THE FORTNITE UNDERGROUND CYBERCRIME ECONOMY.

Written by Vinny Troia

NIGHT LION SECURITY

DATABA$E HACKER$ FUEL A BILLION DOLLAR GAMING ACCOUNT BLACK MARKET.

With each passing day it seems like millions of additional records are stolen in the latest data breach, but what does that really mean? What happens to those records? Where do they end up, and how does it impact consumers?

This report will provide an inside look at the lucrative economy of hacked consumer gaming accounts, where cyber criminals are earning upwards of $40,000 per week in profits.

IN 2019 ALONE, THERE WERE MORE THAN 4 BILLION BREACHED RECORDS.

In 2020 so far, we have an estimated additional 2 billion breached records that have gone up for sale on various darkweb markets.

Hacking groups like **Gnostic Players** and **Shiny Hunters** account for a vast majority of breaches involving stolen user data, and are indirectly responsible for fueling an entire criminal economy of stolen accounts.

These hacked databases are then sliced up and resold, only to provide ammunition for credential stuffing attacks designed to identify valid accounts across different consumer products.

These stolen accounts are then packaged and resold across a number of sub-ecosystems, the most profitable being the market for hacked gaming accounts.

WHAT IS CREDENTIAL $TUFFING?

Taking large combinations of username/passwords and “stuffing” them into a digital service to gain access. Because people reuse the same password, one valid password often works across multiple sites.

...CONTINUES ON NEXT PAGE

© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com

This report will also provide an inside look into the black market of hacked gaming of stolen Fortnite accounts, and even provide direct insight from some of its most profitable hackers.

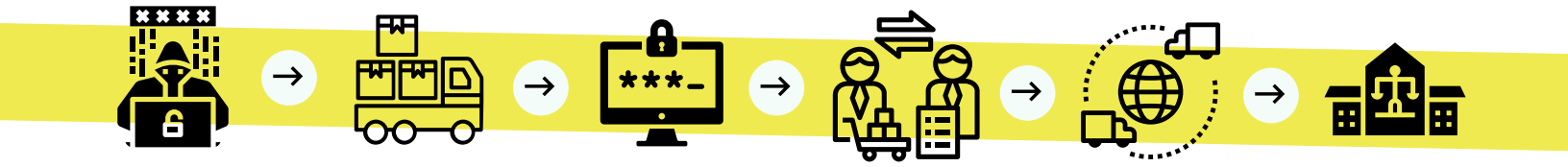
Akamai Technologies' 2019 State of Internet/Security report highlighted how users of gaming platforms are the most common victims of these attacks because the accounts fetch a premium.

The Akamai report goes on to detail that approximately 51% of credential stuffing attacks originating from Eastern European countries between 2017 and 2019 targeted the gaming industry.

Unfortunately, it is impossible to know where these attacks actually originate from due to the use of VPNs (virtual private networks) and VPS (virtual private servers) which can be purchased from anywhere.

This report will dive deeper into this phenomena of stolen account sales and provide an example of the underground ecosystem of just one genre of stolen gaming accounts.

THE STOLEN ACCOUNT SUPPLY CHAIN CYCLE:



MATERIAL GATHERING

Data stolen from hacked companies fuels the market

PROCUREMENT

Fresh data sold to distributors and resellers

TRANSFORM MATERIALS

Credential stuffing attacks used to detect valid accounts

FULFILLMENT

Valid accounts are packaged and resold in groups called "Logs"

DISTRIBUTION

Individual accounts are posted for sale at various online marketplaces

AFTER-SALE SERVICES/RETURNS

An underground court presides over disputes and scams

SUB-MARKETS AND FORTNITE

The market for stolen account sales is much larger than just the gaming industry. Due to the nature of consumers reusing passwords, the supply chain discussed in this report applies to many subgenres of consumer accounts.

Popular account types also include banking and cryptocurrency logins (for financial crimes), as well as media & streaming accounts, ranging anywhere from Spotify to adult entertainment, to Netflix and Disney+.

However, from our research, the black market for the buying and selling of stolen Fortnite accounts is among the most expansive, and also the most lucrative.

Collections of a few thousand stolen accounts are grouped together and auctioned in private Telegram channels selling from anywhere between $10,000 and $40,000!

© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com

MATERIAL GATHERING:
THE INITIAL HACK

The initial hack on an organization can take many forms, including injection attacks or crafted web exploits. Over the past several years, groups like Gnostic Players and Shiny Hunters have been able to successfully hack hundreds of organizations using credential stuffing attacks to access developer Git accounts in search of AWS keys or hard-coded database credentials.

These credential stuffing attacks are relatively easy to pull off. Requests sent to Git accounts include the username and password in a single command, so building millions of password variations can be done easily with the use of regular expressions or tools like JohnTheRipper.

Once the actors gain access to the developer Git accounts, they typically use automated scripts to look for credentials or AWS keys that have been checked into the code repositories.

In many cases, a developer may hard code credentials for testing purposes, then accidentally check in the code leaving the credentials in the Git history.

Once the hackers have access to the organization's AWS or Azure accounts, it is often simply a question of looking around for which data to exfiltrate.

Data exfiltration almost always goes undetected.

Our report on "The Dark Overlord" group describes how these groups have been responsible for approximately 40% of all non-credit card data breaches over the past three years.

PROCUREMENT:
STOCKING THE DATA DISTRIBUTORS

Fresh data is rarely published or announced and is often only sold in private circles. Data containing plain-text passwords or MD5 password hashes are the most valuable because they are easily crackable. Passwords encrypted with Bcrypt are less valuable because they are extremely difficult to crack.

Once the initial data is sold, the password hashes are cracked and the resulting email/password combinations are then repackaged for further credential stuffing attacks.

One of the most profitable uses of fresh account data is the identification and sale of valid Fortnite accounts.

MATERIAL TRANSFORMATION:
EXTRACTING ACTIVE FORTNITE ACCOUNTS

Checking for valid Fortnite accounts can be as easy as loading a list of email/password combinations into the right software.

DonJuji, a well-known and respected cracker in underground hacking circles, states that high-end Fortnite cracking tools can average between 15 and 25 thousand checks per minute, or roughly 500 account checks per second.

But it's not always about brute force and volume of combinations. "Simple variations on existing passwords can yield extremely high results", states DonJuji, who attributes much of his success to his understanding of the common patterns used by people when choosing passwords.

When changing passwords, people commonly make small and predictable changes, like capitalizing the first letter, or adding a single digit at the end of the password.

Some of DonJuji's more effective techniques involve using a person's username as their password, or using the numbers found at the end of a person's email address and appending them to the end of their password.

For example, if an email address is Joe189@gmail.com, one possible password variation for that account would be joesusername189.

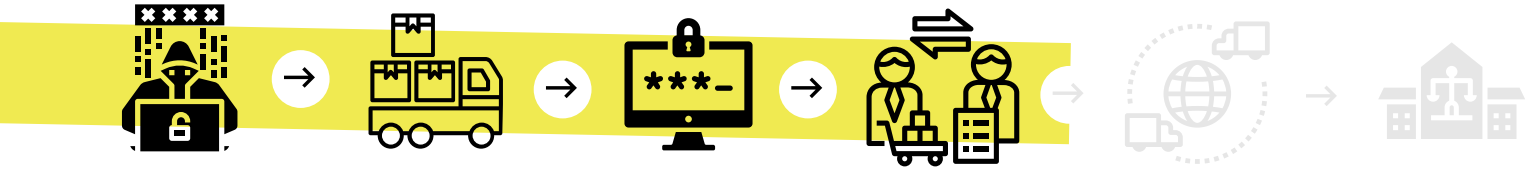
Epic Games makes efforts to stop these mass account checks by limiting the number of logins per IP address. Hackers circumvent this restriction by using expensive proxy rotation services like Luminati or OxyLabs, which provide a new IP address with each request.

Companies like Epic Games can make every attempt to block IPs associated with proxy or VPN companies, but the more expensive proxy services are one step ahead, offering access to "residential IPs" that can easily pass through firewall filters.

"I SPEND MORE THAN $10,000 PER MONTH ON DIFFERENT PROXY SERVICES."

— DONJUJI, THE "DON" OF FORTNITE ACCOUNTS

© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com



FULFILLMENT: CREATING VALID ACCOUNT LOGS

If proxy services provide the means for checking account validity, then all-in-one tools like Axenta enable the use of those services. Axenta, the most popular Fortnite account checker on the market, provides a number of different built-in tools like password checking, automatic password changing, Fortnite skin checking and automatic proxy rotation. The cost for the base version of Axenta is $15 per month.

For hardcore sellers, Axenta has private "EVO" version that sells for $2,000 per month and requires a referral from an existing user.

* *Note: Axenta now has a Valorant variant, designed to check for valid Valorant accounts. Valorant is Riot Games' version of Fortnite. Crackers have already started testing and holding hacked Valorant accounts for a time when the accounts become more valuable.*

THE VALUE OF A FORTNITE ACCOUNT

The value of a hacked Fortnite account comes from the character's in-game "skin". This single digital costume is what makes these accounts so valuable, and is at the core of the entire underground Fortnite market.

*Output of a completed Log from Axenta, packaged with no regard for OP-SEC. You can see the actor's conversation behind it!

CREATING ACCOUNT "LOGS"

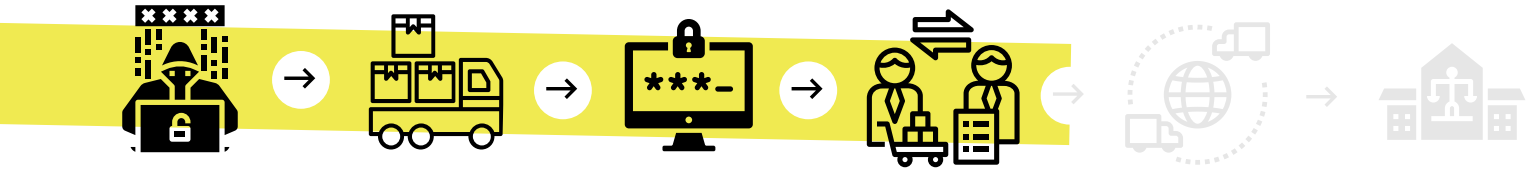
Valid logins are then grouped into batches and fed through tools like Axenta to check for their "skin" contents.

Valid Epic Games accounts may not have Fortnite characters or skins associated with them, so typical checks for valid accounts are done in batches of 10 or 20,000 to reduce costs and processing time.

According to several successful crackers, checking for skins on Epic Games logins will yield an average success rate of 10-15%.

Assuming a batch of 20,000 checked accounts, a seller will end up with approximately 2,000 skins. These skins are then packaged and sold as a single "Log".

© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com

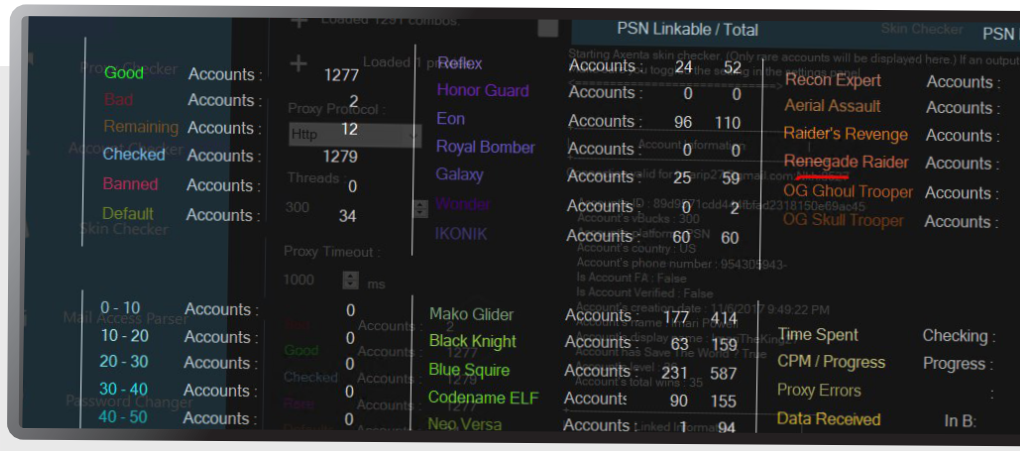


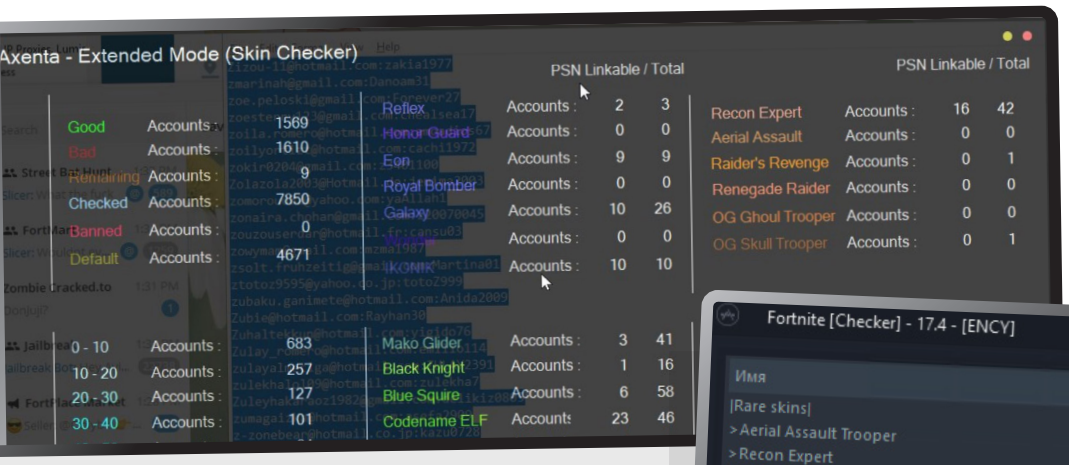
DISTRIBUTION:
STOCKING THE DATA DISTRIBUTORS

During the initial phase of distribution, a Fortnite hacker will screenshot the Log output from Axenta and begin advertising the Log product in various Telegram and Discord channels.

The higher-end Telegram channels are heavily vetted requiring proof of funds and an existing member to vouch for entry. Logs in these channels typically sell between $10,000 and $30,000, but can go as high as $50,000.

"Logs" like this regularly sell for $18,000 in a private Telegram channels.

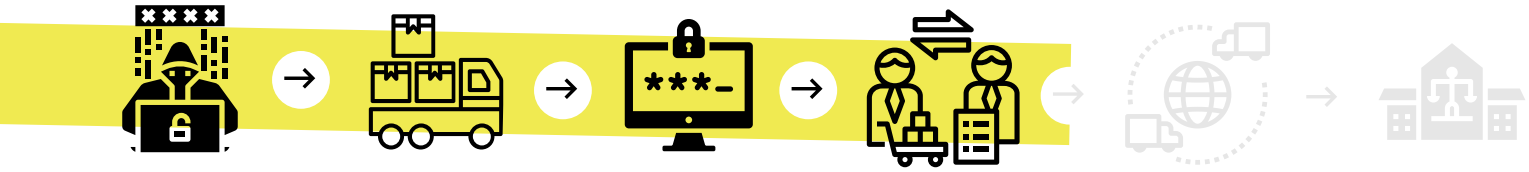




On the higher end of account sales, this Log sold for a whopping $38,000 in a private Telegram auction.

The following Log was sold for $27,000 on "One Stonk Shop", a mid-tier sales channel run by MrTayota, a known associate and reseller of Gnostic Players.

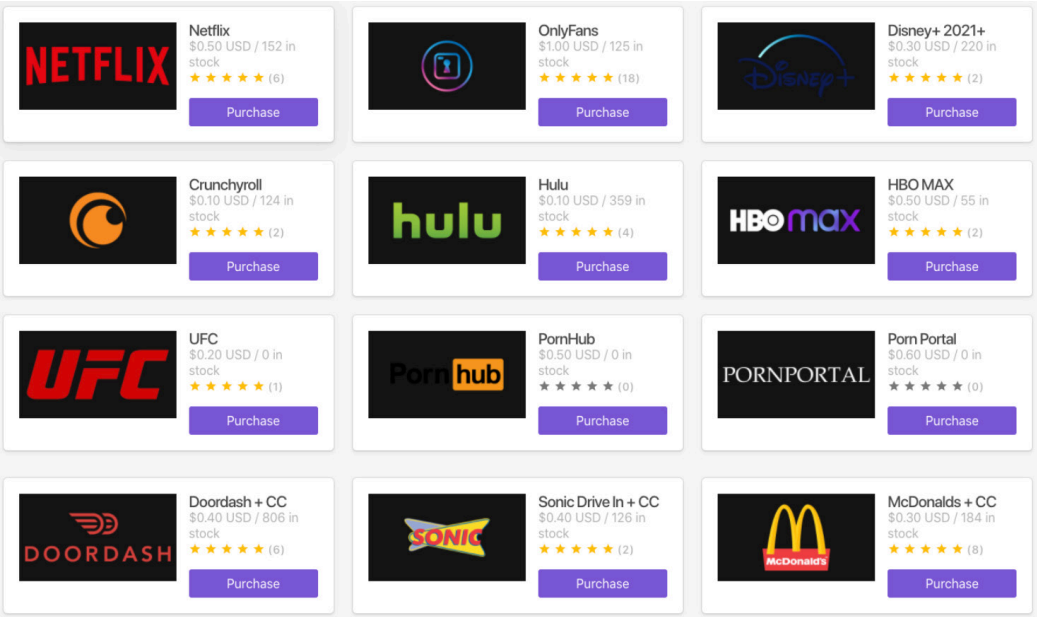
© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com



DISTRIBUTION:
DIRECT B2C SALES CHANNELS

After a Log is purchased, the accounts are extracted and individually posted for sale. Many account resellers host their own "account shops" on websites like shoppy.gg or atshop.io.

Account shops typically contain a wide mix of accounts that can be purchased, including Netflix, Disney+, HBO Max, and a plethora of other paid accounts.



THE PRICE OF INDIVIDUAL FORTNITE ACCOUNTS:

The following is a ballpark pricing chart based on current prices:

SEASON 1 SKINS
$25-250 PER SKIN

Season 1 skins are referred to as "OGs" and typically range between $25 and $250 per skin.

BLACK KNIGHT SKINS
$25 PER ACCOUNT

Black Knight (BK) skins are from season 2, and are worth about $25 per account.

UNLINKED (PSN) ACCOUNTS
WORTH 2X REGULAR VALUE

Accounts not linked to an existing Play Station Network (PSN) account are typically worth 2x. This would allow a player to link the account to their own PSN account.

RECON EXPERT SKIN
$2,500 PER ACCOUNT

Earlier this month the "Recon Expert" skin was the most valuable, averaging roughly $2,500 per account.

WORTH 3X REGULAR VALUE!
FULL ACCESS ACCOUNTS

"Full access" accounts include access to the owner's hacked email, preventing the ability to take back ownership of an account.
FA accounts typically add 3x value.

TO PUT THIS ALL IN CONTEXT, A SINGLE UNLINKED FULL-ACCESS RECON EXPERT ACCOUNT CAN SELL FOR UPWARDS OF $10,000!

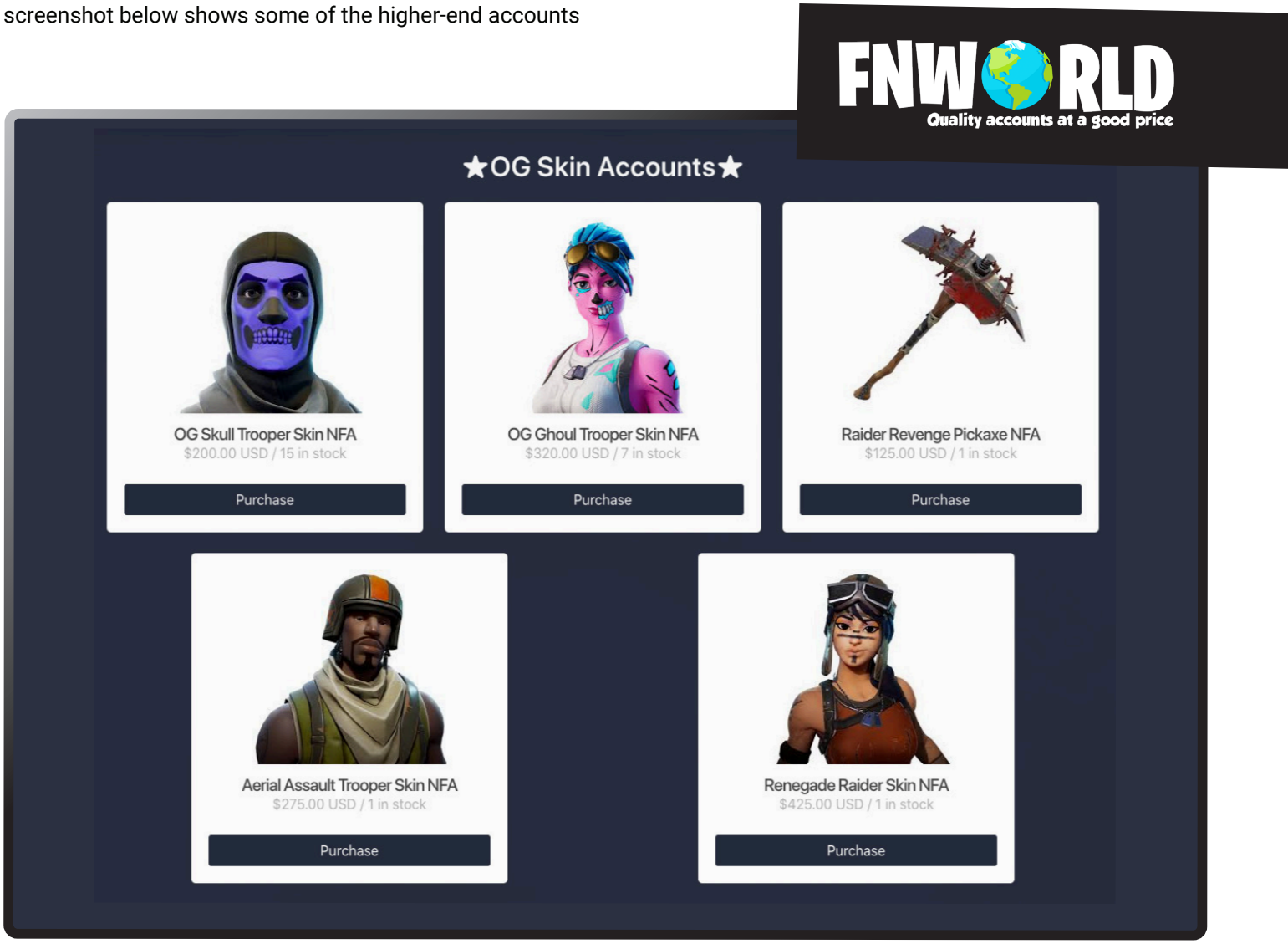
© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com

DISTRIBUTION:
DIRECT B2C SALES CHANNELS

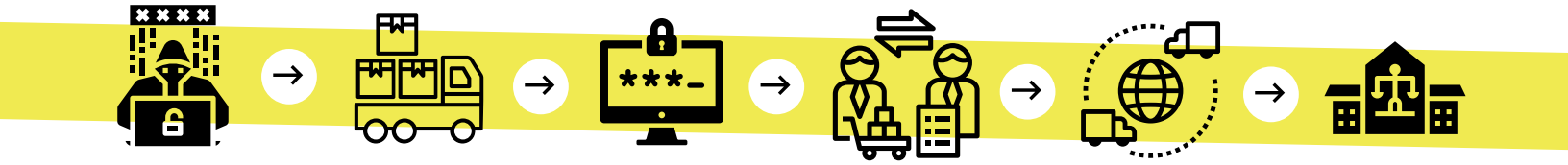
One of the largest known buyer of Fortnite Logs, “Tzetale”, who also goes by @Prostitute or @tzetale on Telegram, is regularly seen spending thousands of dollars in private sales channels. According to several of direct sellers, Tzetale spends 20-30k *per week* on fresh accounts in order to stock his online shop, Fortnite World (www.fnworld.io).

Fortnite World is currently one of the most profitable hacked gaming account shops on the Internet. The screenshot below shows some of the higher-end accounts for sale on the Fortnite World website. New accounts are added daily, and can be seen selling out as quickly as you can press the refresh button on your browser.

FNWorld also sells prestigious “full access” accounts, which means the buyer also gets access to the victim’s hacked email address to prevent the account from being recovered.



© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com



CUSTOMER SERVICE AND RETURNS

ANY LEGITIMATE SUPPLY CHAIN HAS A PROCESS FOR HANDLING CUSTOMER SERVICE AND RETURNS.

IN THE FORTNITE COMMUNITY, THIS IS HANDLED BY "COMMUNITY CHECKUP."

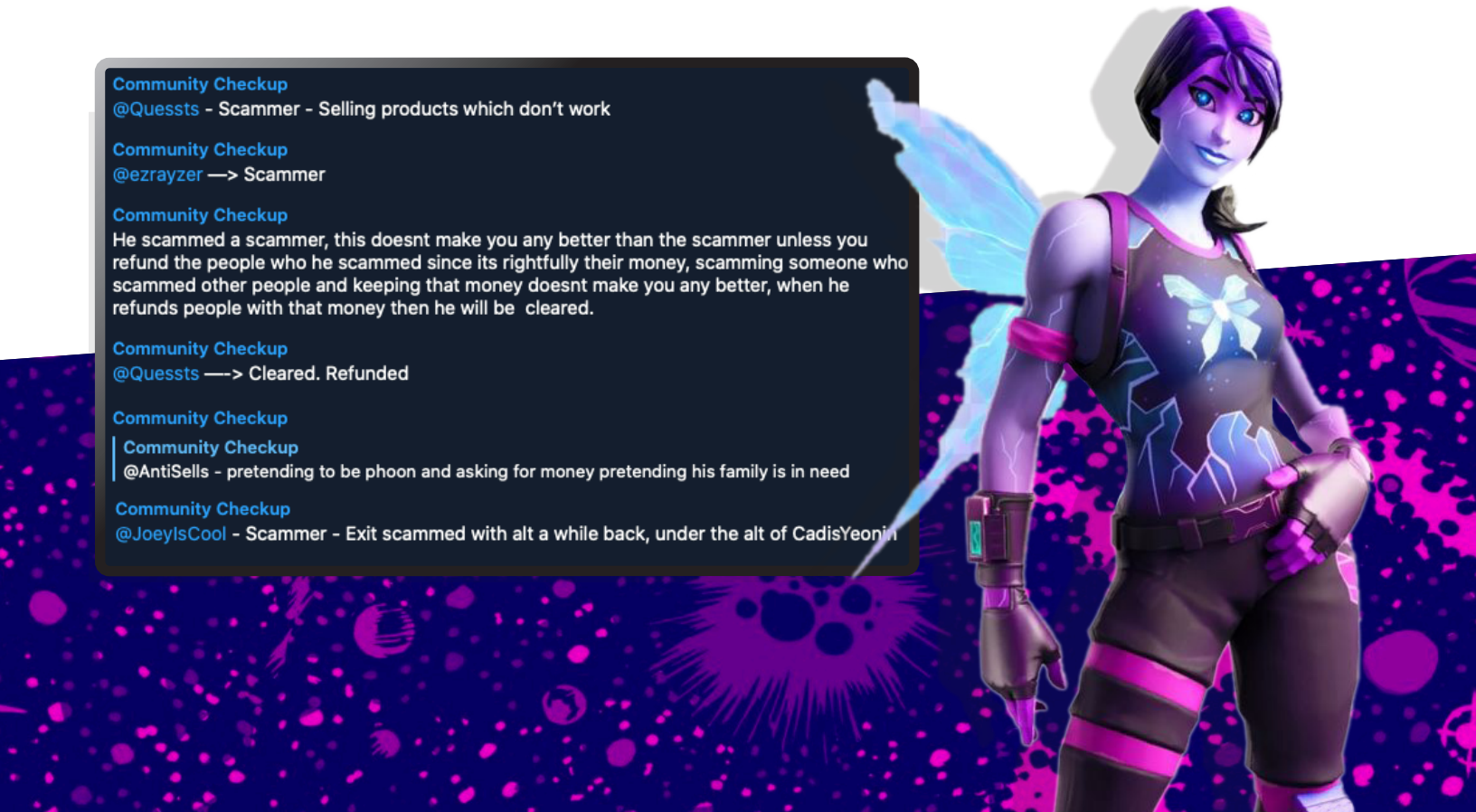
The Fortnite community maintains its own judicial system known as "CC", or "Community Checkup". This process is handled over the Telegram channel RealCommunityCheckup, which is also owned and operated by MrTayota.

The purpose of CC is to keep track of scammers, sellers, buyers who are breaking the community bylaws.

A group of five judges (CC members) preside over any disputes. A dispute can be opened by anyone, and are taken seriously by the community.

If a dispute is decided in the favor of the plaintiff, the defendant must compensate for damages in an amount seen as fitting by the presiding panel.

If the defendant refuses to comply with the ruling, he will be listed as a "scammer", and essentially blacklisted from the online community.



ESTIMATING THE VALUE OF THE HACKED GAMING ACCOUNT ECONOMY

AVERAGING ACTUAL SALES DATA

Our research into several black-markets auctions allowed us to document the large volume of Log sales occurring just in the Fortnite community. This was the beginning of how we calculated the overall size of the underground gaming market.

We then tallied auction sales for several high-end and low-end account sellers over a three month period. On the high end, sellers averaged $25,000 per week, or a roughly $1.2 million per year.

The lower-end sellers yielded an average of $5,000 per month, or $60,000 per year, yielding an overall average of $40,000 per month, or $480,000 per seller/per year in stolen account sales.

CALCULATING THE FORTNITE MARKET

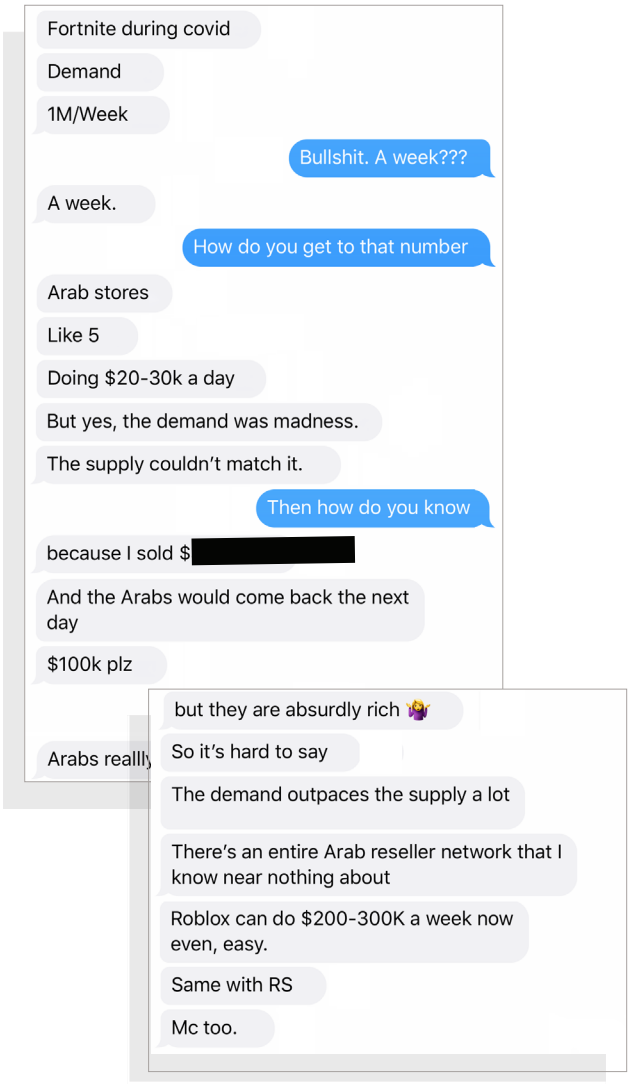
B2B Log Sales: 50 sellers * 480k = 24 million/yr
B2C Shops: (25k/day * 10 high-volume) * 365 = 91m/yr
30 low-end online shops at 10% of sales = 27m/yr
Conservative Fortnite account sales = 142m/yr

ROBLOX, RUNESCAPE, AND MINECRAFT

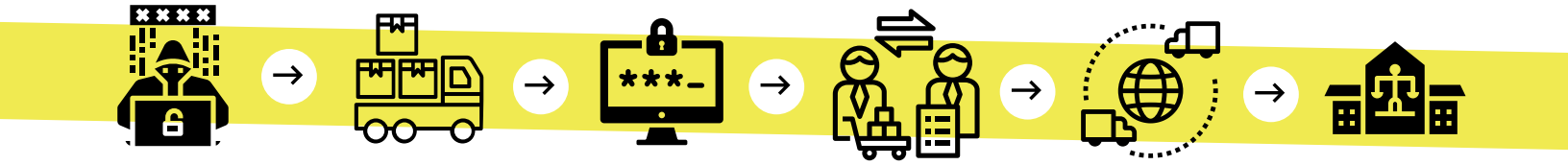
Roblox, Runescape, and Minecraft are three games that appear even more profitable. Adding a variation of +33%, or 186m per game, brings the total gross profits to $700m/yr for just four video games.

We can then confidently predict that an additional 30% revenue, or $300m/yr, can be generated by tallying the black-market sales for *every other video game* in existence, conservatively making the entire hacked video game market a billion dollar a year industry.

The following is a conversation with a high-end Log seller regarding the profitability of the market.



© 2020 Night Lion Security, LLC. • All rights reserved • www.nightlion.com



CONCLUSION

Hacked organizations rarely know where their data ends up, and the consumers of those hacked companies often don't even realize that their information has been compromised. Databases of consumer information are stolen and sold to private buyers, only to be repurposed and used to hack individual consumer accounts.

Hacked video game accounts are among the most profitable of all black-market accounts. The buying and selling of gaming accounts has evolved into billion dollar a year underground industry with its own fully functioning supply-chain.

The ongoing COVID-19 pandemic seems to be accelerating the demand for gaming acocunts as people continue to be out of work, giving them plenty of time to play video games.

To date, video game companies have not been successfully in slowing down this underground economy, with the higher-end hackers and sellers of these accounts continuing to make anywhere between six and seven figures per year in revenue.

ABOUT NIGHT LION SECURITY

Night Lion Security is a cyber security consulting and investigation firm specializing in IT audits, digital forensics, and advanced counterintelligence research. We help organizations uncover evidence active or past intrusions, fraud and other forms illegal or dishonest behavior.

Night Lion's CEO, Vinny Troia, is the author of "Hunting Cyber Criminals", an industry standard for digital investigative techniques.

www.nightlion.com

ABOUT DATA VIPER

Data Viper is a threat intelligence platform designed to provide organizations, investigators, and law enforcement with visibility into private hacker channels, pastes, forums, and to the largest collection of breached databases on the market. Data Viper was used exclusively in the research actors and topics discussed in this report.

www.dataviper.io

NIGHT LION
SECURITY