Ασφάλεια στο χώρο του Gaming

Λεοπάρντι Μάρκος Αντώνιος

ΔΙ.ΠΑ.Ε

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Θεσσαλονίκη, Ελλάδα

*Περίληψη* – Οι μηχανές ανάπτυξης βιντεοπαιχνιδιών χρησιμοποιούν άδειες που επιτρέπουν στις εφαρμογές πρόσβαση σε προσωπικά δεδομένα του χρήστη, στις πληροφορίες συστήματος, στις πληροφορίες της συσκευής όπου χρησιμοποιούνται. Πέρα από τις άδειες, χρησιμοποιούνται και διάφορα αρχεία (Assets) τα οποία μπορεί να είναι επικίνδυνα. Τόσο ο προγραμματιστής των ίδιων των μηχανών, όσο και αυτός αργότερα του βιντεοπαιχνιδιού μέσω της συγκεκριμένης μηχανής, πρέπει να ελέγχει τα assets που θα χρησιμοποιήσει αλλά και να δηλώσει τα δικαιώματα για την εκάστοτέ εφαρμογή. Ο χρήστης χρειάζεται να αποδεχτεί αυτά τα δικαιώματα για την χρήση αυτών των εφαρμογών. Το ίδιο ισχύει και για τα ολοκληρωμένο βιντεοπαιχνίδια που έχουν βγει στην αγορά είναι online και χρησιμοποιούν με κάποιο τρόπο δεδομένα από λογαριασμούς που έχει δημιουργήσει ο χρήστης. Κάποιο αρχείο του παιχνιδιού μπορεί να γίνει corrupt το οποίο θα καταστήσει ολόκληρη την συσκευή ευπαθή σε επιθέσεις. Αυτό το άρθρο αναφέρεται στους κινδύνους που υπάρχουν στις μηχανές ανάπτυξης και ύστερα στους κινδύνους που υπάρχουν στο τελικό παιχνίδι που θα δοθεί στον χρήστη, καθώς και κάποια παραδείγματα «λαθών» αλλά και επιθέσεων που υπήρχαν στον χώρο

# ΕΙΣΑΓΩΓΗ

 Η μηχανές ανάπτυξης παιχνιδιών (GDE=Game Development Engines) είναι ένα πλαίσιο λογισμικού που επιτρέπει την ανάπτυξη βιντεοπαιχνιδιών με την χρήση βασικών λειτουργιών, όπως 2D ή 3D renderers, physics ή collision engines, υποστηρίζοντας επιπλέον και ήχο για την δημιουργία βίντεο, όπως κινηματογραφικά σενάρια και κινούμενα σχέδια [1]. Οι πιο δημοφιλείς στην αγορά είναι η Unreal Engine και η Unity,αλλά υπάρχουν και άλλες, σαν την CryΕngine, Frostbite, Game Maker. Με το πέρασμα των χρόνων, η βιομηχανία των παιχνιδιών (Gaming Industry) έχει αναπτυχθεί σε μια βιομηχανία δισεκατομμυρίων. Συγκεκριμένα, εκτιμάται ότι το 2023, η βιομηχανία θα φτάσει να κοστίζει τα $221,4 Δισεκατομμύρια , ενώ ότι μέχρι το 2030 θα φτάσει τα $583,69 Δισεκατομμύρια, με την κατηγορία του Mobile Gaming να έχει την πρωτιά στα παγκόσμια έσοδα για την βιομηχανία. Επιπλέον, το 2017 υπήρχαν παγκόσμιος 2,39 Δισεκατομμύρια παίκτες, και εκτιμάται ότι θα αυξηθούν στους 3,8 Δισεκατομμύρια μέχρι το 2027 [2]. Με την ανάπτυξη όμως καινούργιων τεχνολογιών τόσο μέσα στην βιομηχανία αλλά και έξω από αυτήν, είμαστε πλέον σε μια εποχή όπου τα περισσότερα αν όχι όλα, από την ανάπτυξη μέχρι και την χρήση ενός παιχνιδιού, γίνονται ολοένα και πιο πολύπλοκα. Διαφορετικά, θα ήταν πολύ ευπαθή σε επιθέσεις και κλοπή δεδομένων, όπως και υπήρχαν κατά καιρούς. Γι’ αυτό χρειάζεται η ανάπτυξη συστημάτων ασφάλειας, καλή ενημέρωση και προσοχή από τον προγραμματιστή και τον χρήστη αλλά και νόμοι που να προστατεύουν τα δεδομένα του χρήστη.

Το υπόλοιπο έγγραφο οργανώνεται στην 2η Ενότητα, που περιγράφει διάφορους κινδύνους που υπάρχουν στον χώρο του Gaming Industry, όπως κλοπές πνευματικών δικαιωμάτων, Malware attacks, παραβιάσεις προσωπικών δικαιωμάτων των χρηστών, cheating στην 3η Ενότητα οπού θα αναφερθούν κάποια breaches που έχουν βρεθεί κατά καιρούς, ως παραδείγματα. Τέλος, στην 4η Ενότητα παρουσιάζονται κάποιοι τρόποι για να κάνουν ασφαλέστερα τα παιχνίδια και να προστατέψουν τους χρήστες.

# ΚΙΝΔΥΝΟΙ ΣΤΟ GAMING

## *Code Injection*

Code Injection είναι ο όρος των επιθέσεων κατά των οποίων εισάγεται ξένος κώδικας στον κώδικα της εφαρμογής, και αργότερα εκτελείται. Συνήθως, αυτό συμβαίνει όταν δεν υπάρχει σωστή μεταχείριση δεδομένων των οποίων δεν γνωρίζουμε την προέλευσή τους ή είναι μη-έμπιστη. Τέτοιου είδους κώδικας μπορεί να εισαχθεί και με την μορφή αρχείων. Οι μηχανές ανάπτυξής χρησιμοποιούν διάφορα assets για την γραφική αναπαράσταση των παιχνιδιών. Τα συγκεκριμένα assets ενώ μπορούν να δημιουργηθούν και κατευθείαν από τον ίδιο τον προγραμματιστή του παιχνιδιού, υπάρχουν και πολλά τα οποία είναι έτοιμα για τον προγραμματιστή να χρησιμοποιήσει φτιαγμένα από άλλους χρήστες. Σε αυτήν την περίπτωση πρέπει ο προγραμματιστής να είναι σίγουρος για την ασφάλεια του asset που θα χρησιμοποιήσει. Μια επιτυχημένη τέτοια επίθεση, μπορεί να επιτρέψει μη εξουσιοδοτημένη πρόσβαση σε αρχεία και δεδομένα του παιχνιδιού, του προγραμματιστή και του συστήματος σε κάποιον άλλο χρήστη, καθώς ο 2ος θα μπορεί να εκτελέσει ενέργειες όπως να καταστρέψει ή να αλλάξει σημαντικά αρχεία και να κλέψει διάφορες πληροφορίες. [3]

## *Insecure Authentication*

Μια κακή αυθεντικοποήση συστήματος, επιτρέπει επίθεσης κατά τις οποίες ο επιτιθέμενος εμφανίζεται σαν κανονικός χρήστης. Τέτοια προβλήματα αυθεντικοποίησης μπορεί να δημιουργηθούν με το να μην αγνοήσουμε περιοχές μεγάλου ρίσκου, λόγω λαθών στον κώδικα ή ακόμα και λόγω κακών επιλογών του ίδιου του χρήστη. Αυτές οι επιθέσεις οδηγούν σε, κλοπή ευαίσθητων πληροφοριών του χρήστη, να πάρουν τον πλήρη έλεγχο ενός συστήματος ή ακόμα και να «κλείσουν» μια εφαρμογή στην περίπτωση που καταφέρουν να αποκτήσουν πρόσβαση στους λογαριασμούς των ίδιων των admin. Επιπλέον, επηρεάζεται αρνητικά η αξιοπιστία της εταιρείας και μπορεί να νομικές συνέπειες αναλόγως τον δεδομένων που κλάπηκαν. [4]

## *Insecure Data Storage*

Insecure data storage αναφέρεται στα δεδομένα και στις πληροφορίες που υπάρχουν χωρίς την προστασία κάπου firewall ή κάποιας κρυπτογράφησης, ή στις μη-σκόπιμες διαρροές δεδομένων λόγω κακού σχεδιασμού εφαρμογής. Αυτού του είδους ο κίνδυνος είναι από τους μεγαλύτερους όσο αναφορά τα κινητά, και μπορεί να προκύψουν εάν ο επιτιθέμενος αποκτήσει πρόσβαση στην φυσική συσκευή ή χρησιμοποιώντας κάποιο malware για την κλοπή των δεδομένων. [5]

## *Insecure Network Communication*

Σήμερα τo gaming στηρίζεται πολύ στον ίντερνετ, κάνοντας έτσι τις επιθέσεις στην επικοινωνία μέσω αυτού πολύ κοινές. Αν το network traffic δεν είναι σωστά κρυπτογραφημένο ή επιβεβαιωμένο, η επίθεση μπορεί να οδηγήσει σε:

* Eavesdropping: ο επιτιθέμενος έχει πρόσβαση σε δεδομένα όπως login credentials, προσωπικά δεδομένα και chat logs καθώς επίσης μπορεί να κλέψει και πληροφορίες ενδοεταιρικές, όπως οικονομικά, πληροφορίες για καινούργια προϊόντα, για το προσωπικό και αλλά απόρρητα στοιχεία με απώτερο σκοπό να κερδίσει λεφτά ή άλλους κακόβουλος σκοπούς. [6]
* Data Tampering: σημαίνει να αλλάξει ή να διαγραφεί ένα πακέτο με σκοπό να χειραγωγήσει τα game data. Με αυτό τον τρόπο, κερδίζει άδικα πλεονεκτήματα στο ίδιο το παιχνίδι έχοντας πρόσβαση στον ίδιο των κώδικα του παιχνιδιού.[7]
* Man-in-the-Middle Attacks: είναι όταν ο επιτιθέμενος σταματάει και τοποθετεί τον εαυτό του στην μέση μιας επικοινωνίας, έτσι ώστε να φαίνεται στον χρήστη ότι επικοινωνεί φυσιολογικά με την εφαρμογή, κλέβοντας έτσι δεδομένα όπως login credentials, πληροφορίες λογαριασμού, αριθμούς τραπεζικών καρτών κτλ. [8]

## *Cross-Site Attacks*

Cross-Site επιθέσεις είναι οι web-based επιθέσεις στις οποίες ο επιτρέπουν την εισαγωγή scripts στον κώδικα. Υπάρχουν 2 ειδών Cross-Site επιθέσεων:

1. Cross-Site Scripting (XSS)

Κατά αυτήν την επίθεση, το script εισάγεται είτε στο web interface του παιχνιδιού είτε στο chat, επιτρέποντας σε κάποιον να κλέψει δεδομένα ή πρόσβαση στο σύστημα ή στον online λογαριασμό του χρήστη (Session Hijacking). [9]

1. Cross-Site Request Forgery (CSRF)

Κατά αυτήν την επίθεση, το script υπάρχει στην μορφή link ή ακόμα και ολόκληρου website. Το χρησιμοποιημένο πλέον script από τον χρήστη, επιτρέπει στον hacker να πραγματοποιήσει ενέργειες την θέση του χρήστη. Τέτοιες ενέργειες συμπεριλαμβάνουν την αλλαγή του password και την αγορά προϊόντων. [10]

## *Buffer Overflows*

Αυτού του είδους οι επιθέσεις εκμεταλλεύονται την υπερχείλιση που μπορεί να δεχτεί ένας buffer. Μέσα σε μια τέτοια επίθεση, εισάγονται περισσότερα δεδομένα από αυτά που μπορεί να διαχειριστεί ο buffer, επιτρέποντας στον hacker να αλλάξει τα δεδομένα σε διαφορετική θέση της μνήμης. Οι Buffer Overflows επιθέσεις χρησιμοποιούνται για διάφορους λόγους, όπως να αλλάξουν σημαντικό κομμάτι του κώδικα, να καταρρεύσουν μια εφαρμογή, να εισάγουν malwares και κακόβουλο κώδικα ή να αλλάξουν την ροή του προγράμματος που μπορεί να οδηγήσει σε διαφορετικού είδους επιθέσεις όπως για παράδειγμα Denial of Service (DoS) Attacks. [11]

# ΓΝΩΣΤΕΣ ΠΑΡΑΒΙΑΣΕΙΣ

Κατά καιρούς έχουν βρεθεί διάφορες αδυναμίες στην ασφάλεια των μηχανών ανάπτυξης αλλά και των ίδιων των τελικών προϊόντων. Άλλες βρέθηκαν και αντιμετωπίστηκαν γρήγορα χωρίς συνέπειες, ενώ άλλες τις εκμεταλλεύτηκαν με αποτέλεσμα την παραβίαση προσωπικών δεδομένων. Μερικά τέτοια παραδείγματα αναφέρονται παρακάτω.

1. Την πλατφόρμα της Epic Games, Unreal Engine (UE), χρησιμοποιεί ο Αμερικανικός στρατός στις περιοχές δοκιμής (proving grounds). Μετά την κυκλοφορία της UE3 το 2004, υπήρχαν αρκετά προβλήματα με την ασφάλεια της νέας αυτής πλατφόρμας. Η συγκεκριμένη πλατφόρμα χρησιμοποιούταν από τα proving grounds του Αμερικανικού στρατού. Το 2008 βρέθηκε ότι η UE3 είναι ευπαθή σε DoS επιθέσεις, αφού στέλνοντας ένα αρκετά μεγάλο ειδικό πακέτο, κάποιος μπορούσε να κρασάρει την εφαρμογή. Ενώ το 2018, βρέθηκε ότι μέσω της UE μπορούσε να σταλθεί ένα «λάθος» πακέτο μέσω User Datagram Protocol (UDP), στο οποίο ο server απαντούσε, ενίσχυε την πιθανότητα DoS επιθέσεις και το καθιστούσε εύκολο στην χρήση του για DDoS επιθέσεις. [12]
2. To 2019, η Unity παρουσίασε μια καινούργια λειτουργία στην πλατφόρμα τους, την εισαγωγή 3D Models. Η συγκεκριμένη λειτουργία επέτρεπε στον χρήστη να εισάγει ένα έτοιμο 3D μοντέλο από τον υπολογιστή, κάνοντας έτσι πιο γρήγορη την διαδικασία την δημιουργίας του προϊόντος. Όμως, αναλυτές ασφαλείας βρήκαν ότι η λειτουργία είχε μια «τρύπα» που έδινε την δυνατότητα σε κάποιον σε κάποιον να εκτελέσει αυθαίρετο κώδικα στον υπολογιστή του χρήστη.[13]
3. Το 2020, η Nintendo, μια από τις μεγαλύτερες εταιρίες στο Gaming Industry, ανακοίνωσε πως τα δεδομένα της είχαν παραβιαστεί. Στην ανακοίνωση τους αναφέρουν πως κάποιος με την χρήση Nintendo Network ID (NNID), παλαιότερων κονσόλων που δεν υποστήριζαν two-factor authentication, απέκτησε πρόσβαση σε πληροφορίες παράνομα. Αργότερα, ανακοίνωσε πως ο αριθμός που δέχθηκαν επίθεση ανερχόταν στα 160000, ενώ το 1% αυτών χρησιμοποιήθηκαν για παράνομες αγορές. [14]
4. Η Sony είναι μια από τις μεγαλύτερες εταιρίες στον χώρο των προϊόντων τεχνολογίας και κατασκευαστής των διάσημων κονσόλων PlayStation, καθώς έχει και πολλά στούντιο παραγωγής παιχνιδιών. Το 2011, η Sony υπέστη μια από τις μεγαλύτερες επιθέσεις στην ιστορία. Κατά αυτήν την επίθεση, κλάπηκαν ονόματα, διευθύνσεις, usernames, passwords, security questions και πιθανώς στοιχεία τραπεζικών καρτών από περίπου 77 εκατομμύρια χρήστες του PlayStation Network (PSN). Κατευθείαν η εταιρεία έκλεισε το δίκτυο της, χάνοντας ο χρήστης κάθε λειτουργία που χρειαζόταν σύνδεση στο PSN, όπως για παράδειγμα την ψηφιακή αγορά και «κατέβασμα» παιχνιδιών.[15]
5. Το 2016 κυκλοφόρησε η Nintendo σε συνεργασία το 1ο augmented reality game κινητού, το “Pokémon Go”. Το παιχνίδι για το login μέσω Google ζητάει πρόσβαση σε διάφορα στοιχεία, όπως το user id και το email. Όμως βρέθηκε ότι στις iOS συσκευές η εφαρμογή είχε πρόσβαση και σε άλλες εφαρμογές της Google που ήταν συνδεδεμένες με το ίδιο Google Account, όπως το Gmail και το Google Docs, καθώς μπορούσε να παρακολουθήσει το location history και το search history. Η εταιρία αμέσως βγήκε και ενημέρωσε πως θα το διορθώσει, όπως και έγινε.[16]
6. To 2017, η Epic Games, δημιουργός της Unreal Engine, κυκλοφόρησε το “Fortnite”, ένα online player versus player online battle royale παιχνίδι. Το παιχνίδι εξελίχθηκε σε ένα από τα δημοφιλέστερα παιχνίδια μέσα στα επόμενα χρόνια, και σήμερα είναι το μεγαλύτερο και δημοφιλέστερο στο είδος του. Όμως, αυτό το έκανε και στόχο επιθέσεων. Στα τέλη του 2018 με αρχές του 2019, hackers κατάφεραν να εισχωρήσουν στον κώδικα του παιχνιδιού, αλλάζοντας το login page σε αυτό προηγούμενης μη-ασφαλούς έκδοσης από του οποίου κατάφεραν να κλέψουν τα tokens αυθεντικοποίησης των χρηστών. Με αυτό τον τρόπο, οι hackers είχαν πρόσβαση σε χιλιάδες λογαριασμούς από τους οποίους πήραν τα στοιχεία των συνδεμένων τραπεζικών καρτών ή ακόμα και πουλώντας τα Login Credentials των ίδιων των λογαριασμών. [17]
7. Το 2017, βρέθηκε ένα corrupted .dll αρχείο που σχετιζόταν με την αντί πειρατεία του παιχνιδιού

“Life is Strange”. Το αρχείο επέτρεπε πιθανούς επιτιθέμενους να το εκμεταλλευτούν ώστε να εκτελέσουν κώδικα ή να πάρουν μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή του χρήστη που εγκαθιστούσε το παιχνίδι. [18]

# ΤΡΟΠΟΙ ΑΤΝΙΜΕΤΩΠΙΣΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ

Όπως είδαμε σε προηγούμενη ενότητα, υπάρχουν διάφοροι τρόποι ώστε κάποιος να παραβιάσει την ασφάλεια. Και ενώ τον μεγαλύτερο κίνδυνο τον διατρέχουν οι χρήστες του ολοκληρωμένου παιχνιδιού, αφού σήμερα χρειάζεται να δώσουν προσωπικά στοιχεία και άδειες χρήσης αυτών, στις εφαρμογές και κατ’ επέκταση στις εταιρείες, αυτό δεν σημαίνει πως δεν υπάρχουν τρόποι για την καλύτερη ασφάλεια από πλευράς εταιρειών. Κάποιοι από αυτούς είναι:

* Code Obfuscation: είναι η «περιπλοκή» του κώδικα, έτσι ώστε σε περίπτωση που πέσει στα χέρια ενός hacker, να κάνει πιο δύσκολη την αντίστροφη μηχανική του. Έτσι, μειώνεται ο κίνδυνος κλοπής δεδομένων και πνευματικών δικαιωμάτων σε πιθανούς επερχόμενους τίτλους παιχνιδιών, μη εξουσιοδοτημένης πρόσβασης καθώς και δημιουργία cheats για το παιχνίδι.[19]
* Ασφαλή Δίκτυο: δηλαδή χρήση εργαλείων, όπως Firewalls, συχνά Intrusion Prevention Systems (IPS) scans, Anti-Viruses και Anti-Malware προγράμματα.
* Asset Validation: δηλαδή πριν την χρήση κάποιου Asset στην δημιουργία ενός παιχνιδιού, να γίνεται σωστός έλεγχος προέλευσης του, για την μείωση πιθανότητας να χρησιμοποιηθεί ως μέσο για επίθεση στο σύστημα μας.
* Multi-factor Authentication: είναι η πολλαπλή διαδικασία Login, βάζοντας τους χρήστες να χρησιμοποιήσουν παραπάνω πληροφορίες ταυτοποίησης τους. Για παράδειγμα, έναν κωδικό σταλμένο στο κινητό ή η απάντηση σε μια συγκεκριμένη ερώτηση. [20]
* «Εκπαίδευση» του παίχτη: δηλαδή η παροχή καλών πρακτικών προστασίας δεδομένων στους παίχτες, όπως tips για την δημιουργία «δυνατότερων» passwords, και αποφυγής επιθέσεων phishing.

Θα μπορούσαμε και την κρυπτογράφηση στους τρόπους, όμως η σχέση παιχνιδιών-κρυπτογράφησης, αυτήν την στιγμή είναι λίγο περίεργη. Από την μια, η κρυπτογράφηση είναι από τους ασφαλέστερους τρόπους επικοινωνίας, αφού στέλνονται τα δεδομένα σε μια μορφή που δεν είναι αναγνωρίσιμη και μόνο ο σωστός δέκτης μπορεί να το αποκρυπτογραφήσει και να το διαβάσει. Και χρησιμοποιείται για την ασφαλέστερη μεταφορά προσωπικών δεδομένων μεταξύ παίχτη και server. Δυστυχώς, δεν μπορεί να χρησιμοποιηθεί για ολόκληρο το παιχνίδι όμως. Διότι, θα «ανακάτευε» το παιχνίδι τόσο πολύ, που θα του δημιουργούσε πολλά bugs, κάνοντας το πιθανώς un-playable. [21]

# ΣΥΜΠΕΡΑΣΜΑΤΑ

Όσο περνάνε τα χρόνια, όπως βλέπουμε το Gaming μεγαλώνει, και έχει φτάσει σε ένα σημείο συνεχούς χρήσης διαδικτύου. Η ασφάλεια του λοιπόν, θα γίνεται ολοένα και πιο σημαντική, αφού πρέπει να προστατεύονται και οι παίχτες αλλά και οι ίδιες οι εταιρείες. Στους πρώτους, για την αποφυγή κλοπής προσωπικών δεδομένων και στους δεύτερους, για την αποφυγή στοιχείων ή ακόμα και κώδικα που μπορεί να θέσει σε κίνδυνο τους προγραμματιστές αλλά και να επιφέρει ζημιές εκατομμυρίων.

Αναφορές

1. “Game Engines: All you need to know” .Available: <https://www.gameopedia.com/game-engines-all-you-need-to-know-about/#:~:text=Game%20engines%20often%20include%20core,are%20capable%20of%20platform%20abstraction>.
2. “Video Game Industry Revenue & Market Share (May 2023)” Available: <https://www.bankmycell.com/blog/video-game-industry-revenue>
3. “Code Injection” Available: https://owasp.org/www-community/attacks/Code\_Injection
4. “11 Common Authentication Vulnerabilities You Need To Know” Available: <https://www.strongdm.com/blog/authentication-vulnerabilities#:~:text=What%20Are%20Authentication%20Vulnerabilities%3F,masquerade%20as%20a%20legitimate%20user>.
5. “Insecure Authentication – Everything You Need to Know” Available: <https://www.appsealing.com/insecure-authentication/>
6. “Dangers of Eavesdropping” - Chapter 3, Seven Deadliest Unified Communications Attacks. Dan York
7. “What is Data Tampering?” Available: <https://study.com/academy/lesson/what-is-data-tampering-definition-prevention.html#:~:text=Data%20tampering%20is%20the%20act,are%20all%20about%20data%20transmission>.
8. “Man in the middle (MITM) attack” Available: <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>
9. “Cross Site Scripting” Available: <https://owasp.org/www-community/attacks/xss/>
10. “Cross Site Request Forgery” Available: <https://www.synopsys.com/glossary/what-is-csrf.html#:~:text=Cross%2DSite%20Request%20Forgery%20(CSRF)%20is%20an%20attack%20that,has%20in%20an%20authenticated%20user>.
11. “A Buffer Overflow Attack” Available: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/what-is-a-buffer-overflow/#:~:text=A%20buffer%20overflow%20attack%20is,in%20other%20parts%20of%20memory>.
12. “National Vulnerability Database” Available: <https://nvd.nist.gov/vuln/detail/CVE-2008-3410> <https://nvd.nist.gov/vuln/detail/CVE-2018-10531>
13. “CVE-2019-9197” Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9197>
14. “The Nintendo Cyber Security Data Breach” Available: <https://cydrill.com/cyber-security/the-nintendo-cyber-security-data-breach/>
15. “Sony Data Breaches: Full Timeline Through 2023” Available: <https://firewalltimes.com/sony-data-breach-timeline/>
16. “Pokemon Go promises to fix the bug that let it access all your Google data” Available: <https://techcrunch.com/2016/07/12/pokemon-go-promises-to-fix-the-bug-that-let-it-access-all-your-google-data/>
17. “Fortnite (Data Breach)” Available: <https://www.fdazar.com/practice-areas/class-action/fortnite-data-breach/>
18. “A third-party DLL vulnerability in Life is Strange could allow malicious code execution” Available: <https://www.pcgamer.com/a-third-party-dll-vulnerability-in-life-is-strange-could-allow-malicious-code-execution/>
19. “What is Obfuscation?” Available: <https://www.preemptive.com/obfuscation/>
20. “What is Multi-Factor Authentication?” Available: <https://aws.amazon.com/what-is/mfa/#:~:text=Multi%2Dfactor%20authentication%20(MFA),question%2C%20or%20scan%20a%20fingerprint>.
21. “Why Encryption Tech is So Important In Gaming” Available: <https://dazeinfo.com/2022/01/05/why-encryption-tech-is-so-important-in-gaming/>