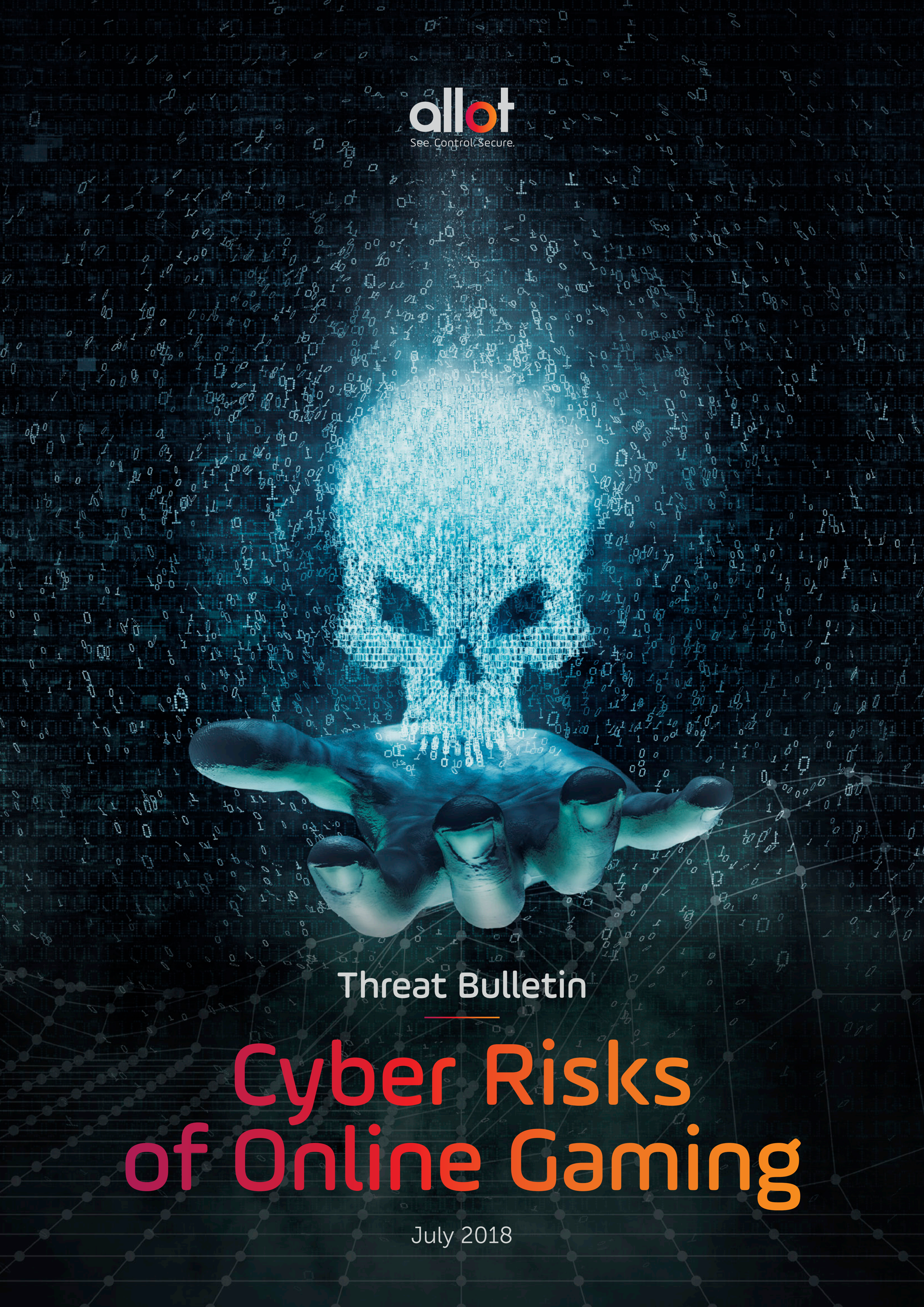
allot
See. Control. Secure.



Threat Bulletin

Cyber Risks of Online Gaming

July 2018

The Cyber Risks of Online Gaming: Real-time Report

In the rush to get new games to market, developers typically release them on the first platform that is ready—usually on IOS. This can have the unintended effect of driving up anticipation for the game release on other platforms in the rest of the marketplace. While this may be great for market hype, it's not so good for cybersecurity.

Overeager gamers, often young and naïve, give in to temptation and download so-called pre-release hacked versions, thinking they will be first to try out something new. In fact, they are walking right into a well-planned trap...

Game Release Frenzy

What is clear is that games released on one mobile platform before being released on another creates a feeding frenzy for those who may have to wait months to get their hands on the latest hit. One example of this was the enormous frustration generated following the release of Epicgames' **Fortnite Battle Royale**, which now has over 125 million registered players. The hunger for this game looks set to eclipse that of the earlier hit, **Pokemon Go**, with 650 million downloads to date, which is still played by aficionados around the world. Released on the Xbox One, PC, PS4, and IOS, **Fortnite** rocketed to the top of the online game popularity charts. However, if you were an Android owner, you were left sitting on your hands. While Epicgames promised the Android release by the summer of 2018, as of July, 2018, it is still not available, causing widespread annoyance among Android users.

Mobile Gaming Attack Vectors

Many Android gamers impatient for the release of **Fortnite** on the Android Package Kit (APK) took to the Internet in a desperate search for an early, cracked release of the game. And they weren't disappointed. Myriad opportunities to download the Android version have been offered across the Web. This download desperation is the *first attack vector* used by hackers to target mobile game players. Multiple weblinks were presented online along with previews of the game (from those platforms on which the game had indeed been released). There was just one small problem—the proffered links were traps that led to the installation of nasty malware onto the devices of unsuspecting gamers. While most of the viruses did little damage to the downloader, the malware that they installed onto their mobiles or tablets did start to generate income for the virus creators.

To understand how gamers are infected by game-related malware, it is useful to understand the life cycle of the games themselves. While the games may be quite different in style and content, there are several features they have in common.

As with most online games for the mobile sector, online games are generally offered as "free to play". To try a game out, a player must simply install the app on their phone or tablet and start tapping. In addition, most of the games are competitive, although Pokemon Go is the exception to the rule. The element of competing online with other players around the world certainly adds to the addictive nature of the gameplay.

So, how do the game manufacturers make money? One way is through an intricate process of micro-transactions inside the game that supply gamers with weapons, game boosters, or enhanced game play. This is the *second attack vector* used by mobile game hackers. These extra features are not necessary for playing the game, but it is more difficult to compete at the higher game levels without them. For example, with **Pokemon Go**, the free game only offered a limited number of actions to keep you playing. However, enter the online store and there's a whole world of goodies available to help you "move to the next level", which is what these games are all about. Non-game players would probably be unable to understand how players could spend real money buying imaginary items to play in an online game, but players do so, in the millions.

Malware Infiltration

Once they had identified the two attack vectors specified above, cybercriminals were then able to target the emotional drives of young, and sometimes uninformed mobile game players. The first vector targeted was the gamer's desire to play the game as soon as possible. They leveraged this motivation by planting malware bombs on specific website links to which gamers were directed. YouTube invitations to play a game that was not yet released proved irresistible to many game enthusiasts who were prepared to take a chance and load potentially damaging software onto their devices. **Fortnite** was a case in point where, even though it was widely publicized that the APK had not been released, Android users would attempt to download a free version and start playing.

The average user who falls for this trick is normally a young person without too much experience in the world of cybersecurity. Users must beware of malware attackers who try to exploit the desires of young, impressionable mobile game players. Players must heed the message that downloading online games from any location other than official sites like Google Play or the Apple Store could result in significant damage to their devices and security. Aside from the damage that this malware can inflict on mobile devices, the financial gain accrued by many malware programmers may not be something to which gamers would necessarily wish to contribute.

Some of the Android spyware presents a **Fortnite** icon on the user's mobile device, which, when tapped, installs its malware payload. Other infiltrations have resulted in the harvesting of call logs and phone contacts. The malware was also found to enable the malware creator to make free calls from the target's mobile phone.

In the above case, ThreatLabZ researchers said they observed Android spyware and cryptomining malware posing as the official **Fortnite** game app, ultimately tricking users. Mobile hacks have also been able to access phone cameras, read keystrokes, and make audio recordings through the user's microphone. Other malware variations have turned a target's mobile device into a coin-mining app that mines cryptocurrency for the malware infiltrator. The most popular technique uses the JavaScript created by CoinHive. While such infiltration does not result in direct financial loss to the target, the mobile device's CPU is overclocked producing excessive heat and potential damage to the user's phone, in addition to rapid battery drain and lower performance.

One further attack vehicle used by cybercriminals involves the offer of fake **Fortnite** "V-Bucks". This currency would enable players to purchase in-game bonuses to use while playing the game.

Prior to receiving these free tokens, players are requested to complete a brief, online survey. Of course, even if players do complete this survey, there is no pot of gold waiting for them at the other end. Instead, links in the survey implant viruses on the user's phone, which hackers can exploit. In-game money is used to buy cosmetic items and gestures (it only has aesthetic benefits for players). One fake app was downloaded 5,000 times, and boasted five-star rating over 4,000 times before it was summarily removed by Google Security.

To succeed at **Fortnite**, players must eliminate all their opponents, and become the last man/woman standing. There are some malware websites offering gamers the opportunity of purchasing invincibility modes, enabling them to slaughter their opponents mercilessly and then climb up to higher game levels. Again, unsuspecting gamers will click on links that install malware on their cellular devices, which can lead to hackers accessing data on their phones, or abusing their devices in one way or another, such as remote cryptomining.

Conclusion

Even though the focus of this bulletin has been on the game **Fortnite**, the concerns and cautions raised are applicable to all mobile online games. No enthusiastic gamer wants to wait to play the latest hit game, or wishes to watch others playing on one platform while another platform version is not yet available. Cybercriminals manipulate this frustration against the users and take advantage, especially of impatient and uninformed individuals.

Our recommendation is only to download apps from the official app store (Google Play Store, or the Apple Store), and wait until a game is formally launched before downloading it. Any "similar" or "leaked" game that claims to be the original one will most likely turn out to be malware that wants to infect your device.

CSPs are advised to deploy Allot's NetworkSecure, which provides full protection against malware attacks on mobile devices attached to the network.

Concerned about the cyber risks of online gaming?
Are you seeking to boost your security offering for gamers?

We can help.

Contact Allot »