

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

February 17, 2021



THE BUSINESS OF FRAUD: Sales of PII and PHI



Recorded Future analyzed current data from the Recorded Future® Platform, dark web and special-access sources, and open-source intelligence (OSINT) between January and December 2021 to observe the sale of compromised PII and PHI and how this data can be used to facilitate criminal activities. This report expands upon findings addressed in the first Insikt Group Fraud Series report, [“The Business of Fraud: An Overview of How Cybercrime Gets Monetized”](#).

Editor's note: This research covers January to December 2021. Since then, the following dark web sources are no longer in operation: UNICC Shop (January 2022), ToRReZ Market (January 2022), and Amigos Market (January 2022).

Executive Summary

Personally identifiable information (PII) and patient health information (PHI) are highly sought-after data across criminal sources, both on the clearnet and dark web. Our research identified that threat actors use various attack vectors, including social engineering and infostealer malware variants, to obtain victim PII or PHI. Once this data has been harvested, threat actors monetize it through traditional cybercriminal sources (dark web, including forums, marketplaces, and shops) and messaging platforms. Threat actors interested in buying and selling PII and PHI data continue to improve their tactics, techniques, and procedures (TTPs), with vendors selling customized services and methods that include access to accounts with sensitive user data, methods to defeat security measures, and counterfeit documentation.

Key Judgments

- Threat actors have various tools and capabilities at their disposal that facilitate access to victim networks to harvest and steal PII and PHI data.
- Financially motivated threat actors will continue to use all aspects of the cybercriminal ecosystem (forums, marketplaces, shops, and messaging platforms) to advertise, discuss, sell, and purchase compromised PII and PHI. Each of the 4 aforementioned source types is independent but all share overlaps that enable cybercrime.
- In addition to dark web and special-access sources that specialize in listing compromised user accounts containing PII, sources with a low barrier to entry, such as dark web marketplaces, are attractive destinations for threat actors to buy and sell scans and counterfeit documentation that contain PII.
- Ransomware extortion websites are another attractive source for threat actors to obtain PII and PHI, as their records contain proprietary data made available for free download when victims do not pay ransoms. These extortion websites will likely continue for the foreseeable future, as this method of extorting ransoms has proven effective.

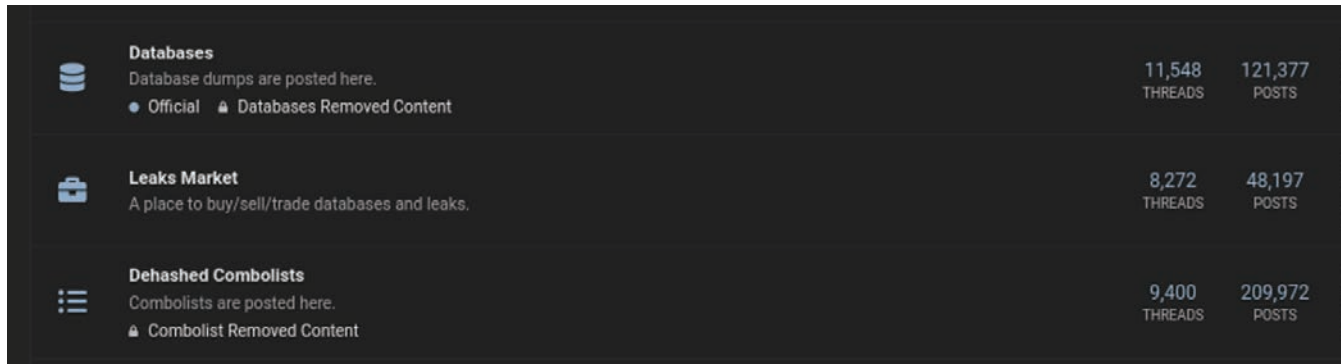


Figure 1: Sections of Raid Forums dedicated to the sale and sharing of database dumps and combolists (Source: Recorded Future)

Background

Personally identifiable information (PII) refers to data unique to individuals, such as full names, Social Security numbers, driver's license numbers, physical and email addresses, IP addresses, bank information, passport information, and more. Patient health information can include the same information, as well as demographic information, medical histories, test/laboratory results, mental health conditions, and more. Both types of data are highly sought after by threat actors for various reasons, from financial motivations to facilitating cyber espionage-related activities.

As most of modern society now functions on direct, interconnected communication and access via the internet, more and more PII and PHI data are going online. There are an estimated 4.66 billion internet users globally as of [January 2021](#), and the average American [manages](#) 100 different passwords (not including reuse per account). As of [2019](#), 100% of primary care physicians in New Zealand used electronic medical records (EMR, including PHI); England, the Netherlands, and Norway were at 99%. As of 2017, nearly [9 in 10](#) (86%) office-based physicians in the US had [adopted](#) EMR, and 96% of non-federal acute care hospitals possessed an ERM certification.

With such a large amount of personal and private records being stored on servers that are accessible to users worldwide with an internet connection, the exploitable attack surface is vast, making it nearly impossible to secure all systems properly.

Threat actors have at their disposal a plethora of tactics, techniques, and procedures (TTPs) to obtain PII and PHI, including keyloggers and infostealers, bank injects, spam and phishing services, sniffers, and released databases. Once PII data has been harvested, a threat actor can use it to carry out additional attacks through identify theft, social engineering, account takeover, phishing/spearphishing, business email compromise (BEC), credential stuffing and brute force attacks, and phone-related scams (vishing and smishing). A threat actor may also choose to advertise the data across the dark web's ecosystem in forums, marketplaces, and shops. Messaging platforms have become more mainstream and are more advanced in their encryption, ensuring greater anonymity and resulting in threat actors leveraging them to advertise, purchase, and sell PII and PHI records.

The Role of Database Dumps

A robust section of the underground economy relies on sales of compromised databases containing credentials, PII, PHI, or financial data. Threat actors obtain "fresh" databases by exploiting vulnerable technologies to gain access to victim systems, accessing misconfigured or exposed cloud buckets, using infostealer malware, or phishing campaigns. Threat actors then sell these databases by auctioning them off to other threat actors or by advertising them for a set price on special access forums like Raid, XSS, and Exploit.

Forums allow threat actors to quickly and easily advertise stolen data to a large number of potential buyers. Many forums have frameworks in place to ensure that data can be traded reliably among users, including escrow services and credibility (reputation scores) on users' profiles. These measures help decrease the risk of bad faith transactions and provide an added incentive for threat actors to continue using forums to reach a wider market.

FORUM	POSTS	THREADS	LAST POST
Cracking Tools This section is collecting all tools for scraping and parsing data, automated pentesting.	514.808 Posts	4.563 Threads	🌟[Combo Leecher] Nano Sc... Qui414 , 11 minutes ago
Cracking Tutorials This section contains tutorials on how to use tools to perform certain tests or scraping data.	288.822 Posts	4.344 Threads	Free Netflix Premium ? Ho... Bigniga20192 , 22 minutes ago
Cracking Configs You can find configs for all kind of tools here to perform web requests for scraping, parsing data or pentesting.	522.966 Posts	11.405 Threads	[OPENBULLET] CONFIG IZZI ... luisangelp349 , 6 minutes ago

OpenBullet Silverbullet Sentry MBA BlackBullet STORM SNIPR

Figure 2: Sections of Cracked forum dedicated to cracking tools, configs, and components to operate them (Source: Cracked Forum)

Recorded Future obtains and indexes such data dumps as well as combo lists shared publicly or privately on the dark web. A combo list is a data file containing email addresses/username and hashed or plaintext passwords. Threat actors assemble combo lists of credentials exposed in past data breaches into a single file and either sell or leak the combo lists on the dark web for other threat actors. The threat actor creating the combo list seldom provides specific information about the sources of the credentials. These dumps are often used for credential stuffing, an automated form of exploiting credentials found in compromised databases.

Role of Credential Stuffing/Brute-Forcing Tools

Threat actors use account checkers and brute-forcers because of the success they have had with gaining unauthorized access to user accounts on various platforms. Threat actors profit from selling cracked accounts on the dark web, which threatens users of various organizations around the world whose credentials were exposed in earlier data dumps and breaches and those who do not practice good password hygiene.

Configuration files (known as “configs”) are files required for account checking or cracking software such as OpenBullet/Black Bullet, SentryMBA, and STORM. A config file contains information required to check the validity of accounts and navigate the unique characteristics of the website being targeted. For example, the URL for the targeted website’s login page is typically specified in this config file. Other components typically required for a “cracking” tool such as OpenBullet/BlackBullet to operate effectively include:

- A proxy file or list of IP addresses to route traffic through to protect the anonymity of the user operating OpenBullet
- A combo list or database of usernames/password pairs to test against the targeted site, typically obtained in the aftermath of other breach events or as a result of being shared across underground sources

Special-access and dark web sources that focus on cracking tools, configs, and components to operate them include forums such as Cracked, Nulled, Sinisterly, Raid, and Hack Forums.

We found that many of the same threat actors that advertise configs on underground forums also sell them on Sellix, a go-to automated shopping website for cybercriminals for selling accounts and tools used in credential stuffing attacks.

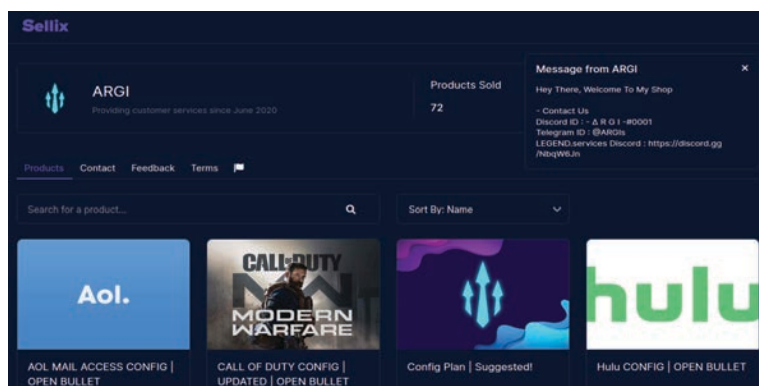


Figure 3: Threat actor “xARGIx” aka “ARGI” selling configs on Sellix (Source: Sellix)

This example of xARGIx selling config on Sellix highlights that cybercriminal activities are not specifically reserved or occurring just on dark web and special-access sources; rather, they are advertised on e-commerce, messaging services platforms, and clearnet sources that are more widely accessible to internet users.

Threat Analysis

PII and PHI records are in high demand across all facets of the cybercriminal ecosystem, especially on forums, marketplaces, and shops. Due to the large number of results identified for compromised PII and PHI data, for this report, we focused our research efforts on identifying sales trends, types of PII and PHI data being advertised, and the most active sources for listing specific types of compromised PII and PHI data. As each source type serves a purpose in propagating cyber-enabled crimes (for example, forums serving as messaging boards to announce products while messaging platforms, mostly used on mobile devices, are where prices for these advertisements are negotiated and finalized), there is not one source that dominates in regards to the most activity. For investigators conducting research and analysis of compromised PII and PHI records, as well as for other physical and digital commodities, it is essential to be cognizant of these separate source types, their role in facilitating cybercrime, and how each overlaps with the other.

PII Sales

Given the large amount of PII-related data in circulation, once a threat actor has acquired said data, the challenge becomes how to monetize it. From our investigations, threat actors resort to dark web and special-access sources to advertise, discuss, and sell PII data not just because of the anonymity that comes with these sources but also how specialized these sources are. As highlighted in our 2020 [report series](#), the dark web is an organized and structured ecosystem that provides threat actors direction as to where to conduct business (specific sources) and to reach threat actors most interested in purchasing their product. We have identified individual and databases being advertised under the following source types:

- Compromised user login accounts collected via infostealer variants
- Compromised payment card and account data
- Compromised and counterfeit documentation

Compromised User Logins

Compromised user login accounts have always been a sought-after commodity for cybercriminals, as gaining access permits a threat actor to take over the account as well as harvest any PII data within the account's profile that could be used towards further criminality, especially identify theft. Given this high demand and the need for anonymity, sellers of compromised user login data have moved away from advertising data on forums and into operating independently run shops. As of December 2021, the most popular and widely used shops for advertising this data are Genesis Store, Russian Market, Amigos Market, and Zeasy Shop.

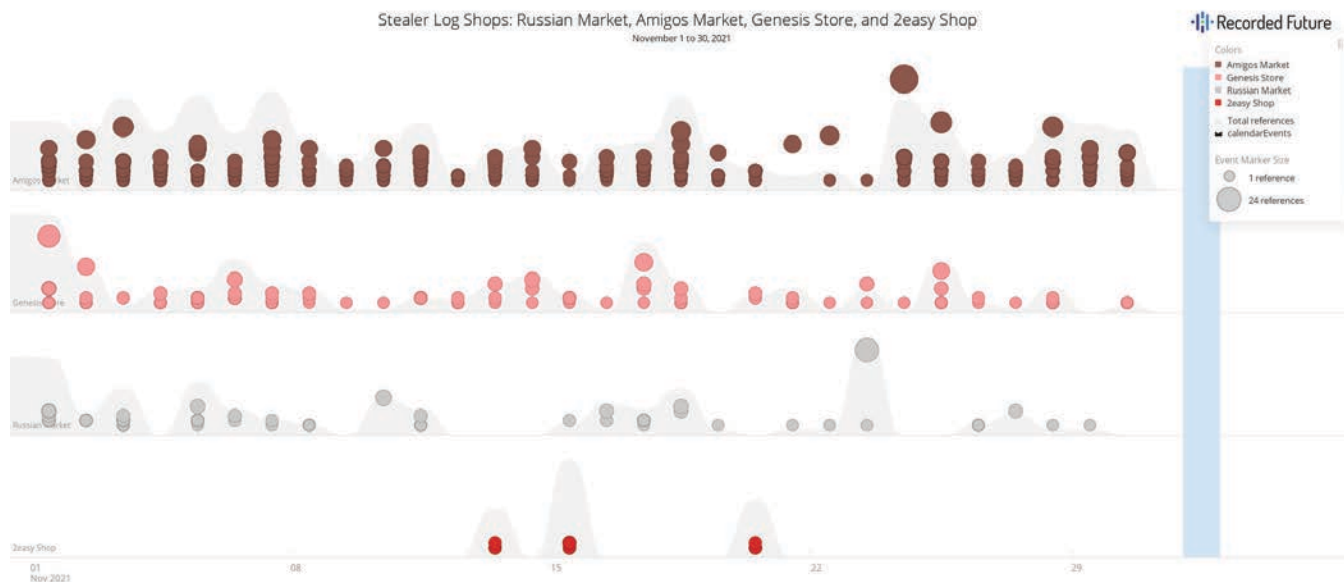


Figure 4: Sample of activities from November 2021 on 4 shops that sell compromised user logs (Source: Recorded Future)

As the first to launch in 2018, Genesis Store brought to the cybercriminal community a shop that combined anonymity when using a victim's accounts (through the shop's plugin, Genesis Security) with an easy-to-use interface. This uniqueness in victim listings coupled with security paved the way for copycat threat actors to set up similar shops, with the administrators of Russian Market launching their shop in 2020, followed by Amigos Market in 2021 and 2easy Shop in 2021. These shops are or likely are using the following infostealer variants to infect victim machines to harvest credentials: AZORult, Taurus, Vidar, RedLine, FickerStealer, and Raccoon Stealer.

In the summer of 2021, Insikt Group reported similarities shared between Russian Market and Amigos Market, specifically posting identical listings (at different prices) as well as these listings being removed from one shop after purchase from the other. Further analysis of both shops confirmed their overlaps, and we believe that the administrators of Amigos Market are ripping listings from Russian Market and selling these listings at similar prices. While there are some differences, the vast majority of listings are identical, which could be why the administrators of Russian Market announced that they are now only operating on The Onion Router (Tor) network as well as setting up additional security measures in November 2021. Lastly, the operators of Amigos Market remain banned on reputable, mid- to high-tier forums, further suggesting that Amigos Market is conducting more scamming than legitimate activities.

Given the popularity of these sources and their ability to collect, organize, and sell user credentials, we believe they will remain popular, go-to destinations for threat actors, with the exception being Amigos Market. The effectiveness and availability to rent or create customized infostealers (source code/cracked versions are available) will also remain a threat for the foreseeable future. As some variants (AZORult) have low barriers of entry to operate, threat actors can use infostealers with a variety of attack vectors, specifically phishing and smishing.

Compromised Payment Data

Shops that predominantly specialize in selling compromised payment data are often overlooked as sources of PII and PHI, but they will often also list PII data that comes with compromised payment cards or accounts, or sometimes list separate data, specifically full names, physical addresses, and at times dates of birth, phone numbers, and other non-payment card data. Shops such as DOC Shop and DATABASE Shop have in recent years listed more PII along with payment data, as the high volume of users interested in buying compromised payment cards can also purchase PII, allowing these shops' administrators to cut into the market share of those selling PII. Even with the closure of reputable payment card shops in 2021, specifically Joker's Stash in February 2021 and SliIPP, which was seized by law enforcement in [June 2021](#), the void left has been quickly filled by other payment card shops.

Since the closure of Joker's Stash and SliIPP, Insikt Group continues to monitor dozens of payment card shops that are listing PII alongside compromised payment cards and accounts. As of December 2021, the most popular shops are All World Cards Shop, Feshop, VClub, Infinity, BriansClub, Trump's Dumps, Unicc Shop, and BinBoss. Within some of these shops, users can search for specific PII of interest, as shown in Figure 5.

The screenshot shows a web interface for searching PII. At the top, a green banner displays 'SEARCH PRICE: FREE | ORDER PRICE: \$5'. Below this, a dark-themed section titled 'SSN with DOB search' contains several input fields. On the left, there are fields for 'DOB' and 'ZIP', with a note below the DOB field: '- DOB Formats: YYYY, YYYYMM, YYYYMMDD'. In the center, there are fields for 'STATE', '* FIRST NAME', and '* LAST NAME'. On the right, there is a 'CITY' field and a 'SEARCH BY' dropdown menu currently set to 'ZIP + FULL NAME'. A blue 'Search' button is located at the bottom right of the search area.

Figure 5: Example of PII user interface (Source: VClub)


















































	FINLAND Passport HQ PSD template Category: All Items » Counterfeit » Fake IDs MULTISIG:  ESCROW:   	 INSTANT DELIVERY	\$8.95 Buy Now	realfknhigh (288) (110/0/9) Rank 3 
	Australia High Quality Editable Passport Template Category: All Items » Fraud » Personal Information » Templates ESCROW:   	From Australia 	\$21.23 (AU\$30.00) Buy Now	auspride (4504) (2268/36/47) TOP 
	PASSPORT SCAN + SSN + UTILITY BILL USA Category: All Items » Fraud » Personal Information » Scans ESCROW:    		\$45.00 Buy Now	victorviran (1858) (509/18/55) TOP 
	Custom Scans Passport Scan 100% Guaranteed Category: All Items » Fraud » Personal Information » Fake ID's ESCROW:  		\$40.00 Buy Now	ubuntu009 (133) (47/0/7) Rank 2 
	SPAIN ID PACK x3 Passport +Gas Bill +ID card Category: All Items » Counterfeit » Fake IDs MULTISIG:  ESCROW:   	 INSTANT DELIVERY	\$19.95 Buy Now	realfknhigh (288) (110/0/9) Rank 3 
	USA DOCUMENT (DRIVER LICENSE,ID,PASSPORT) Category: All Items » Fraud » Personal Information » Scans ESCROW:   		\$150.00 Buy Now	yoshisteam (554) (217/10/16) Rank 6 
	Taiwan Passport PSD Template Category: All Items » Fraud » Personal Information » Templates MULTISIG:  ESCROW:  	 INSTANT DELIVERY	\$9.99 Buy Now	GoldApple (2277) (541/28/34) TOP 
	UK GENUINE PASSPORT SCAN Category: All Items » Fraud » Personal Information » Scans ESCROW:  		\$25.00 Buy Now	kingscan (98) (70/1/1) Rank 1 

Figure 6: Sample of listings containing scans and templates with PII (Source: ToRReZ Market)

Counterfeit Documentation

Another popular means for threat actors to acquire compromised PII is through stolen documentation like passports, driver's licenses, billing statements, vaccination cards, diplomas, and other records. The term "fullz" refers to accounts that contain full information — full names, dates of birth, Social Security numbers, and so on. The documentation is usually sold as digital scans or uploaded images. These scans and images facilitate identity theft and help threat actors create counterfeit documents that can be used to open banking accounts, file tax returns and unemployment claims, register phone numbers, and more. Some shops advertise stolen documentation and fullz, but the most popular sources for listing these types of documents remain dark web marketplaces.

Since the launch of Silk Road in 2010 and even after its [seizure](#) by law enforcement in 2013, these digitized and anonymous marketplaces have remained an active destination for threat actors of all levels to trade all types of commodities. Even after the seizures of AlphaBay and Hansa marketplaces in 2017, and despite competition between dark web marketplace administrators, the dark web marketplace ecosystem continues to flourish. In 2021, the following dark web marketplaces committed exit scams, were seized by law enforcement, or closed operations: The Canadian Headquarters, DeepSea Market, White House Market, Neptune Market, DarkMarket, Berlusconi Market, Aurora Market, Corona Market, and Daeva Market. Despite the turmoil and uncertainty of the marketplace ecosystem, as of December 2021, we are monitoring over 20 active dark web marketplaces listing hundreds of different products by hundreds of different vendors that are viewed by thousands of daily users.



Figure 7: Most newly launched marketplaces will list PII due to high demand and popularity (Source: Cartel Market)

The following sources contain the most PII-related activities (including listings of passports, scans, and general PII, customer feedback, and more): DarkFox Market, DarkOde Reborn, Kingdom Market, Liberty Market, World Market, ToRReZ Market, and Versus Market.

In addition, smaller and recently launched marketplaces, such as MGM Grand Market, WeTheNorth Market, Cartel Market, Bohemia Market, and Tor2Door Market, also post listings for compromised PII and counterfeit documentation. Because compromised PII and counterfeits are always in high demand, newly launched marketplaces will almost always list it to attract users, boost profits, and capture market share.

In August 2021, one of the former administrators of the original AlphaBay Market, "DeSnake", relaunched the marketplace after its [seizure](#) by law enforcement and arrest of its administrator in July 2017. The relaunch included some enhanced security measures (proprietary "AlphaGuard" for cryptocurrency wallet access, bulletproof servers to handle disruptions, among others) not seen before in other dark web marketplaces. DeSnake is pushing users to access the marketplace via [Invisible Internet Project](#) (I2P), a more anonymous and erupted layered network than Tor that permits user peer-to-peer communication and great security.

Although there is skepticism of DeSnake's motivations for relaunching AlphaBay, its relaunch shows that the dark web marketplace ecosystem remains an active environment where administrators feel confident that they can develop and host platforms for users to transact while also garnering profits (commissions) per sale. Given the often low barrier of entry to access these sources, we believe that dark web marketplaces will remain attractive destinations for threat actors to buy and sell PII, PHI, and other commodities for the foreseeable future.

PHI Sales

Similar to PII, PHI records are in high demand due to their sensitivity as well as overlaps with general PII like full names, email and physical addresses, SSNs, and other proprietary data. From January 1 to December 1, 2021, Insikt Group reported over 80 incidents of healthcare-related facilities being affected by a data breach, third-party compromise, insider threat and human error, or a cyberattack that led to the compromise of PHI records. Many of these incidents also included the exposure of PII:

- In January 2021, Hendrick Health Systems of Texas notified patients that their PHI records had been compromised after a threat actor gained access to their network between October and November 2020.
- In February 2021, University of Pittsburgh Medical Center (UPMC) disclosed a data breach after the law firm Charles J. Hilton & Associates (who handles UPMC's legal services) had their network accessed by a threat actor. The threat actor harvested PII and PHI data, which affected over 36,000 patients.
- In April 2021, Red Deer Regional Hospital Centre of Alberta, Canada had their network accessed by a threat actor who compromised 3,224 patient records.
- In May 2021, Rehoboth McKinley Christian Health Care Services (RMCHCS) was affected by a Conti ransomware attack that resulted in threat actors harvesting PHI data of at least 200,000 patients.
- In June 2021, the healthcare provider Physicians Dialysis reported that a threat actor accessed their network (March 2021) and PHI data was harvested.
- In August 2021, Harris County in Texas revealed a data breach that resulted in the theft of at least 26,000 patient records from the county jail's healthcare provider. The data was exposed on the county's Justice Administration Department website from March to May 2021.

- In August 2021, University of New Mexico (UNM) Health was targeted by a threat actor who gained access to their network and harvested over 637,000 PHI records. Affected hospitals included UNM Medical Group, UNM Sandoval Regional Medical Center, and UNM Hospital.
- In October 2021, an insider threat collected over 9,300 PHI records from the University Hospital Newark and gave these to an illegal third party from January 1, 2016, to December 31, 2017.
- In November 2021, Huntington Hospital of California notified 1,800 patients that their PHI data was illegally accessed by an employee from October 2018 to February 2019.

Over the last year, Insikt Group reported on threat actors indiscriminately stealing PHI from healthcare-related institutions including hospitals, rehabilitation facilities, fertility and cosmetic clinics, and government level health-related departments. Furthermore, threat actors were opportunistic in their harvesting of PHI-related data from these institutions by targeting healthcare facilities around the globe, including institutions in the United Arab Emirates (UAE), United States, Colombia, China, India, Canada, Indonesia, Mexico, Iran, and Brazil, among others. A majority of this data is listed for purchased on dark web and special-access forums, as well as marketplaces, with a sample of PHI and physician records listed below (prices listed in USD):

Threat Actor	Intelligence
"jsamada7864"	In November 2020, the threat actor auctioned off (\$25,000 minimum bid, with \$40,000 for immediate purchase) on Exploit Forum 2 million PHI records from various hospitals across the US that included full names, Social Security numbers, dates of birth, genders, marital statuses, and physical addresses.
"538463"	In January 2021, the threat actor advertised on the Mandarin-language Exchange Market over 176,000 China-based physician records for \$300 that included full names, phone numbers, hospital addresses (city and province), and employment and departments per hospital. The threat actor claimed to have collected the data via unspecified, personal channels.
"Scarfac33"	In January 2021, the threat actor shared over 700,000 PHI records of compromised data on Raid Forums that affected a Mexican hospital and included full names, dates of birth, genders, physical addresses, dates of hospitalization, and additional patient information.
"595084"	In May 2021, the threat actor advertised over 7,000 PHI records of diabetic patients for \$25 from an unnamed rehabilitation center in China that included full names, phone numbers, and physical addresses.
"Lorax"	In July 2021, the threat actor listed PHI records from an unnamed, US-based medical service provider (likely based in Florida) that included medical charts for \$100 per document.
"Brady"	In August 2021, the threat actor advertised on Exploit Forum hundreds of stolen PHI records from servers of unspecified hospitals via different third-party account login credentials that included full names, dates of birth, physical addresses, Social Security numbers, and identification cards.
"injection"	In September 2021, the threat actor advertised at least 65 databases composed of 16 million records from Thailand's Ministry of Public Health on Raid Forums for \$500 that included full names, genders, dates of birth, healthcare information (doctor names, hospital locations, registration and discharge dates, and more), and financial data (bills, payments received, and more)

Table 1: List of threat actors selling PHI and physician records and databases (Source: Recorded Future)

In addition to listing downloadable files that contained the aforementioned databases, threat actors also list or sell access to (usually via auction) compromised healthcare-related networks, which provide buyers greater access into the compromised network, allowing them to deploy malware that facilitates credential harvesting or data capture, as well as anti-detection mechanisms for long-term presence. Insikt Group reported over the last year on examples of these activities:

Threat Actor	Intelligence
"fooble"	In December 2020, the threat actor auctioned off Citrix account credentials for an unnamed Canada-based healthcare provider listed as having over 18,000 employees and an annual revenue of \$3 billion. The auction's starting bid was \$4,000, with immediate purchase available at \$15,000.
"pshmm"	In March 2021, the threat actor listed for purchase RDP access to the network of an unnamed US-based healthcare center for \$6,000. The company was described as operating over 650 workstations and 50 servers within the network domain, as well as having an annual revenue of \$91 million.
"V.V.P"	In September 2021, the threat actor auctioned off RDP access to the networks of 2 organizations, 1 being an unnamed Australia-based health organization that works with remote indigenous Australian communities and was listed at a \$19 million annual revenue. The opening bid was \$500, with immediate purchase available at \$1,200.
"3073a"	In September 2021, the threat actor auctioned off an unspecified network access method for an Italian healthcare products manufacturer that operates multiple domains and has an annual revenue of \$1 billion. The threat actor listed the initial bid at \$3,000, with immediate purchase available at \$5,000.
"NooSphere"	In October 2021, the threat actor auctioned off Citrix account credentials with administrative privileges of an unnamed French company that specializes in emergency medical transportation services on Exploit Forum for \$800. Immediate purchase was available for \$2,000.

Table 2: Threat actors listings compromised network access for healthcare-related entities (Source: Recorded Future)

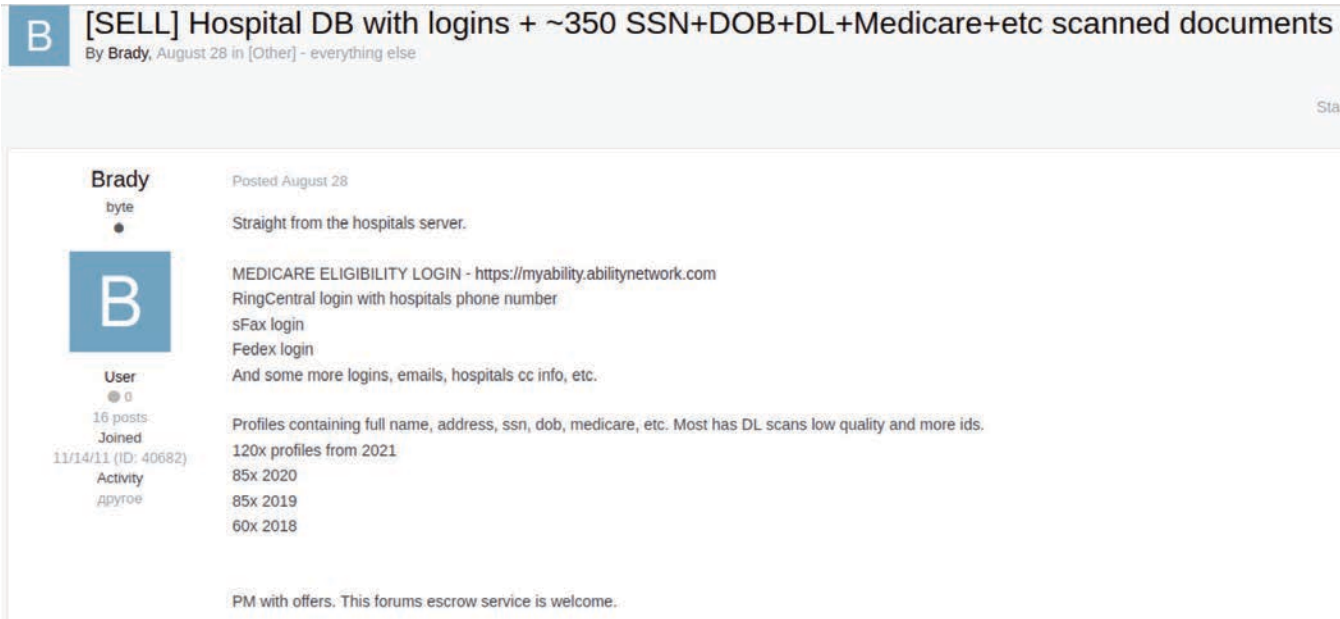


Figure 8: Hospital database with logins as advertised by Brady that is still available for purchase as of December 2021 (Source: Exploit Forum)

Lastly, PHI and physician records are often associated with leaked documentation and records posted by ransomware threat actors on extortion websites if ransoms were not paid. Once the records have been posted, they are free to download to any user that is able to access the extortion website (usually no login credentials but Tor access is required). In the beginning of the COVID-19 pandemic, ransomware threat actors did not target hospitals due to the uncertainty of the evolving health crisis as well as the negative publicity. But as the pandemic continued, threat actors [resumed](#) ransomware attacks against hospitals due to them being incentivized to pay ransoms so as to maintain function of hospital networks and systems. As [reported](#) by The Record, ransomware attacks on healthcare providers remain a consistent threat, with 7 providers being affected in October 2021.

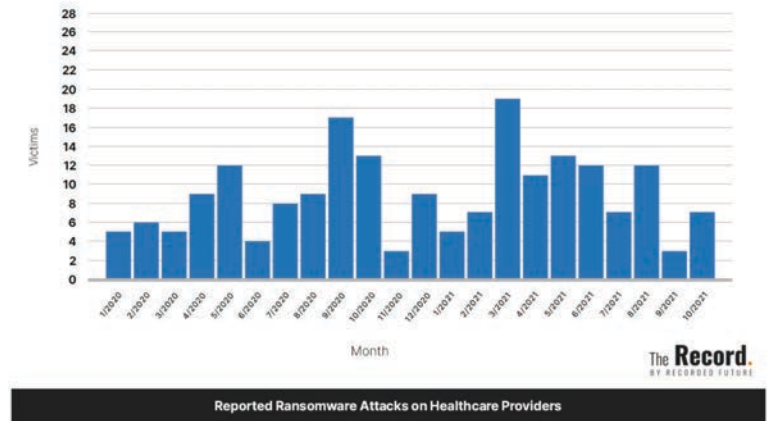


Figure 9: Ransomware attacks directed at healthcare providers for November 2021 (Source: [The Record](#))

Over the last 6 months, BlackByte Blog (BlackByte ransomware), HiveLeaks (Hive ransomware), Corporate Leaks (Nefilim ransomware), Conti.News (Conti ransomware), and Pysa's Partners (Pysa ransomware) were the top 5 leading extortion websites for listing PHI-related data:

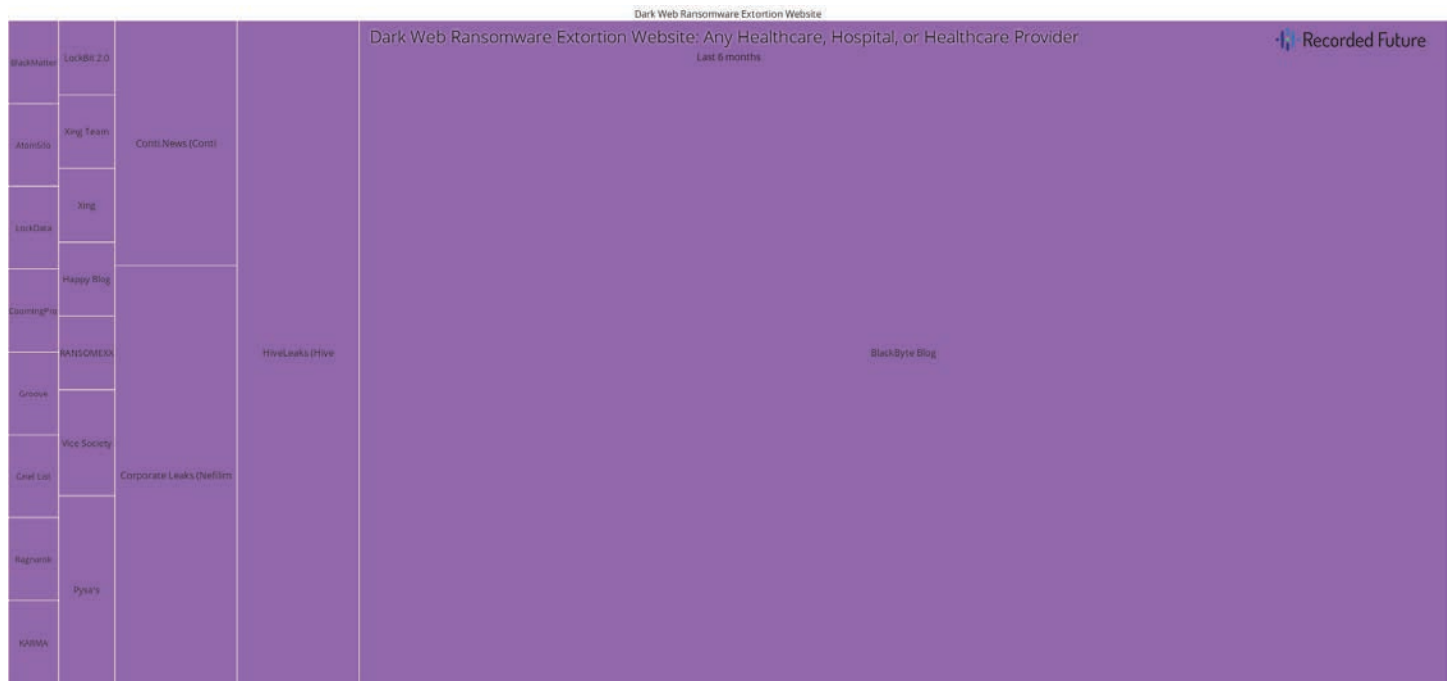


Figure 10: Leading ransomware extortion websites for posting PHI-related data over the last 6 months (Source: Recorded Future)

Mitigations

Credential leaks and email exposure amplify the risks associated with phishing and ransomware attacks, as the data can be used to devise tailored spearphishing lures and serve as initial points of compromise via credential stuffing and account takeover. Recorded Future clients can surface exposed credentials in the Recorded Future Platform. Organizations should determine if the exposed credentials that appear alongside passwords are still active and, if so, force password resets for those users, specifically accounts that contain sensitive PII or PHI data.

Threat actors can attack networks using proprietary tools, vulnerabilities in networks, or other attack vectors. The following practices may mitigate the risks of threat actors targeting PII and PHI:

- Keep all software and applications up to date, especially operating systems, antivirus software, and core system utilities.
- Filter email correspondence and scrutinize attachments for malware.
- Make regular backups of your system and store the backups offline, preferably offsite so that data cannot be accessed via the network.
- Have a well-thought-out incident response and communications plan.

- Adhere to strict compartmentalization of company-sensitive data. In particular, look at which data anyone with access to an employee account or device would have access to (for example, through device or account takeover via phishing).
- Strongly consider instituting role-based access, limiting company-wide data access, and restricting access to sensitive data.
- Employ host-based controls; one of the best defenses and warning signals to thwart attacks is to conduct client-based host logging and intrusion detection capabilities.
- Implement basic incident response and detection deployments and controls like a network intrusion detection system (IDS), netflow collection, host logging, and web proxy, alongside human monitoring of detection sources.
- Be aware of partner or supply chain security standards. Being able to monitor and enforce security standards for ecosystem partners is an important part of any organization's security posture.

Outlook

The large amount of compromised PII and PHI data advertised by cybercriminals highlights the vulnerability of networks and data and the demand for that data. As most threat actors are financially motivated, if the market demanded another product, efforts to meet this demand would likely follow. Given this high demand and the challenges associated with monetizing compromised PII and PHI, the dark web and criminal ecosystem continues to evolve and update so as to stay ahead of law enforcement, researchers, and those tasked with protecting security networks and proprietary information. We believe that not only will forums and marketplaces remain high-volume source types for posting compromised data, but that threat actors will continue to migrate towards establishing independent shops selling PII and PHI that incorporate messaging platforms on mobile devices due to greater autonomy and instantaneous communications and transactions.

Due to the large volume of PII and PHI data being submitted to forums, marketplaces, shops, and messaging platforms daily (and even hourly), it is essential for investigators to collaborate with companies like Recorded Future that provide data aggregation and alerting that is easy to interpret. In most cases, once PII or PHI data has been posted to a source, it becomes available to all users. Once your company has been alerted, we recommend triaging this immediately so as to gauge its sensitivity and ascertain appropriate mitigation. Lastly, we recommend staying abreast to the latest TTPs being deployed by threat actors focused on stealing, buying, or selling PII and PHI data, as threat actors are constantly changing tactics and targeting.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.