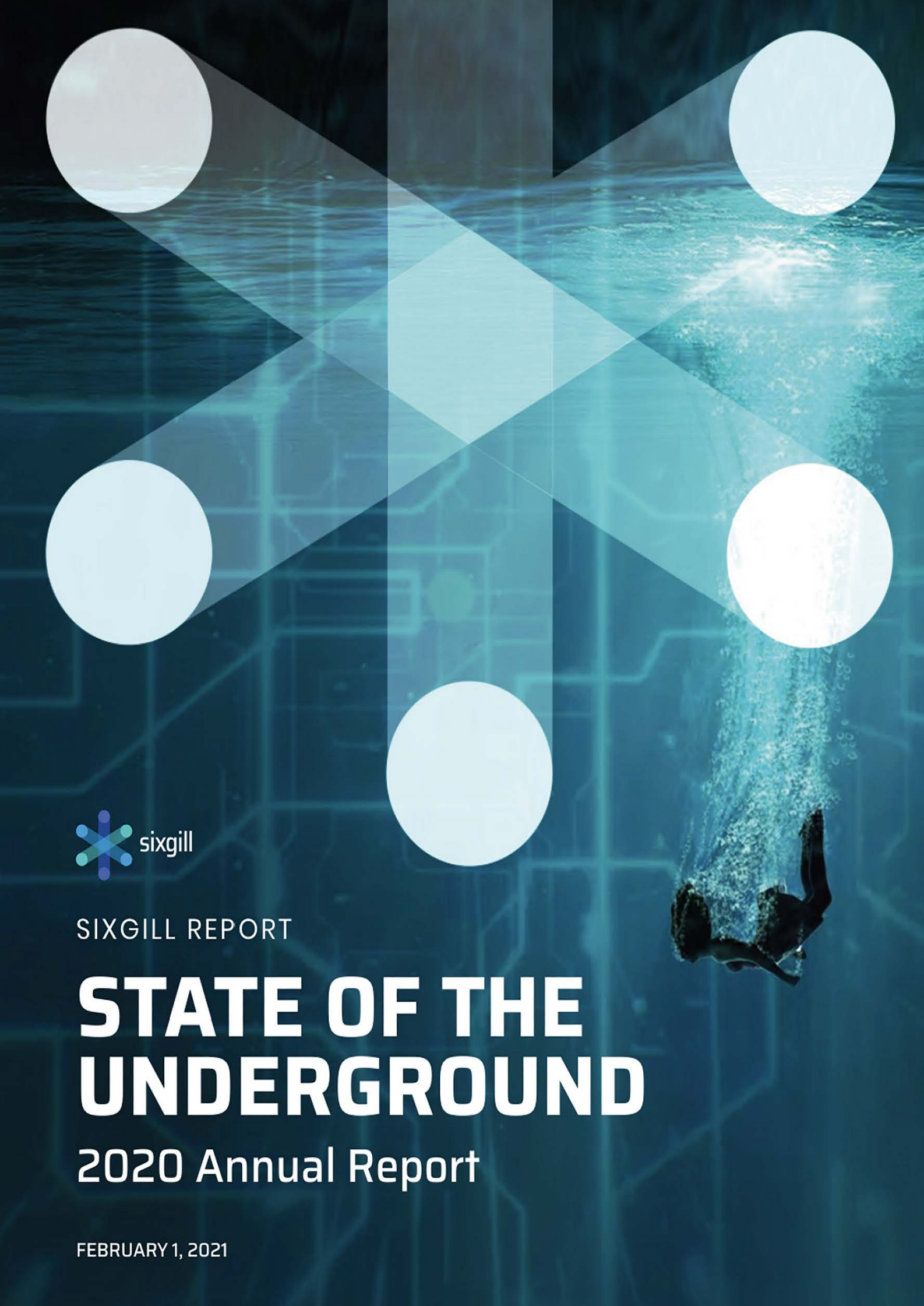


sixgill

SIXGILL REPORT

STATE OF THE UNDERGROUND

2020 Annual Report

FEBRUARY 1, 2021

INTRODUCTION

There is no need to say that 2020 was ground-shaking. The pandemic affected just about all aspects of life in ways that we are only starting to understand. It tremendously impacted the cyber underground as well.

Nearly all of Sixgill's research reports dealt directly or indirectly with the impact of COVID on the cyber underground. The months of the lockdowns brought an unprecedented spike in actors and posts in underground forums and platforms, peaking in April. In addition to the large volume of discourse about the virus itself ("are we all going to die?"), threat actors openly expressed that the lockdown, fear of contagion, remote-working chaos, and stimulus cash all presented opportunities for financial windfalls.

Because of this, criminal activity rose in all areas; our reports documented a major surge in hacked gaming store accounts, compromised RDP credentials, money laundering services, and narcotics. Due to their rise in importance, videoconferencing, remote learning, ecommerce, and hospitals became more appealing targets.

While COVID is the central theme of the year, we told other stories as well. We investigated hacking against education, social media, eSports, and IoT devices. We reviewed vishing, election discourse, and the underground market for counterfeits. And we set out to understand just how many actors are active in dark web forums to begin with.

Altogether, this is a comprehensive body of work that affects nearly every major vertical. These reports demonstrate just how big the world of the dark web really is, the diversity of its threats, and how, through usage of our portal and API, a researcher can really get to know what's out there.

In this, Sixgill's first annual report, we decided to take a bird's eye view on underground activity in 2020 and compare it with what we observed in 2019. Then, we will dare to make some predictions for 2021, and finally, we will conclude with a detailed summary of this year's threat reports.

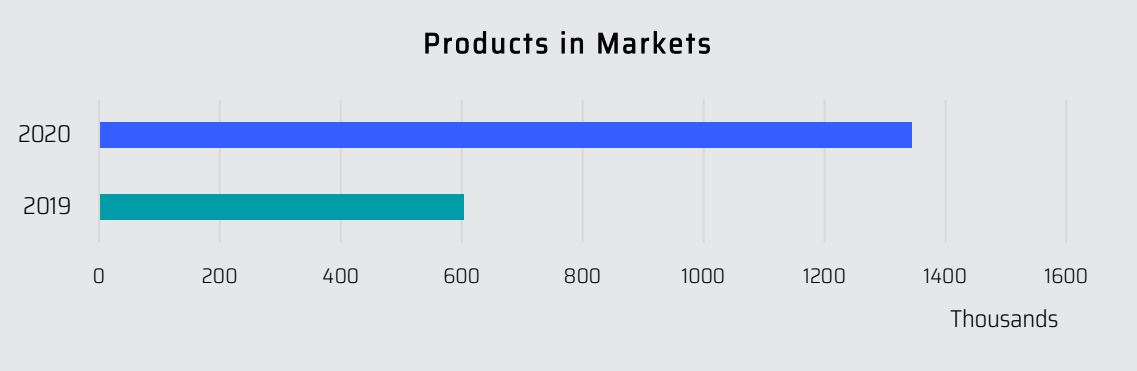
TABLE OF CONTENTS

2020 IN REVIEW[1]

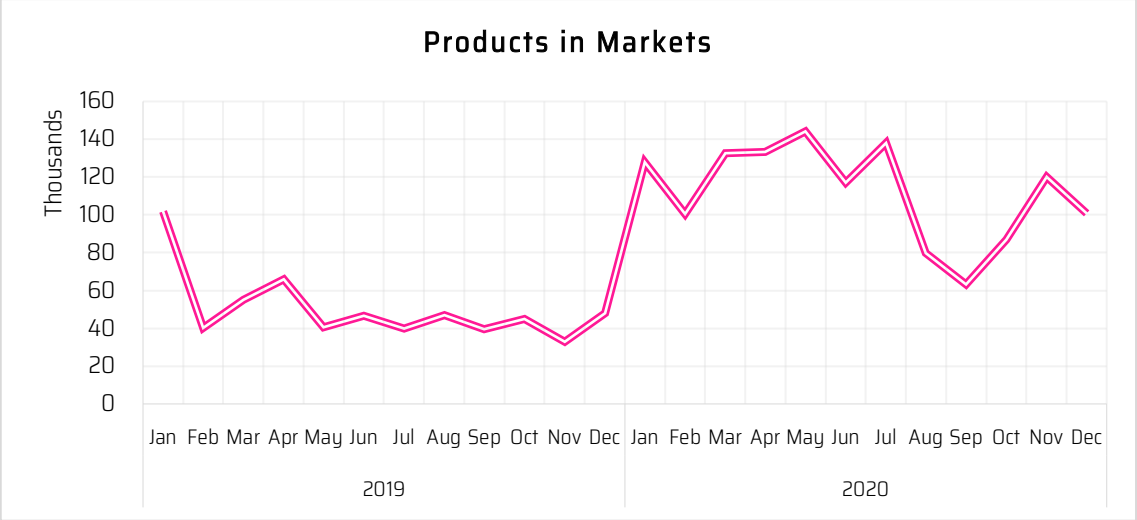
GENERAL UNDERGROUND ACTIVITY

Products sold in markets

We reviewed the number of non-digital products for sale in underground markets.[2] In 2020, there were 1,344,415 products posted for sale in underground markets, 223% of 2019's figure (602,441).



The largest monthly increase was between December 2019 to January 2020, and numbers remained strong until dipping in August.

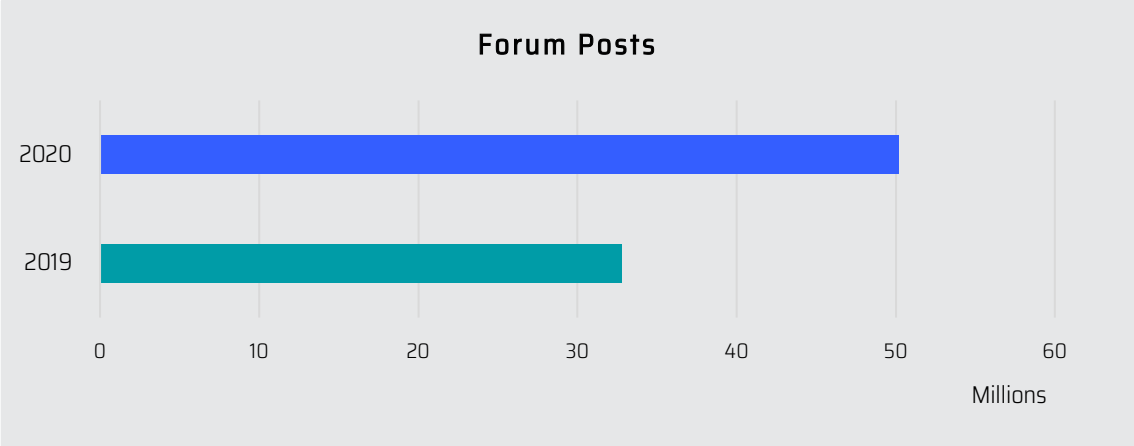


[1] We must note that Sixgill's collection has improved considerably over the last two years. While others talk about collecting millions of items, we collect by the billions. Therefore, some of the higher figures in the more recent data can be attributed to this (which we explicitly note when relevant). Even so, we believe that the trendlines reflect an accurate picture of patterns in the underground.

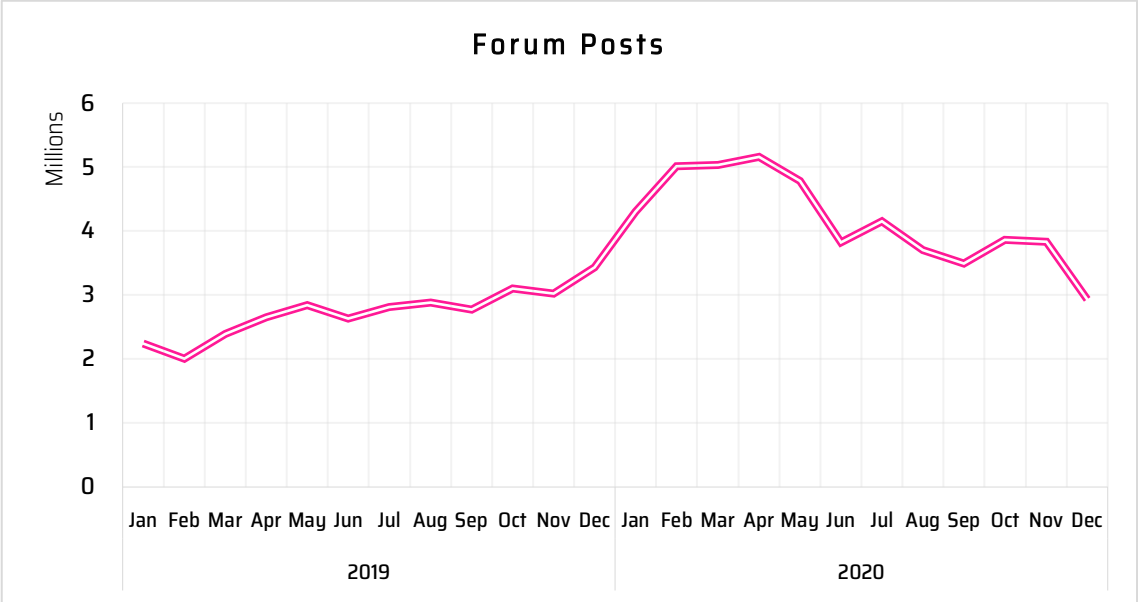
[2] We excluded digital products such as credit cards, compromised accounts, logs, RDPs, and bots.

Forum posts

Compared to its peers, Sixgill collects from 5x more dark web onion sites. This resulted in a collection of 50,156,373 forum posts and replies in 2020. This represents 153% of 2019's figure (32,794,811).

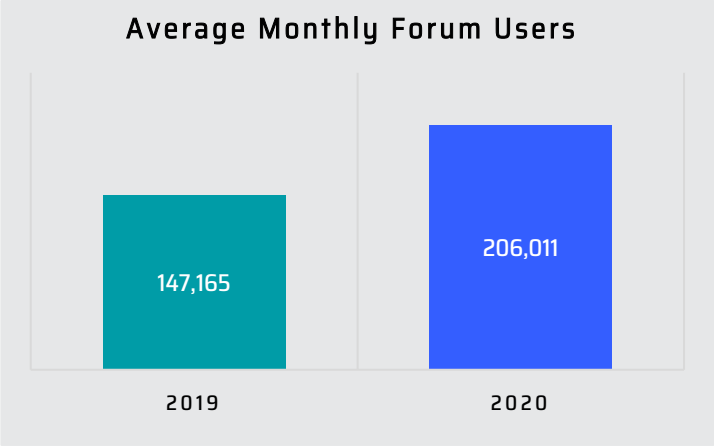


Forum posts peaked in April 2020, during which Sixgill collected 5,159,965 items. Some of this rise can be attributed to an increase of interest in cybercrime due to the effects and opportunities caused by the pandemic. Other rise in chatter can be attributed to boredom; actors were locked down and idle, so they resorted to the dark web for entertainment.

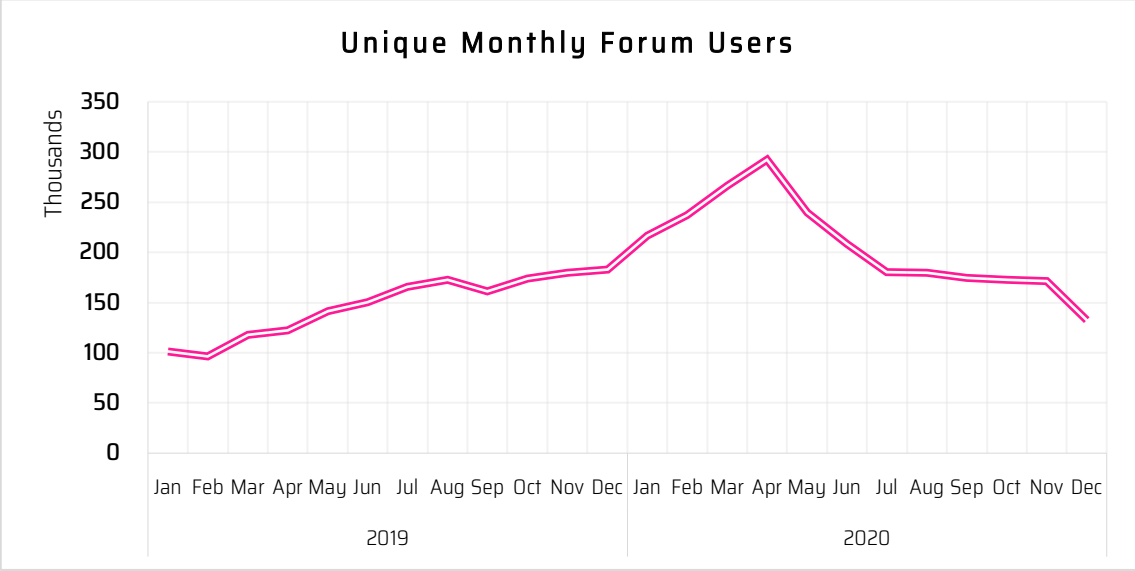


Forum users

We created a tracking index of the top 11 cybercrime forums (based on the largest volume of posts) over 2019-2020. In 2020, there were an average of 206,011 unique monthly users[3] within these forums. This was 140% of 2019's figure.



Taking a closer look at the monthly figures, we can note that the number of unique users trended upwards throughout 2019, but then spiked in spring 2020, in parallel with the COVID lockdowns. Indeed, the number of users peaked in April (292,359), the same month in which the total number of forum posts hit its high.

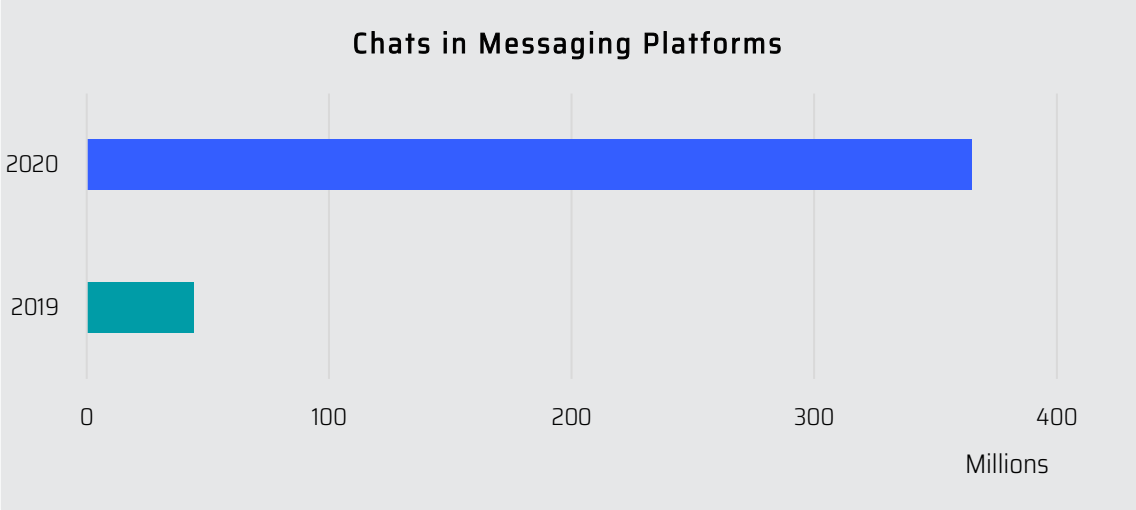


[3] Monthly users are defined as those that posted 1+ times per month.

It is also interesting that forum users reverted so much after the peak. This is a trend worth following: over the next year, will forum users from these established forums continue to rise over time, or will new users branch out to other forums and messaging platforms?

Messaging platforms

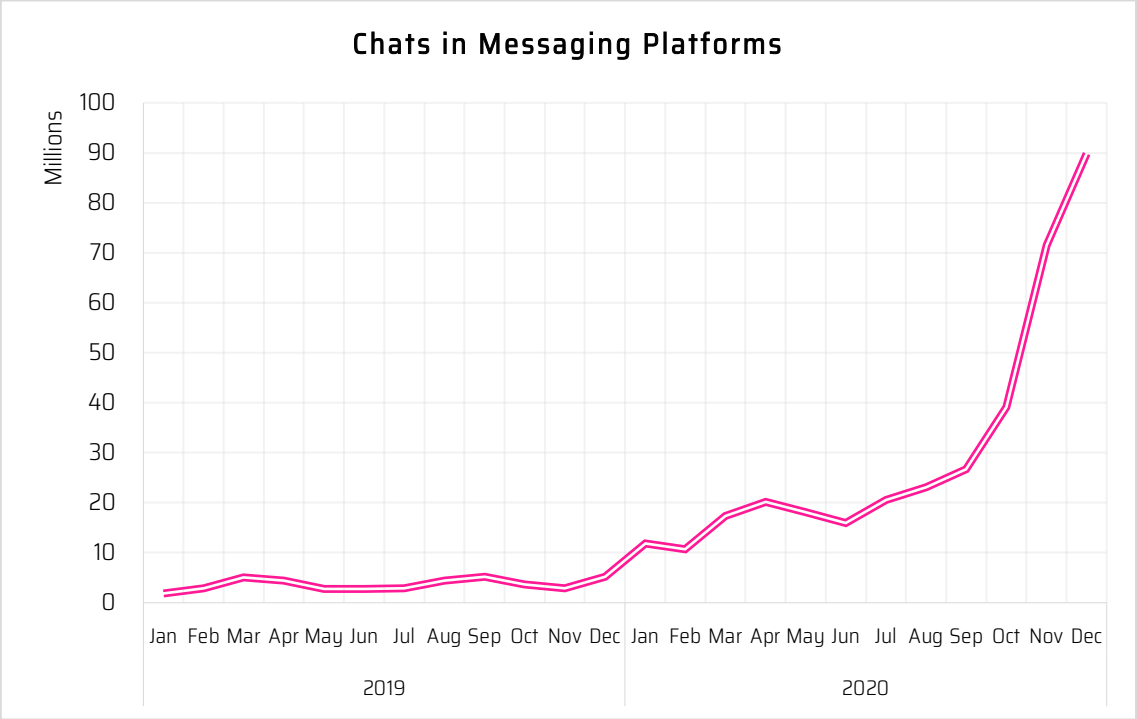
There was a vast difference between the number of collected items from messaging platforms in 2020 vs 2019. **In 2020, Sixgill collected 364,978,045 chats from messaging platforms, an increase of 730% of 2019's figure (43,986,244)**



The number of collected items from these sites has risen steadily since the beginning of 2019, and like forum posts and actors, also reached an all-time high in April 2020.

Collection from messaging platforms rose for two reasons. First, they are increasingly used as threat actors' preferred method of communication due to their relative ease-of-use and security.

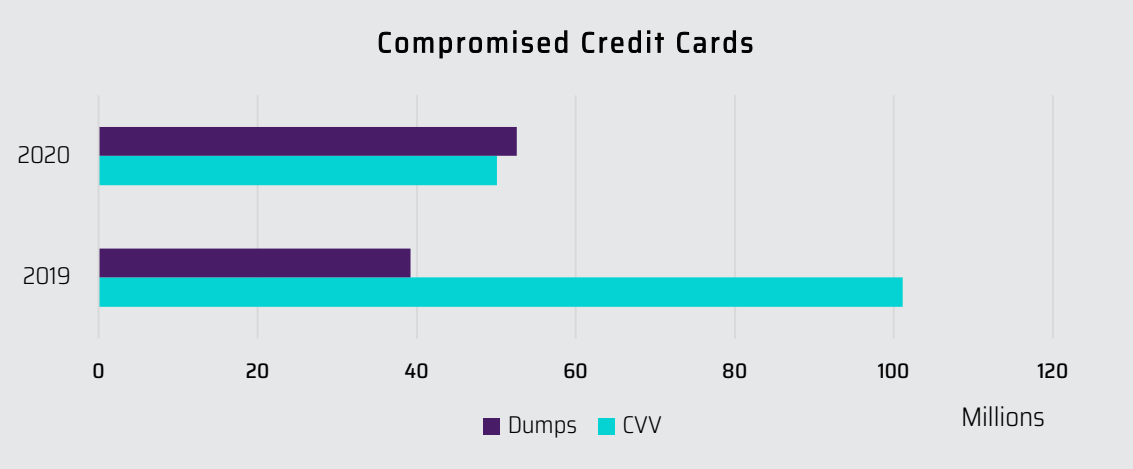
Second, in recognition of this, Sixgill has been vastly improving its collection methods from these platforms. This is especially apparent in the dramatic rise in the final months of 2020. Sixgill collects from 20x more Telegram groups than its industry peers.



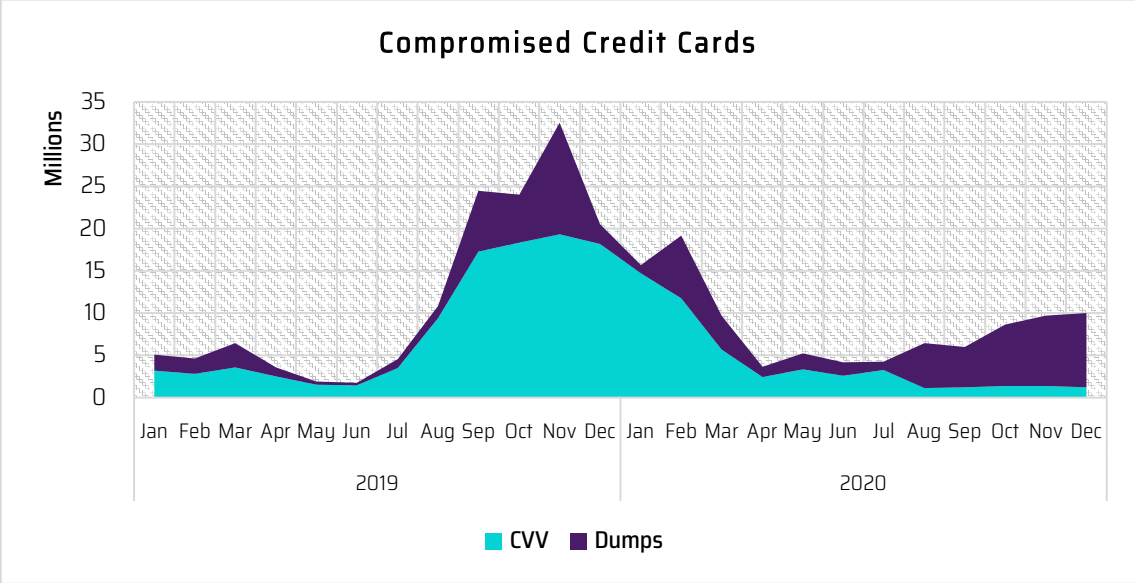
FINANCIAL FRAUD

Compromised credit cards

The number of compromised credit cards with CVV decreased by nearly 50% from 2019 (101,146,147) to 2020 (50,109,526). The number of dumps (cards without CVVs) rose to 134% (39,195,596 to 52,623,699).



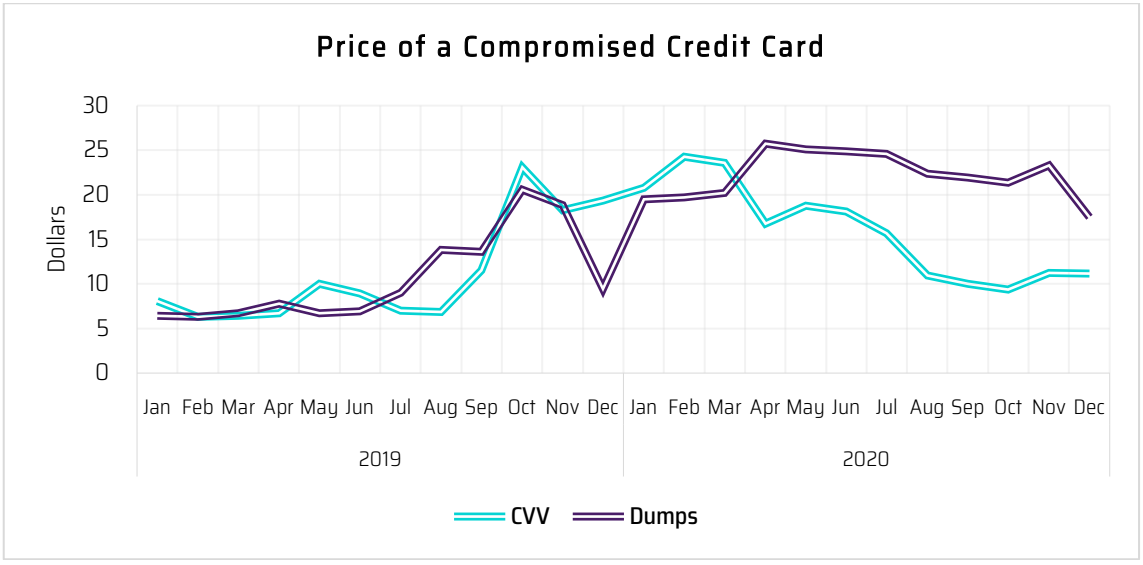
The number of compromised credit cards dropped precipitously in March 2020. This corresponds to when fourteen markets in our collection were shut down in a major operation by Russian law enforcement. The number of compromised credit cards has yet to recover from this operation, indicating that the gap left by the closures has not been filled.



Cards with CVV are generally compromised via malicious web apps (such as Magecart-style sniffers on ecommerce sites), while dumps are usually harvested by a compromised point-of-sale terminal. While dumps were low in April-July, when many brick-and-mortar stores were closed, broader reopening could have enabled more opportunity for PoS compromise. Furthermore, it is unclear to us why the number of CVVs dropped so much relative to dumps, especially during a period in which ecommerce rose. Perhaps this indicates a reduction of successful web app attacks in 2020.

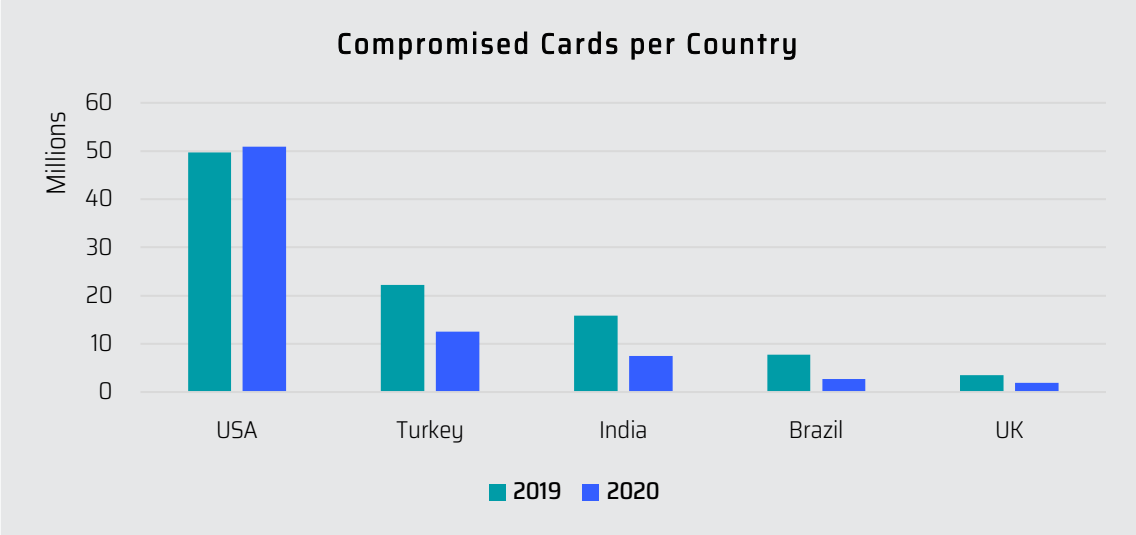
Prices

The average selling price of a card with CVV in 2020 was $15.98, and of a dump, $22.18. Both prices represent an increase from 2019's rates of $11.04 for a CVV and $10.51 for a dump. Certainly, it appears that the prices for dumps rose in March after the major drop in supply. The price of CVVs, however, puzzlingly continued to drop even when supply was so low.



Cards per country

The leading five nationalities of compromised credit cards in 2020 were: USA (57.2% of all cards), Turkey (14.1%), India (8.4%), Brazil (3%), and the UK (2.2%). The quantities of compromised cards for all countries decreased from 2019 to 2020, except for the US, which rose by 2.5%.

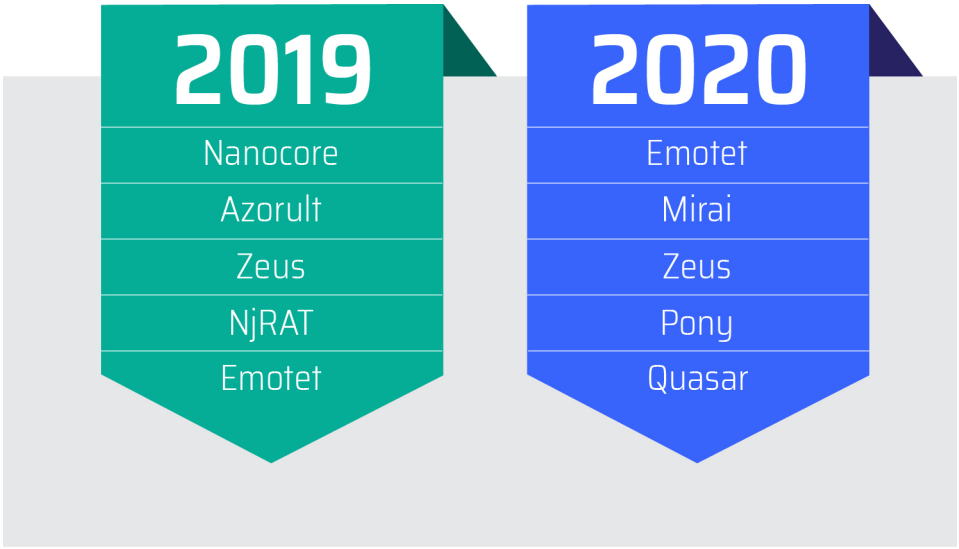


Russian cards stayed near the bottom of the country list, in 128th place, between Eswatini and Jamaica. These numbers continue to reinforce the understanding that Russian threat actors operate with relative impunity if they avoid targeting Russian and CIS citizens.

MALWARE

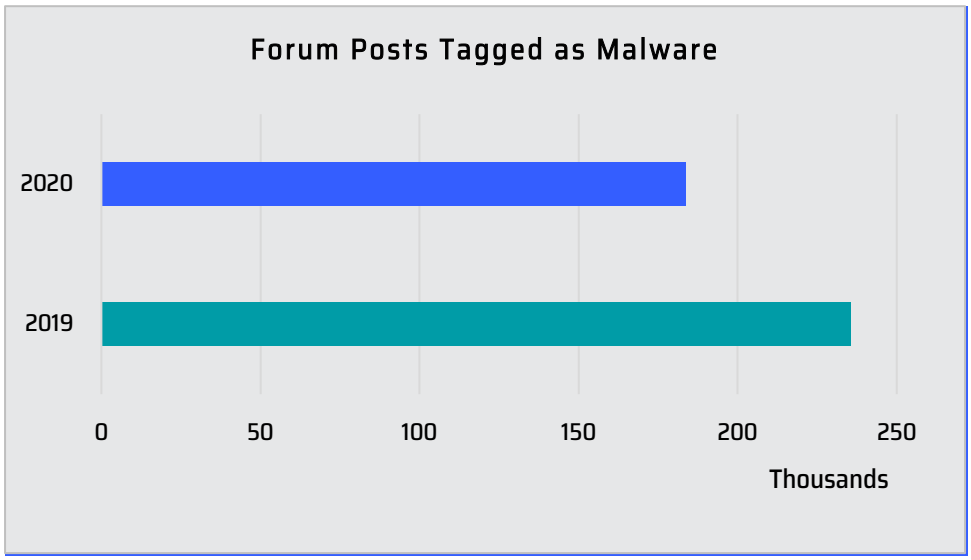
Top malware

The following lists represent the top-five malware families mentioned on forums and paste sites each year:



Malware in forums

Posts tagged as *malware*[4] in underground forums reduced by 22% from 2019 to 2020.



[4] Posts are tagged as malware if they include the name of a malware family (ex Emotet) or a malware type (ex. ransomware).

VULNERABILITIES AND EXPLOITS

We ranked the vulnerabilities with the highest average monthly DVE score.[5]

CVE-2020-1895, a vulnerability targeting Instagram, maxed out at a score of 10 in both October and November. It was followed by CVE-2020-0796 ("SMBGhost") and CVE-2020-14882 (vulnerability in the Oracle WebLogic Server), which averaged at 9.99 in April and December, respectively.

2020

CVE	Affected Product	DVE Score	Month
CVE-2020-1895	Instagram for Android	10	October
CVE-2020-1895	Instagram for Android	10	November
CVE-2020-0796	Windows SMBv3	9.998711	April
CVE-2020-14882	Oracle WebLogic Server	9.99871	December
CVE-2020-4006	VMware Workspace	9.996452	December
CVE-2020-1938	Apache Tomcat	9.991245	March
CVE-2020-16898	Windows TCP/IP handling	9.985821	November
CVE-2020-3452	Cisco ASA and FTD	9.971648	August
CVE-2020-1472	Netlogon	9.96231	October
CVE-2020-14882	Oracle WebLogic Server	9.958647	November

In comparison, in 2019 the top-rated CVEs were CVE-2019-5736 (Docker container escape) and CVE-2018-20250 (WinRAR exploit).

[5] Sixgill's Dynamic Vulnerability Exploit (DVE) Score is derived from automated AI analysis of underground discourse on deep and dark web forums and is combined with intelligence from other sources, such as code repositories and technical know-how. The resulting score adds a much-needed dimension of probability, and ultimately helps the user understand how likely the CVE will be exploited in the near future.

2019

CVE	Affected Product	DVE Score	Month
CVE-2019-5736	Docker	10	March
CVE-2018-20250	WinRAR	10	April
CVE-2018-20250	WinRAR	9.999737	March
CVE-2019-0708	Windows RDS	9.999538	June
CVE-2019-11510	Pulse Secure PCS	9.999299	September
CVE-2019-15107	Webmin	9.992903	September
CVE-2018-20250	WinRAR	9.992057	May
CVE-2019-0841	Windows (AppXSVC)	9.991829	June
CVE-2019-0841	Windows (AppXSVC)	9.991262	May
CVE-2019-1181	Windows RDS	9.99	September

LOOKING AHEAD TO 2021

If there is ever a time in which we ought to be too humble to make a prediction about next year, it's this year. But we'll try. Looking ahead to 2021, we anticipate that the cybercrime underground will continue to grow.

It will grow in terms of activity and participation. The ongoing pandemic and economic crisis will motivate additional users to seek illicit financial gain. Many may turn to crime and fraud out of personal financial difficulties. Others, because the opportunities of pandemic cybercrime are too lucrative to refuse.

Opportunities for cybercrime will also continue to grow. Driven by social distancing, more of our daily routines are becoming digitized, including work, socialization, shopping, banking, and healthcare. Each one engenders an array of options for dark web actors to exploit, whether through hacking or social engineering. And as more actors meet and collaborate on the underground, attackers can grow their schemes in complexity and scope.

The underground will also continue to branch out from the traditional onion sites to messaging platforms. Especially in the wake of very effective law enforcement measures against credit card markets, actors may seek to set up shop on more bulletproof platforms.

Finally, we believe that the cyber underground could become the central arena for radical political discourse. The recent crackdown of hate speech and incitement by social media giants may drive the nexus of this discourse from Twitter to dark web forums and messaging platforms such as Telegram.

APPENDIX: SIXGILL THREAT REPORTS

In case you missed any of our threat reports, below is a summary of our 2020 reports and their corresponding links on our website.

Underground Financial Fraud H2 2019 (January 27): During the last six months of 2019 (H2-2019), 76,230,127 compromised cards were offered for sale by threat actors in illegal credit card markets monitored by Sixgill, compared to 23,319,709 cards offered in H1-2019.

Caller ID Spoofing in Vishing Attacks (February 13): In a vishing (voice phishing) attack, fraudsters use caller ID spoofing for identity fraud and provide PII or other information to impersonate an account holder. The use of caller ID spoofing has increased, in part due to the ease of using VoIP technology. References to call spoofing on the underground have increased by 2X from 2018 to 2019.

Virus in The Wild: Coronavirus Discourse on the Dark Web (March 1): The novel coronavirus has captivated the attention of worldwide media, social media, and internet discourse. Many that want to discuss it on secure channels have turned to secure messaging apps and deep and dark web forums.

Coronavirus Discourse Update (March 24): Mentions of coronavirus in the dark web have fallen into four major categories: general discussions, fraud (to gain government stimulus), profiteering and scamming (from selling PPE and even "vaccines"), and social engineering and malware.

Zooming in on Zoom: Discourse on Video-Conferencing Applications in the Underground (April 16): Especially during the pandemic, Zoom and other videoconferencing applications are now becoming key targets for hackers and trolls, damaging their brand integrity and putting their users at risk.

Overstimulating: CARES Act Fraud on The Dark Web (April 30): Threat actors sensed an opportunity when the U.S. government announced it would deposit checks into the accounts of millions of Americans. On the dark web, we found that there was a rise in stolen identity packages (fullz) and a nearly 90% spike in identity-related terms (tax ID,

paystub, Social Security Numbers, and Form 1040) in the immediate days prior to the disbursement of the payments.

The Corona High: Covid-19's Boost to the Underground Illicit Drug Economy (May 13): The coronavirus pandemic has caused nearly wholesale damage to the economy, across industries and geographies. But there is one industry where business is booming - dark web drug sales, which have experienced a growth spurt of 495% between December and April.

In it to Win it! Esports on the Underground: Hacks, Exploits & Fraud (May 31): The gaming industry has now evolved into a massive professional sport and broadcasting genre mainly through the streaming platform Twitch. This report analyzes Twitch fraud while looking at several of the top competitive games streamed on the platform, along with the cheats that help gamers gain an edge.

When the Underground Comes A-Knocking: Hacks & Exploits of Smart Home Devices (June 15): As employees working from home implement a variety of connected devices, the potential attack surface becomes larger, with more endpoints attempting to reach company networks.

Remote Desktop Pandemic (August 13): Remote Desktop Protocol (RDP) is a tool that allows a user to remotely connect to and control another device over a network or the internet. On the dark web, there are markets that sell access to compromised RDP servers, which can be used by attackers to deploy many types of attacks, such as ransomware. The number of RDPs for sale spiked during the coronavirus lockdown, presumably as businesses scrambled to work remotely.

Underground Financial Fraud: H1- 2020 (August 20): Despite the extraordinary events of 2020, the digital underground continued business as usual. During this period, 45,130,117 compromised cards were offered for sale in credit card markets monitored by Sixgill in the underground.

Gaming the System: Overview of Dark Web Threats Against the Gaming Industry (September 2): The deep and dark web is popular with gamers because most of their users belong to the same demographic - young and computer-savvy. The dark web hosts

a tremendous amount of content that violates terms of service of games and challenges their integrity (cheats and hacking tools), as well as items that are outright illegal, such as breached accounts, gift card generators, and services for DDoS attacks against game servers and for doxing rival gamers.

Corona Cash: Payment Platforms on the Dark Web During Covid-19 (September 15): Payment platforms and apps are increasingly mentioned on the deep and dark web within three contexts: payment for goods and services, fraud (money laundering), and account takeover. Though mentions of payment platforms were on the rise prior to COVID-19, they spiked tremendously during lockdowns. The rise is staggering: from February until the peak in May, the total number of mentions rose 262%.

#NO FILTER: Social Media Hacking from the Underground (October 6): In a time of "social distancing", people around the world have relied on social media platforms to maintain relationships. This report examines two types of motivations for abuse of these platforms: economic and personal.

Another Brick in the Firewall: Dark Web Threats to Education (October 20): Dark web chatter around education consists of multiple topics, including data leaks, ransomware, services, compromised or fraudulent accounts, and fraudulent use of eLearning platforms. Since 2017, Sixgill has observed an upwards trend in mentions of education-related discourse.

Dark Web Politics: A Guide to 2020 Election Chatter on the Dark Web (November 2): With the imminent US presidential elections gripping both American and global discourse, we explored how Decision 2020 is playing out on the deep and dark web. We reviewed discourse about the candidates, about hot-button political issues, and hacktivism motivated by US politics.

Not What the Doctor Ordered: Threats to Healthcare on the Underground (November 10): Malicious discourse on the underground related to the healthcare industry generally includes leaked data, the selling of access to healthcare systems that can be used for attacks, and exploits targeting medical devices. This report investigates these aspects of

the healthcare industry on the underground and delves into why the industry is frequently targeted and why it remains vulnerable.

Terms and Conditions Apply: Refund Fraud on the Dark Web (November 24): Refunding, which involves defrauding eCommerce vendors by claiming undeserved refunds, exploits both couriers and retailers, seizing on technical loopholes in delivery and customer support services while leveraging social engineering. Return fraud has risen in popularity as consumers have turned to online shopping amid the pandemic. They will almost certainly spike as retailers rush to meet the crush of post-holiday demand.

Forumology: Dynamics of Dark Web Forums (December 15): This report analyzes five underground forums and investigates their counts of unique actors and their activity. It found that forums grow exponentially in accordance with the technology adoption lifecycle model, that the top 20% of actors contribute about three quarters of the posts, and that during the COVID lockdowns, there was a staggering 44% increase in unique monthly users when compared with January 2020.