The State of the Underground

2021 ANNUAL REPORT

Cybersixgill Report

cybersixgill

Introduction

The headline story of 2021 was ransomware. While also a hot topic in 2020, in 2021, ransomware was even bigger, solidifying its standing as the highest-impact cyberthreat as countless organizations worldwide were disrupted and even debilitated by attacks. The damages caused by ransomware attacks are as devastating as its victims are diverse - affecting organizations large and small across many different verticals, including software vendors, schools, governments, broadcasters, a major meat processing plant, and a critical US oil pipeline.

Indeed, only seven months into the year, the FBI reported that it had already "received 2,084 ransomware complaints with over $16.8M in losses, a 62 percent increase in reporting and 20 percent increase in reported losses compared to the same time frame in 2020."

The cybercriminal underground provides the perfect environment for the development, expansion and proliferation of ransomware attacks and their extortionist aftermaths. First, it provides a platform for the planning and execution of the attacks, where ransomware groups can advertise calls on cybercriminal forums for affiliates (operational partners) to support their operations, and where operators can purchase access to a vast array of compromised systems in illicit initial access markets, which provide the first entry point from which to launch their attacks. Secondly, after executing the attack and infiltrating their victims' systems, ransomware groups use their dark web-hosted dedicated leak sites (DLS) to extort victims, threatening to publicly share their stolen confidential data should they refuse to comply with the hackers' ransom demands.

Cybersixgill's sources demonstrate a tremendous expansion in the underground ransomware economy during 2021. Throughout the year, access to 4,286,150 compromised endpoints was sold on the underground, a whopping 457% of 2020's total. Evidently, vendors on access markets increased their supply capacity to match the exploding demand. Similarly, **we collected 3,264 posts on ransomware groups' dedicated leak sites in 2021, more than double the total collected in 2020** (1,509).

In addition to the dramatic rise in ransomware, analysis of the underground activity throughout 2021 produced another major insight of value: while the total number of posts in forums and on messaging channels rose considerably (45% and 338%, respectively), the number of posts and participating actors decreased significantly in the ten most popular underground forums. This seems to suggest **that the underground has become increasingly decentralized.** Accordingly, analysts can no longer rely on the top forums as the lone source of their intel. In order to gain a comprehensive understanding of underground developments and compile an accurate intelligence picture, analysts must expand their investigative search to include as many sources as possible.

In this annual report, we provide a comprehensive overview of underground activity throughout 2021, evaluating emerging trends and developments by comparing these metrics with those observed in 2020.

With these insights in hand, we will dare to predict the expected trends and forecasts for 2022.

TABLE OF CONTENTS

General Underground Activity[1]

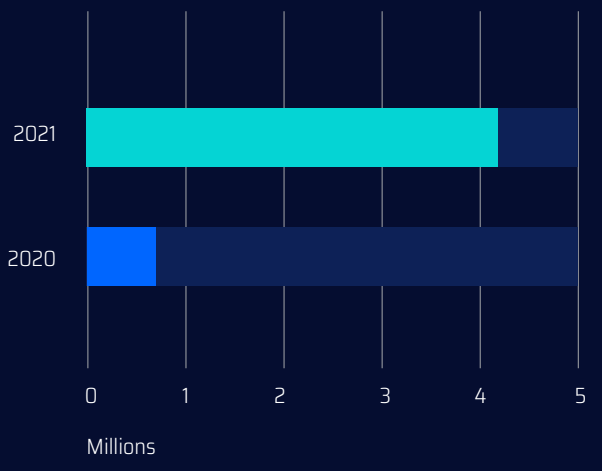
Initial Access Sold in Markets

In the underground economy, the services of initial access brokers are in high demand for any aspiring cybercriminal. For a fee, various markets sell access to compromised endpoints or via remote protocols such as RDP, allowing other cybercriminals to buy the first step into their targets' networks.

For as little as several dollars, attackers can gain a foothold into the targeted system, and from this beachhead they can deploy ransomware, siphon system resources, harvest confidential information, and assume control of logged-in financial accounts. Considering how lucrative ransomware has become for attackers, it is unsurprising that these initial access markets are popular with ransomware operators, who no longer need to invest resources in gaining entry.

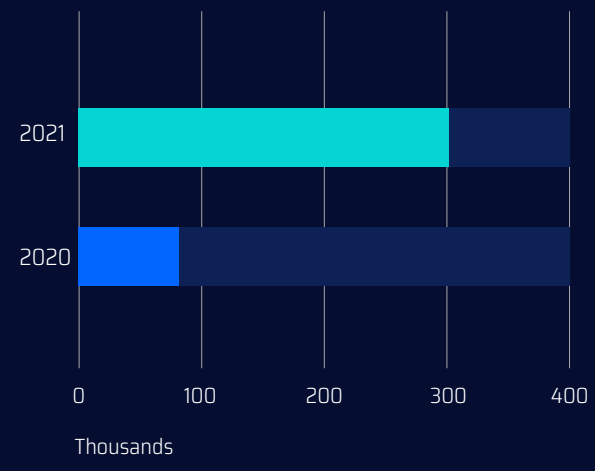
Inventory in these markets is booming. In 2021, access to 4,286,150 compromised endpoints was sold on the underground, a massive 457% of 2020's figure (937,430). Similarly, in 2021, a total of 307,478 compromised RDP connections were also sold, 481% of 2020's figure (63,883).

Compromised Endpoints



Compromised RDP Connections

Figure 1



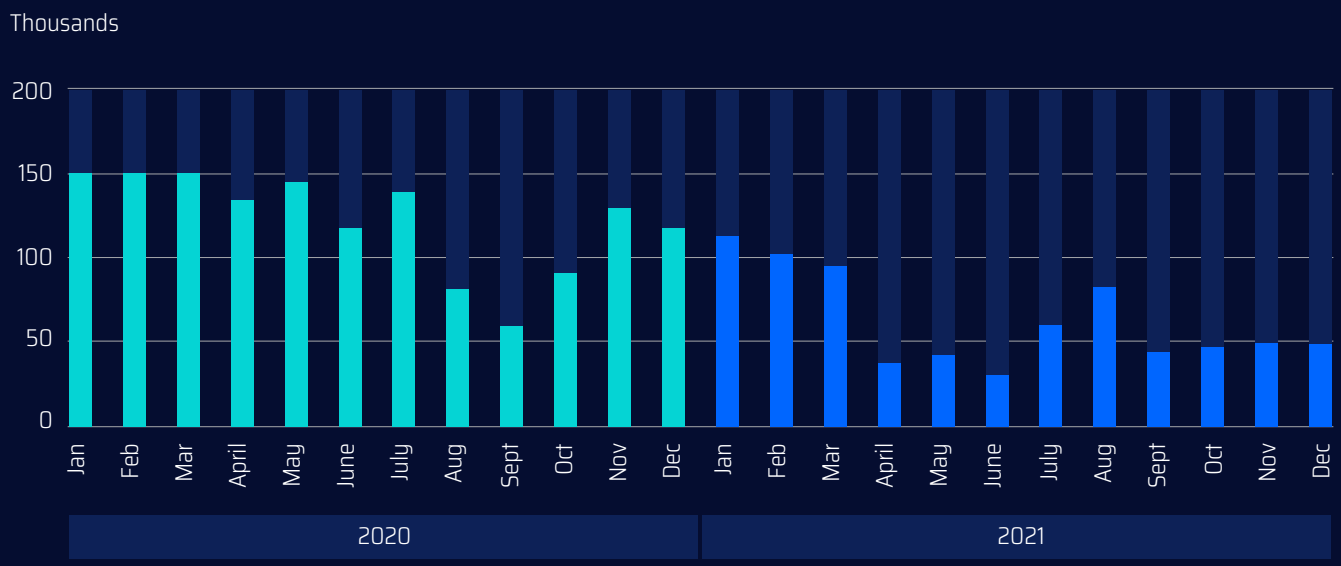
[1] We must note that Cybersixgill's collection capacities continue to improve. While others talk about collecting millions of items, we collect by the billions. Therefore, some of the higher figures in the more recently collected data during 2021 could be attributed to advancements in our collection mechanisms (which we explicitly note when relevant). Even so, we believe that the trendlines reflect an accurate picture of patterns in the underground.

Physical Products Sold in Markets

These virtual underground markets do not stock only digital items, and in fact offer a variety of illicit physical products for sale.[2] In 2021, Cybersixgill identified a total of 756,783 physical products listed for sale in underground markets, a decrease of 45% from 2020's total (1,381,714).

Physical Product Sold in Markets

Figure 2



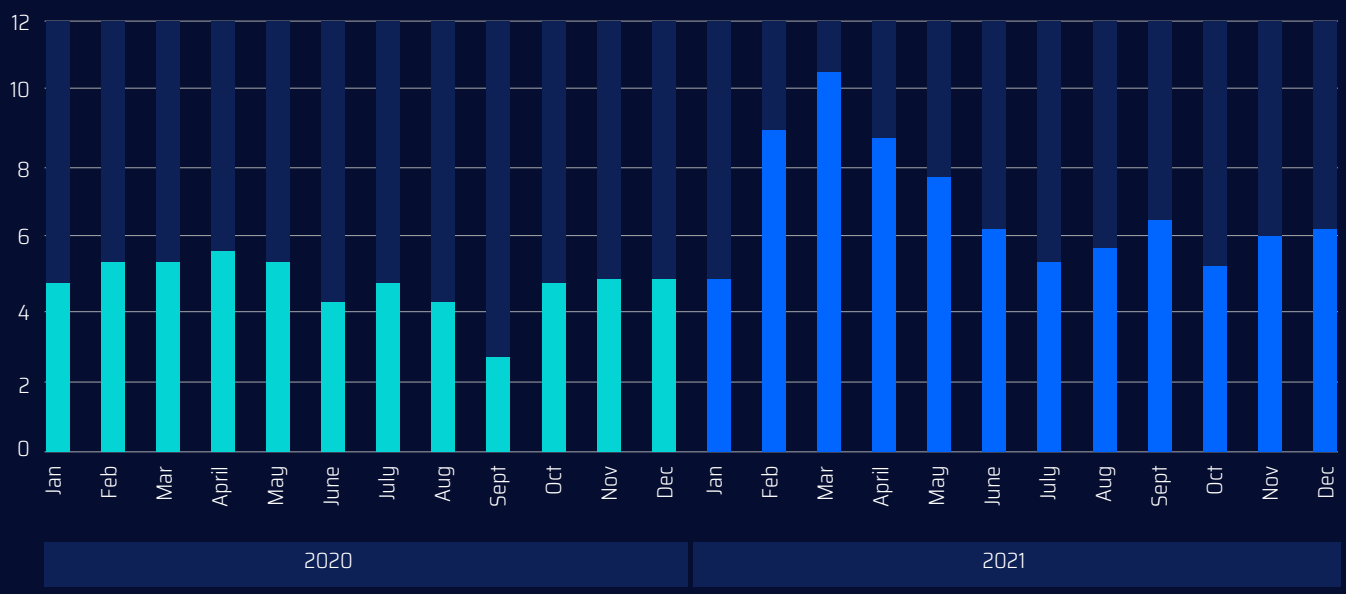
Forum Posts

Cybersixgill's intelligence extraction capacities from the dark web vastly outpace those of our industry peers, with collection from more dark web onion sites than any of our competitors – five times over. These advanced collection mechanisms extracted a total of 82,665,214 forum posts and replies in 2021. This represents 145% of 2020's figure (56,929,383).

[2] This figure excludes digital products such as credit cards, compromised accounts, endpoints, RDPs. etc.

Total Forum Posts

Figure 3



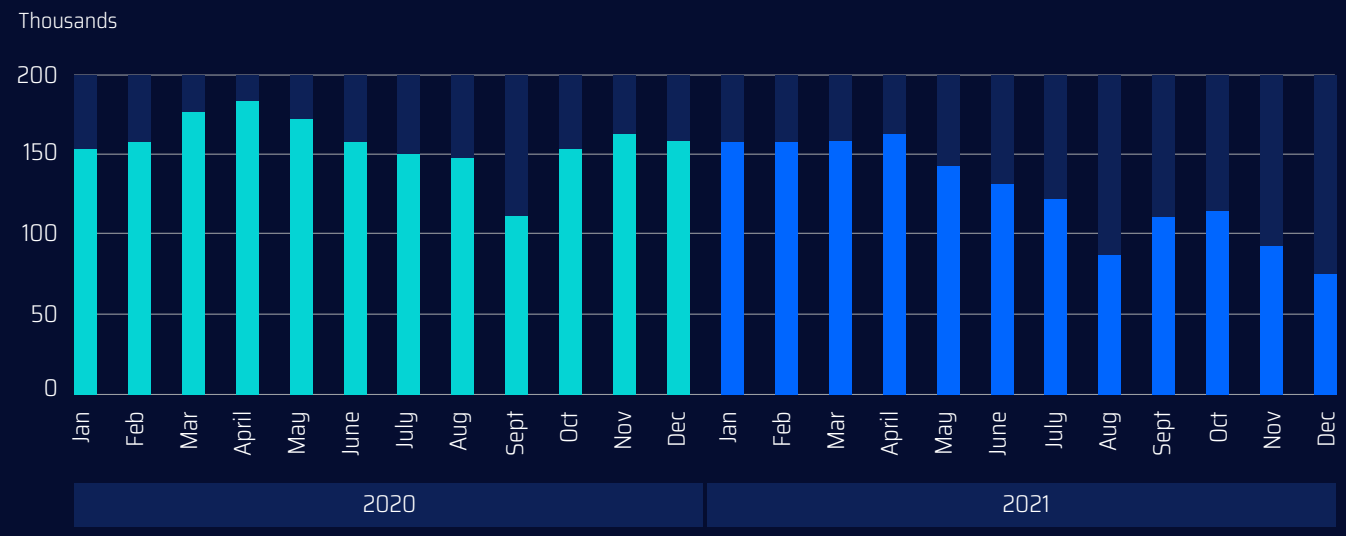
In 2020, forum posts peaked in March, an apparent result of the initial wave of COVID-19 lockdowns across the world. Those highs from 2020 were quickly surpassed in the early months of 2021.

Forum Users

We created a tracking index of the top 10 cybercrime forums over 2020-2021. In 2021, we identified an average of 125,405 unique monthly users[3] operating within these forums – a decrease by 20% than the number of actors operating in these same forums in 2020 (156,934).

Unique Monthly Forum Users

Figure 4



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

This 20% decline is significant, marking a shift in the underground threat landscape. Further investigation revealed that, while overall activity in all dark web forums increased by 45% from 2020 to 2021, within these ten most popular and populated forums, activity dropped by nearly a third, from 14,515,322 in 2020 to 10,029,149 in 2021. This steep reduction in posts and participation within the leading cybercriminal forums suggests that the underground is becoming more decentralized. While overall activity is rising, it is increasingly distributed.

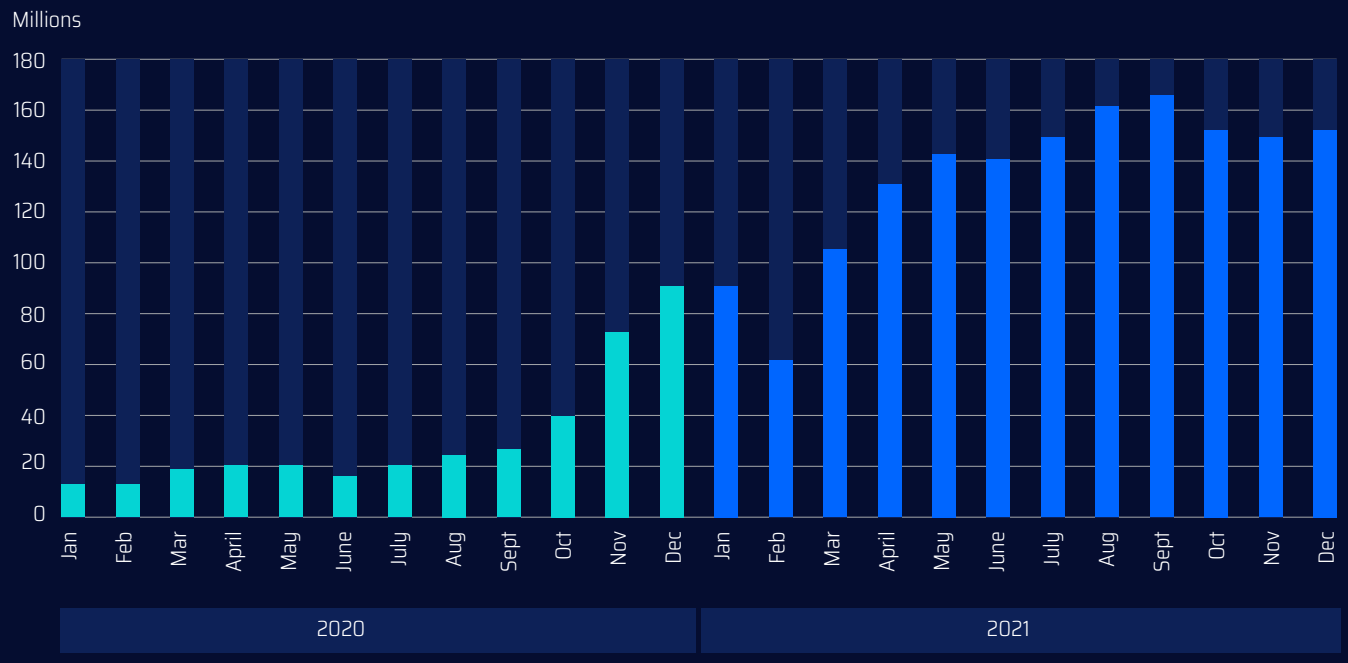
One possible explanation of this phenomenon is that some of the more senior actors in the larger forums became wary of the overwhelming presence of n00bs (novice actors) within their forum ranks. As a result, some forums implemented more selective admission processes, requiring payment, a referral, or a demonstration of hacking abilities as a prerequisite for admittance.

Messaging Platforms

There was an enormous difference between the total number of collected items from messaging platforms in 2021 vs 2020. In 2021, Cybersixgill collected 1,597,788,764 chats from several messaging platforms (including Telegram), an escalation by 338% of 2020's figure (364,720,150).

Posts from Messaging Platforms

Figure 5



This rise in the total number of collected items from messaging platforms can be attributed to two primary factors. First, messaging platforms have been increasingly embraced by cybercriminals, replacing other platforms as threat actors' preferred method of communication by virtue of their relative ease-of-use and security.

Second, in recognition of this cybercriminal migration to messaging platforms, Cybersixgill has been vastly improving its collection methods from these sources, collecting from 20x more Telegram groups than its industry peers.

FINANCIAL FRAUD

Compromised Credit Cards

The number of compromised credit cards advertised for sale on the underground dropped to 41,875,374[4] in 2021, a 59% decrease from the total in 2020 (102,212,103).

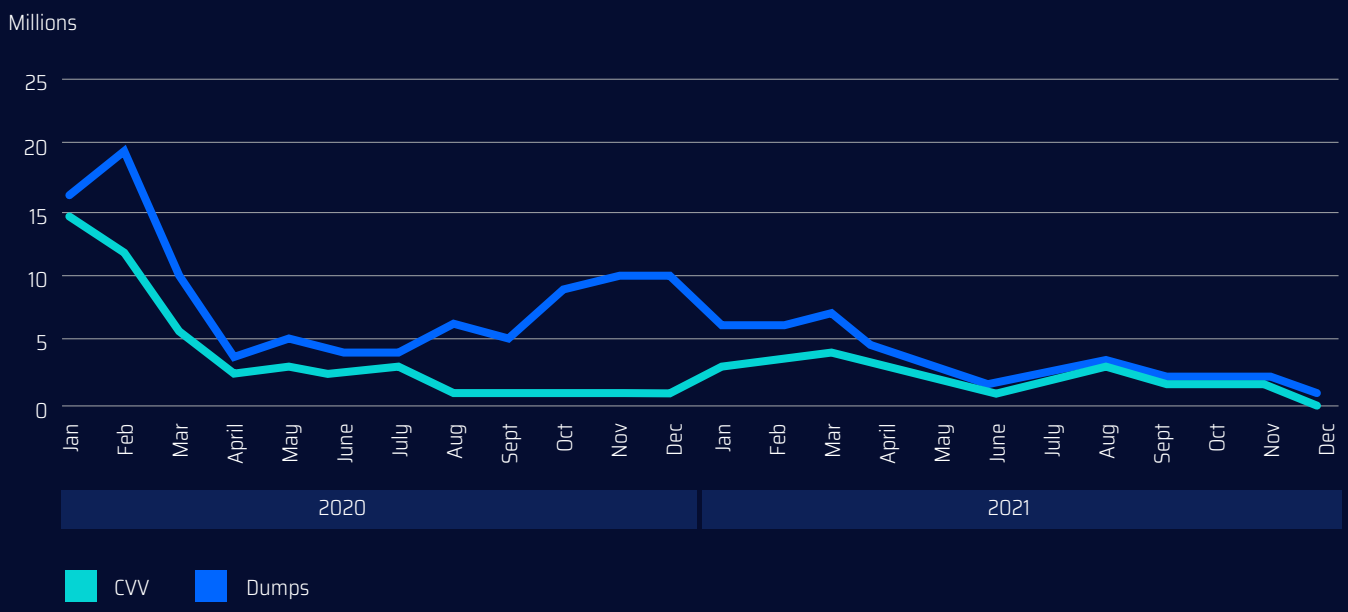
On underground credit card markets, there are two predominant forms of compromised cards offered for sale - those categorized as dumps, and those including CVV/CVV2 information. Cards from dumps contain the data included in the card's magnetic strip, and are generally procured using a compromised point-of-sale terminal. CVV/CVV2 information (the 3-4 digit code on the back of the card), on the other hand, is only transmitted in online or phone purchases, and therefore compromised CVV cards are generally procured through hacked e-commerce sites.

Of this total, the number of cards sold in CVV[5] format reduced by 45% (27,588,325 from 50,109,526), while cards sold as dumps[6] dropped by 73% (14,287,049 from 52,102,577).

[4] Note that these numbers are preliminary, as updates in our collection methodology are likely to cause them to be revised upwards.
[5] CVV cards are generally compromised via malicious web apps (such as Magecart-style sniffers on ecommerce sites)
[6] Dumps are usually harvested by a compromised point-of-sale terminal.

Compromised Credit Cards

Figure 6



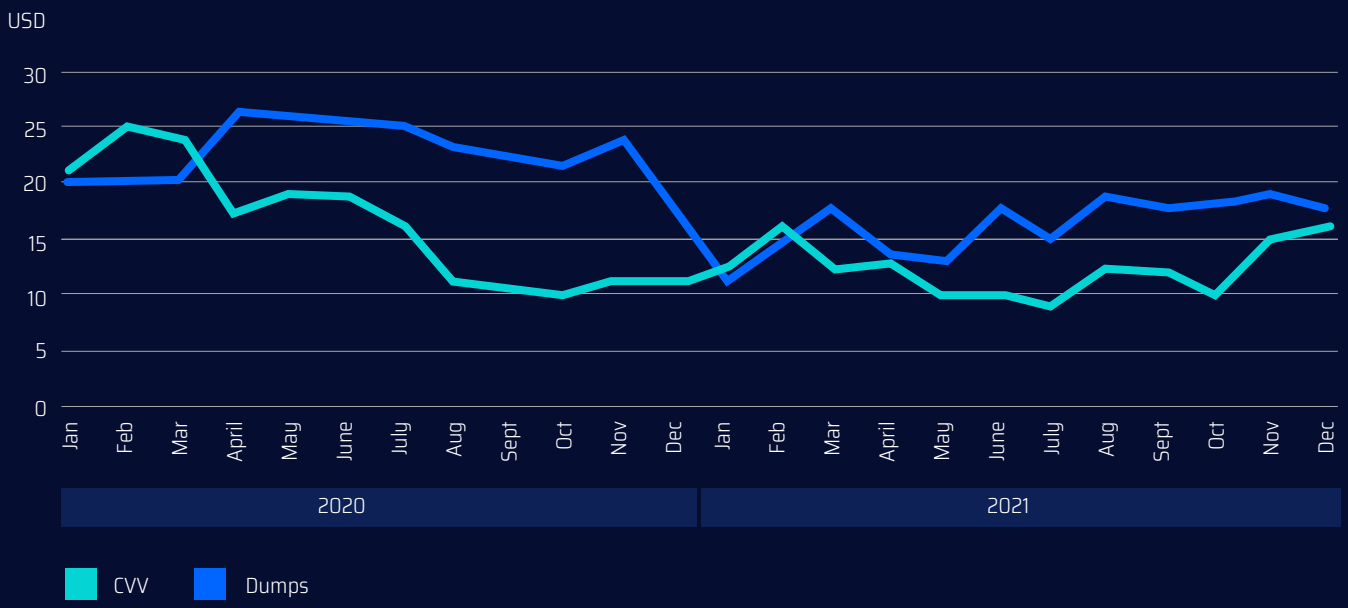
In last year's report, we noted an aberration in the usual distribution between cards sold in CVV format and those sold as dumps, whereby the quantity of dumps sold exceeded CVVs in the second half of 2020. This was especially surprising due to the global gravitation towards ecommerce purchases as a result of pandemic social distancing mandates. However, this trend appears to have corrected itself in 2021, with CVVs once against constituting the predominant format for compromised cards sold on the underground.

Prices of Compromised Cards

The average selling price for compromised credit cards in CVV format during 2021 was $11.87, while the price of dumps averaged at $15.86. Both figures represent a decrease from 2020's rates of $15.89 for a CVV card and $22.18 for a dump.

Prices of Compromised Credit Cards

Figure 7



Cards Per Country

Of the compromised credit cards sold in the underground during 2021, five countries dominated the global distribution in 2021: USA (57% of all cards), Mexico (5.9%), UK (4.1%), Australia (4%), and Brazil (3.7%).

This is a slight rearrangement of the top-5 list of 2020, which comprised the US, Turkey, India, Brazil, and the UK. Meanwhile, while US-issued cards remain the most popular target of credit card compromise, their total reduced by 61% (34.3 million) in 2021, just slightly greater than the overall drop of compromised cards globally (59%). It is notable that the rise and fall of US-issued card dominance in the underground credit card market remains in-line with broader trends, as this is not always the case. Between 2019 to 2020 for example, while there was a slump in the global total for compromised cards, the number of US-issued cards sold between those years rose by 2.5%.

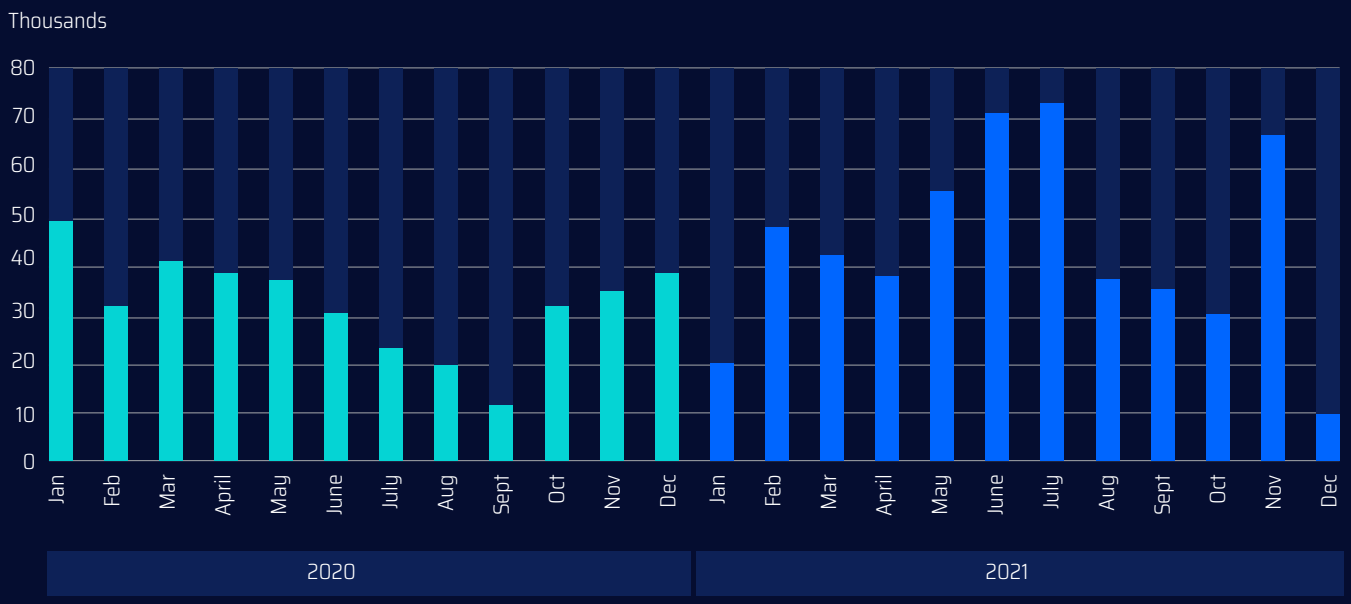
MALWARE AND RANSOMWARE

Malware in Forums

Forum posts dealing with malware[7] increased in 2021 to 527,180, increasing by 36% from 2020's figure.

Malware-Related Posts in Forums

Figure 8

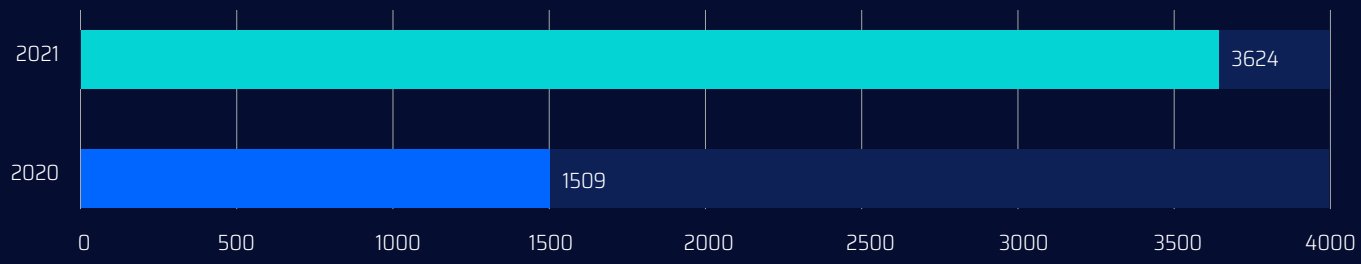


Ransomware Posts on Leak Sites

Cybersixgill collected a total of 3,264 posts[8] on Dedicated Leak Sites affiliated with various ransomware groups throughout 2021, representing an escalation of 116% from 2020's figure (1,509). This signifies a substantial increase in the total number of ransomware attacks.

Posts on Ransomware Dedicated Leak Sites: Year- to-Year

Figure 9



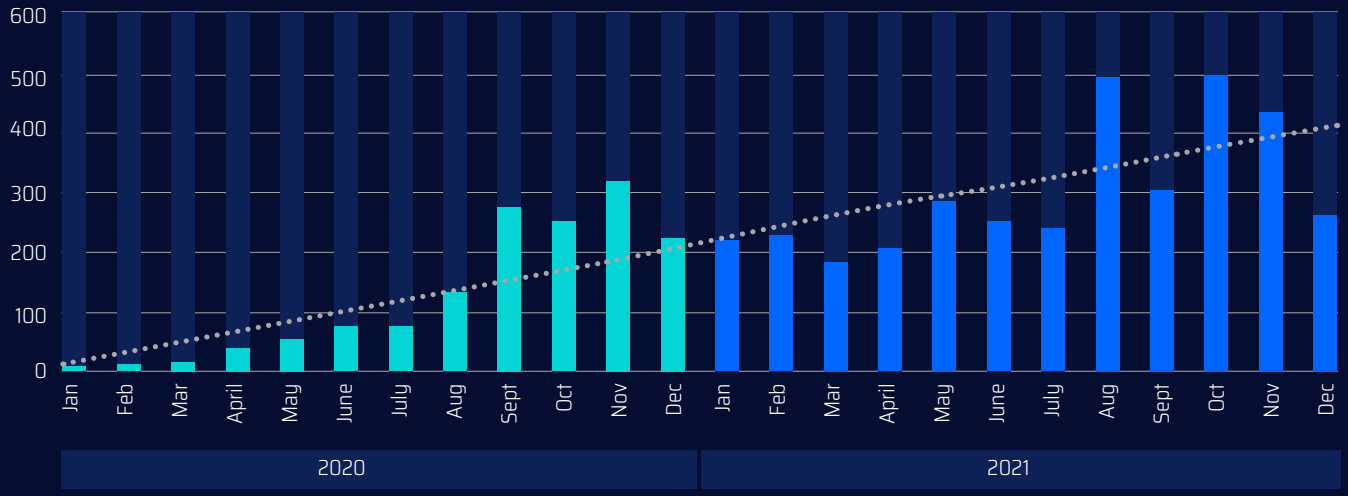
[7] Posts are tagged as malware if they include the name of a malware family (ex. Emotet) or a malware type (ex. ransomware).

[8] Not every post represents a unique ransomware attack, as occasionally groups will post about the same attack several times. However, this number can be seen as a rough stand-

Month-to-month, these attacks followed a steady upward trend.

Posts on Ransomware Dedicated Leak Sites: Month-to-Month

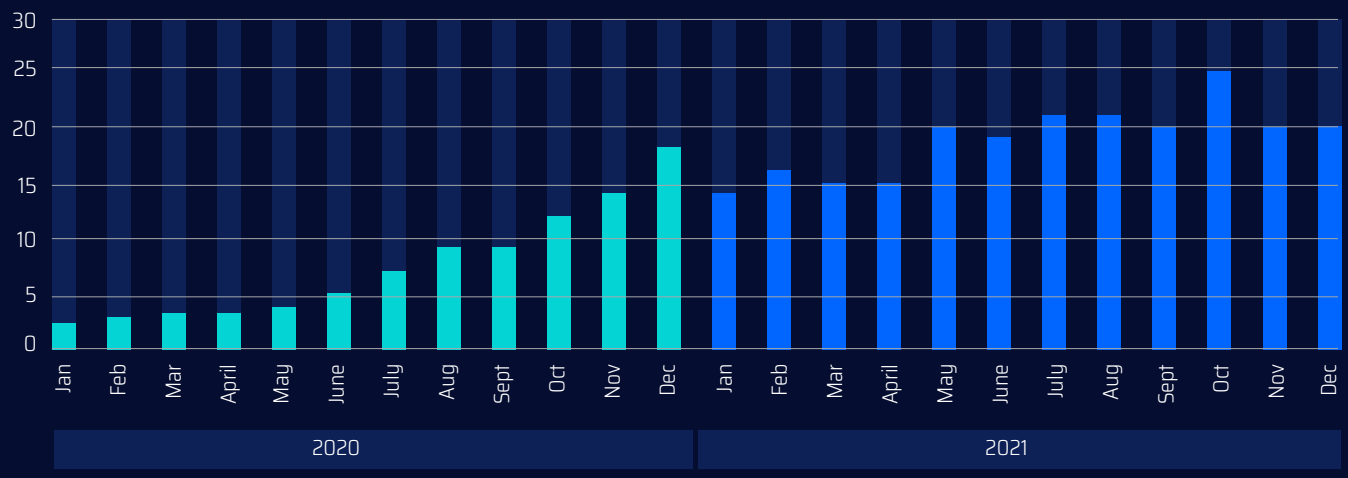
Figure 10



Furthermore, the number of unique ransomware groups active each month has been trending upwards, peaking at 25 in October 2021.

Active Ransomware Groups

Figure 11



The increase in the total number of active ransomware groups follows the known cybercrime pattern of **diffusion**. The diffusion process is initiated when an advanced threat actor formulates an innovative new method of attack, developing novel TTPs (tactics, techniques, and procedures) for its execution. Once this new attack chain proves to be successful, other threat actors will seek to emulate it, clamoring to achieve a similar victory for themselves. This drives demand, which cybercriminal vendors are happy to satisfy, providing the tools and services needed to launch this new type of attack. Thus, what was once an advanced and innovative attack is diffused and commoditized, easily accessed and executed by less-sophisticated threat actors.

VULNERABILITIES AND EXPLOITS

You can be sure that a vulnerability constitutes a serious threat when it is designated with a recognizable name. Several vulnerabilities attained such a designation during 2021, most notably, ProxyLogin in April, PrintNightmare in October, and Apache Log4J in December. Unsurprisingly, each one received a perfect DVE Score[9] of 10/10.

However, threat actors don't limit their attention to named CVEs. Various other unnamed vulnerabilities attained significant DVE Score ranking throughout the year, as demonstrated in this table reflecting the highest-ranking vulnerability for each month of the year. Consistently, every month, at least one vulnerability scored a 10.

All of these vulnerabilities share one core commonality: all relate to exploitable flaws in some of the market's most popular and widely-used products and platforms. Undoubtedly, the more potential targets of an exploit, the more actors are interested in using it.

Monthly Vulnerability Score

Figure 12

MONTH	CVE	AFFECTED PRODUCT	DVE SCORE
January	CVE-2018-13379	Fortinet FortiGate SSL VPN	10
February	CVE-2021-3156	Cisco products	10
March	CVE-2021-21972	VMware vSphere Client	10
April	CVE-2021-26855 (ProxyLogin)	Microsoft Exchange Server	10
May	CVE-2021-28310	Microsoft Windows	10
June	CVE-2021-3493	Ubuntu Linux	10
July	CVE-2021-21551	Dell BIOS	10
August	CVE-2021-33909	Linux Kernel	10
September	CVE-2021-36934 (HiveNightmare)	Microsoft Windows	10
October	CVE-2021-1675 (PrintNightmare	Microsoft Windows	10
November	CVE-2021-30860	Apple iOS	10
December	CVE-2021-44228	Apache Log4J	10

[9] Cybersixgill's Dynamic Vulnerability Exploit (DVE) Score is derived from automated AI analysis of underground discourse on deep and dark web forums, correlated with 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.

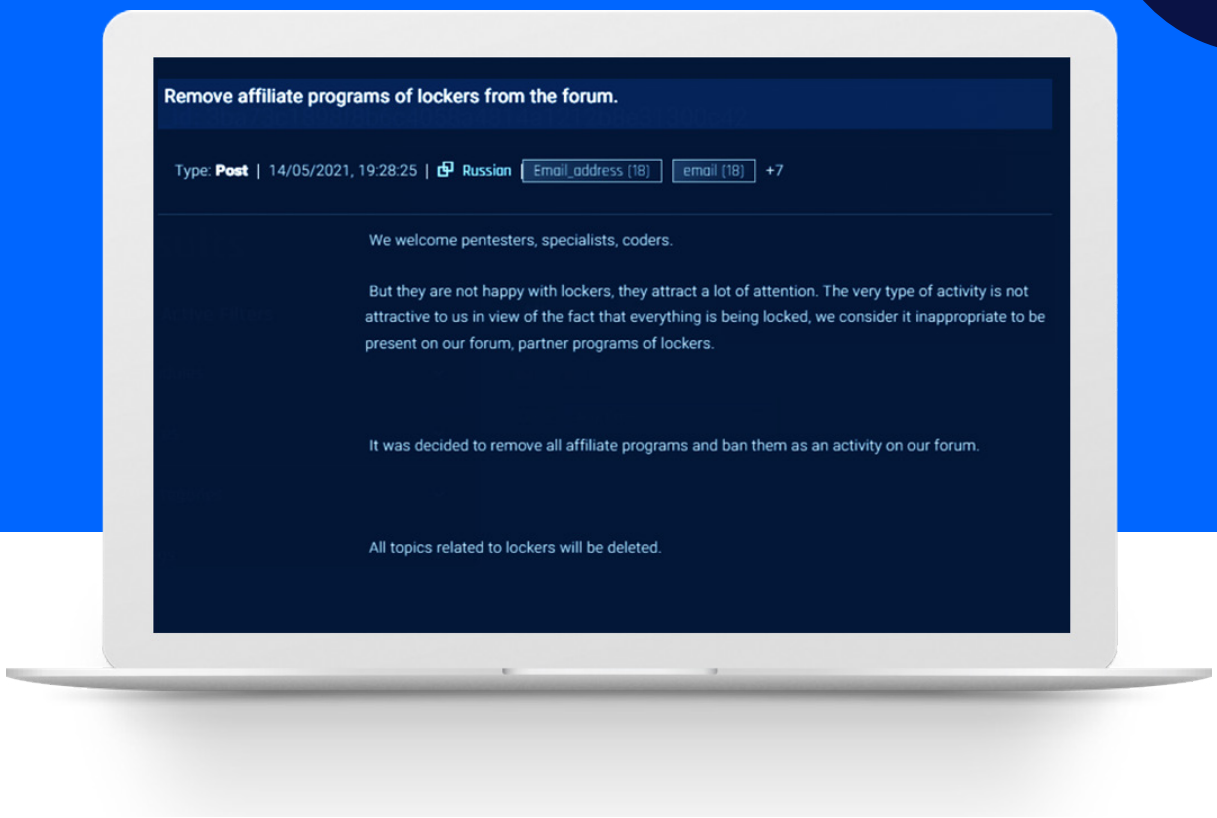
LOOKING AHEAD TO 2022

The threat of ransomware has grown significantly throughout 2021, exceeding the already record-breaking havoc that it caused in 2020. While many may extrapolate that this clear upward trajectory implies a continued rise in ransomware in 2022, such a projection is an oversimplification, and in our mind, not entirely accurate.

Throughout 2021, two significant developments within the underground threat landscape generated difficult headwinds for large ransomware groups. First, in mid-May, following the highly disruptive Colonial Pipeline attack, multiple cybercriminal underground forums implemented a strict ransomware ban – prohibiting any and all activity advertising ransomware or affiliated partnership programs. In banning ransomware, the cybercriminal community expressed their distaste for the widespread destructive impact caused by attacks against "softer" targets, such as critical infrastructure, hospitals, and schools.

Furthermore, forum administrators expressed that they did not welcome the increased public, media, and law enforcement scrutiny of their forums as a result of the ransomware activities taking place across their platforms. By designating them as persona non grata, underground forums cut ransomware operators off from their main platform for recruitment, partnerships, and promotion of their activities.

Second, in addition to the backlash from the cybercriminal community, the Colonial Oil Pipeline attack also inspired the US Federal government to implement broad and ambitious changes to national cybersecurity protocols, in attempt to curb the rapid acceleration of the ransomware threat. In May 2021, President Biden issued the "Executive Order on Improving the Nation's Cybersecurity," committing to lead the global effort to address the threat of ransomware to economic and national security. As part of this effort, President Biden declared that ransomware no longer be addressed through the prevailing cybercrime lens, and instead would be treated as a direct threat to national and global security.



Additionally, in July, the US Department of Justice established a dedicated Ransomware and Digital Extortion Task Force, declaring ransomware attacks as a priority akin to terrorism. These new policies had dramatic impact on the cyberthreat landscape, driving aggressive actions by the government against the Darkside, Netwalker, and REvil ransomware groups, as well as crackdowns on cryptocurrency exchanges that processed ransomware payments.
If anything, ransomware attackers have become victims of their own success. While profiting from exorbitant ransom payments, they now suffer the repercussions of their notoriety.

Accordingly, we assess that in 2022 ransomware groups will be more selective when choosing their targets, largely eschewing attacks on sensitive or prominent targets (and perhaps avoiding targeting US-based organizations altogether) in favor of lower-profile targets, so as to avoid the wrath of a federal response. Some ransomware groups may choose to shut down their dedicated leak sites—designed to generate publicity—instead choosing to carry out their ransom attacks and negotiations over private channels. Overall, we assess that ransomware groups will adopt a more discreet modus operandi instead of aiming for splashy attacks.

If anything, this will encourage remote access markets to up their game. If ransomware operators demand a broader menu of potential targets, the markets will be driven to step up accordingly to provide the supply.

With ransomware gangs choosing to operate more discreetly, we expect that the increased distribution and decentralization of the underground ecosystem will persist. The largest forums can be too noisy, inundated with spam and raucous chatter, and due to their popularity, often attract the scrutiny and attention of law enforcement officials, researchers, and otherwise curious observers. It is therefore reasonable to expect that the threat actors of the underground will branch out to new forums and messaging channels, perhaps seeking out platforms that are more focused on a single subject matter in place of the larger, broad-based forums that deal with everything - from hacking, to recipes for cooking.

With the rapidly evolving cyberthreat landscape and continued impact of the COVID-19 pandemic on digital security to support the remote workforce, one thing remains certain: cybercriminals are fast innovators, quickly adapting and retooling their tactics to maximize their profits at their victims' expense. It is therefore imperative that organizations maintain vigilance, staying aware of the developments in the underground to enable proactive cyber defense.

Fortunately, no matter where malicious actors choose to set up shop – be it new sites, messaging apps, forums or other platforms – Cybersixgill will be there with eyes in the underground, making sure you **KNOW WHAT'S OUT THERE.**