attention in class at all because it just seemed so boring compared to what he was doing online. He was even failing his computer class.

DYLAN: Okay, so back then, computing classes weren’t what you get now. They weren’t as involved. You didn’t get your certifications; you didn’t get any of that. All you got was hey, let’s go on up here, let’s do this. Open this, let’s make that. I never really came across a guy who really gave two shits about that kind of stuff. I was in a class full of people who had no prior interest in IT and I would say I was smarter than even the IT teachers themselves.

JACK: Yeah, that’s a good point. Imagine being an expert dancer and taking a beginner dance class with a bunch of people who don’t want to learn how to dance. You’d be bored out of your mind. These hacks went on and on for months and months. David

started getting a little worried. There had been too many digital tracks left all over. He told the group, quote, “If they notice any of this, they’re going to come looking for me.” Unquote. But he was too enthralled with his access into all these networks and just couldn’t stop at this point. David accessed Activision’s network and poked around, looking for games to play. He found a pre-released version of Modern Warfare Call of Duty 3 and grabbed it and shared it with the group so they could play. These hackers would sometimes let their friends come over and play some of these games.

SANAD: No, totally, all the people I knew in the real world, they would come over and hang out with me and we would play pre-released games all the time. But I would never give anybody anything ‘cause I – who’s to say if somebody didn’t want to sell their dev kit or something that they acquired from me, and next thing I know, there’s more stuff leaked online.

JACK: Was this blowing your friends’

minds that you had this?

SANAD: Oh, yeah. No, it totally did, especially when I got Modern Warfare a little early. They were like, going ballistics over it ‘cause most of my friends are huge Call of Duty fans.

JACK: [MUSIC] Dylan was also having his friends come over and play, but he wasn’t telling them any of the secrets, either. Yeah, it was weird that he had this game, but his friends really didn’t care. They just wanted to play.

DYLAN: I’m trying to think back to that, but I don’t really think there was much to explain more than oh yeah, I just kind of got this. No questions asked. It was really just oh yeah, you’ve got this. Cool, let’s play.

JACK: It’s now been a year since their initial hack into Epic’s network where they stole Gears of War 3. Now the game is being released to the public. Here’s something that shocks me about these guys stealing these

games.

SANAD: I didn't play the game all the way through 'til it launched in stores, and I bought the Special Edition Gears of War 3 Xbox Slim that came with the game.

JACK: While Sanad had the ability to play this game a year before it was released, and all the way up until it was released, he only played it a little so it wouldn't ruin his experience when it officially came out. Not only did he buy it, but he bought the Special Edition version of it and a Special Edition Xbox to go with it.

SANAD: Well, Epic is a great company. I want to support them. I know what I did was wrong, but I still wanted to support them.

JACK: It's just so weird to me. It's weird because of how much he risked to get this early access, but then still buy it anyway. But most of these Xbox hackers were really big

into gaming. They didn't have just one Xbox; they had many, actually. They had Special Edition ones, and some to tinker with, and some to take apart, and not to mention the Xbox dev kits that were going around still. Rowdy was continuing to grab them from the recycling center and sell them [01:15:00] to Dave who he'd then sell to people he trusted. By this time, people were practically hoarding the dev kits. It wasn't uncommon for some of these people to have like, ten dev kits each. Remember, the dev kits were fully playable Xboxes themselves and during all this hacking, every now and then there'd be a hint that the game companies were onto them.

SKITZO: I remember I was on Partners playing some shit, and my console got bricked. [MUSIC] I told Howdy, I'm like Howdy, I think they're doing something. He goes no, no, no, it's probably an old kit, yadda, yadda, yadda. I plugged in another kit. Bricked. Within seconds, bricked. Plugged in another kit; bricked. We had their attention or they had their attention. Something had to have been

done, and it was out of control.

JACK: By the way, Skitzo had so many Xbox dev kits that breaking three of them was not even close to a big deal. He had so many more that this was not even a worry for him. But none of this would slow the group down. They continued to infiltrate, exfiltrate, compile, and play stolen games from video game companies.

DYLAN: This was already two years into it, and I guess what happened was, well, it got so big. It just blew up so fast. Within two or three years we had everyone. When I said everyone, we literally had everyone in the gaming industry.

SKITZO: I would hear all this shit, and I was like guys, I don't want to know. I don't. I don't need to know any of this shit. For a while, I removed myself from everything. Don't get me wrong, dude, it's a thrill. You getting shit, it's a thrill. You breaking into something, absolute thrill. But at what cost? I had

talks with certain people; get out, focus on school. I'm gonna sound like that PSA ad, but focus on school, focus on making money legit and worry about something stupid like where am I gonna go on vacation. That should be your worry. You've been there, you've done that. You got to say that you did it. You got to say that you were ahead of the Alphabet Boys. Cool the jets. It's over.

JACK: By this point, they were gaining access to places beyond just gaming studios. They had access to Disney's network, AMD, Intel, Google, and even Warner Brothers. It was absolutely insane how much access they had. More people started joining this group too, people I can't name here, but they were there. Some were skids, barely knowing what they were doing, and some were pretty good at reverse-engineering, hacking Xboxes, or hacking networks. Oh, and their old friend Justin started hanging out again. Remember him, MTW? The guy who got arrested at PAX? He was slowly coming back into the scene. People were talking about whether he

could be trusted or not. People weren't sure but Justin was doing stuff to try to earn his trust back. People would see him do illegal things and he was getting away with it, which got them talking. Some people believed he was okay.

SANAD: He's doing these Amazon scams and stuff. If he was a snitch or whatever he wouldn't be doing that stuff.

JACK: Justin was cooking up all kinds of scams at this time. He was learning how to exploit returned merchandise that he didn't have. Basically, he'd call a company and say an item is defective, and lie to them, and get them to send him a new one. He was teaching others how to do this in the group, and it was sort of a way to prove that he was willing to do illegal stuff.

SKITZO: He was like yeah, all that you need to do is have a prepaid MasterCard with a dollar on it, and do an RMA, and they only put a dollar on

the card just to make sure that the card is valid. He would have RMA scams from Amazon, God knows where else, to an abandoned house out in Delaware that he would sit ‘cause he knew the post people’s time. He would sit there, pick up the shit, and go. This guy ran scams for years. He was also scamming the shit out of Apple, on Craigslist. On eBay he’d get people to give him the serial number and run that scam as well. He’s a scam king. Fuck him, he should get hit by a car.

JACK: Just to go over some of the members of this group again, we have Rowdy who’s selling Xbox dev kits like crazy now; Skitzo who’s just trying to stay low and out of the scene altogether; Dave who’s organizing a lot of this and modding, and hacking, and cracking passwords. Anthony is also participating in a lot of this and doing some reverse-engineering; Sanad who’s trying to reverse-engineer the Xbox and downloading a ton of stolen data on his hacked cable modem; Dylan, the teenager in Australia who’s just wreaking havoc on everything, and

Justin, [01:20:00] who may be a little hard to trust, he's teaching people how to scam, and Austin and Nathan are fiddling around with the Apache Helicopter software. That's just like, nine people alone. There were many more than this, too, and this group didn't really have a name that they called themselves, but the media would later refer to this group as the Xbox Underground.

DYLAN: Xbox Underground comes from, okay, so there was a forum that was once existing called the Xbox Underground. I'm not sure how they came across it but we were like oh yeah, in prison we'll all be together like the Xbox Underground gang, as a joke. These guys, they already had this gang-presence in prison so we were like yo, fuck it, that's what we're gonna call us.

JACK: Things were getting bigger and crazier with this group. They had hacked into practically the entire Xbox gaming industry and they had access like nobody else had. By this point, it's grown so out of control

and there are now dozens of people with all serious levels of access into networks, and each day they're digging further into it, showing each other what they found. There's no safe way to come back down from this. Everyone is too high from the adrenaline of stealing these things and trying to one-up each other. Being online, hanging out with this group, was so different than whatever real life world experiences people were going through.

It was like when they sat at the computer late at night, they were wearing a mask and they take it off to go out, but if you wear that mask more than not, it's really hard to start taking it off. It becomes more a part of you than you. This can't end well for anyone, and it doesn't. The story isn't even close to being over yet. Everyone knows there's going to be a crash, but every developer will tell you it's not about avoiding the crash; it's about being able to safely recover from one. Are you ready for their crash? If so, join me in the next episode to hear how this

operation gets terminated unexpectedly.

[OUTRO MUSIC ENDS]
[END OF RECORDING]

Transcription performed by Leah Hervoly
www.leahtranscribes.com