



# Pricing Analysis of Goods in Cybercrime Communities

# Pricing Analysis of Goods in Cybercrime Communities

BY IAN GRAY

Illicit activity within cybercrime communities is anything but static. Threat actors react to new vulnerabilities, keep up with and bypass anti-fraud measures, and continue to support a robust economy around stolen payment card data, credentials, and access to compromised systems.

Yet one thing that seems to stay relatively constant—during the past two years anyway—is pricing of the products and services for sale on deep and dark web (DDW) markets.

Flashpoint analysts have twice since 2017 conducted a survey of prices for various offerings available across the DDW, evaluating changes in pricing for "fullz" (full packages of personally identifiable information [PII]), passports, distributed denial-of-service (DDoS)-for-hire attack services, exploit kits, remote desktop protocol (RDP) servers, payment card data, and bank logs.

Since 2017, there have been modest price bumps for some long-standing offerings related to fraud and cyberattacks. But these shifts are miniscule compared to the dramatic innovation happening in other depths of the cybercrime ecosystem—specifically with respect to targeted ransomware and SIM swapping, to name two.

Another constant from 2017: It's still unclear what the determinants are for pricing trends within the cybercrime economy. Prices can vary drastically across the DDW, and the reasons for the discrepancies remain largely unexplained.

What follows is a comparative look at pricing over the past two years and an examination of trends within each area of offerings within cybercrime communities. Organizations should understand that any fluctuations in price listings and future changes should inform how the cybercrime landscape is developing, and how businesses should respond to this threat.





# COMPARATIVE PRICING 2017-2019

While Flashpoint analysts observed various pricing ranges and patterns related to specific offerings within illicit online marketplaces, forums, and card shops, the determinants of pricing trends for various items within this underground economy remain unclear. It is important to note that the product listings surveyed by analysts were primarily sourced from the most popular cybercrime marketplaces, many of which shut down over the last year, either through law enforcement intervention or exit scams. The listings within these marketplaces are designed to bolster fraud, such as carding and identity theft, and act as an entry point for less sophisticated threat actors. The trends presented in this paper function largely as case studies and general observations rather than precise pricing statistics.

Similar to the previous pricing survey in 2017<sup>1</sup>, analysts assess with moderate confidence that prices will likely vary drastically across the DDW, and the reasons for the discrepancies are largely unexplained.

## FULLZ

Slang for a full package of personal information connected to an individual, fullz provide enough information for a criminal to steal and profit from a victim’s identity. Fullz generally include the victim’s name,

Social Security number, date of birth, account numbers, and more. Given the endless parade of data breaches and the continued use of Social Security numbers, for example, as identifiers, fullz sourced from the United States are generally priced as a commodity inside English speaking illicit communities. The typical range stretches from \$4 to \$10 USD, up slightly from 2017. A variety of factors can influence this price, such as the availability of accompanying financial information.

Fullz that include the victim's financial information often cost more because they can be used for a greater variety of fraud schemes than PII without such information. Fullz with this additional information on average range in price from \$30 to \$65 USD.

Additionally, some actors organize their fullz for sale by credit scores; fullz with higher credit scores are priced higher because they are viewed more favorably by financial institutions and other organizations that cybercriminals may wish to defraud. Fullz with a credit score of 700 or higher are typically priced at \$40 USD. In our previous survey, actors were soliciting \$60 typically for credit scores of 700 or higher, while 800 or better were priced at \$80.

Flashpoint analysts have yet to carry out a full analysis of the pricing of international PII. For comparison purposes, in one example, fraudulent

Australian documents, specifically driver's licenses, tend to be priced higher than U.S. documents. Flashpoint analysts assess with a low degree of confidence that international PII—especially European and North American PII—is likely priced higher than U.S. PII due to the relative scarcity and potential fraud value of such information in the DDW.

## REPRESENTATIVE SAMPLE OF 2019 FULLZ PRICING IN USD

2018 credit card and fullz from service industry	\$10
Cashing out bank accounts and fullz empty it	\$4
EU/Asia/UK credit cards / fullz	\$860
\$20,000 bank loan cashout using fullz	\$30
Fullz SSN - DoB	\$5

<sup>1</sup> <https://go.flashpoint-intel.com/docs/analysis-pricing-of-goods-and-services-on-the-ddw>

## U.S. PASSPORTS

U.S. passports are available within cybercrime communities primarily in three formats:

1. A scanned copy where the vendor sends the buyer a digital scan of the passport with their information inputted
2. A template for a U.S. passport where the buyer is free to input their own information
3. A physical U.S. passport where a passport with the buyer's information is mailed to the buyer

Passports, as with most other U.S. government-issued identification documents, are protected by numerous anti-fraud measures<sup>2</sup> such as certain cardstock, ink, perforations, patterns, and more. Bypassing these security measures is difficult, but it's a challenge many operating within cybercrime communities have accepted, and some are finding success in doing so. Those with higher quality documents and proficiency in bypassing anti-fraud measures can demand a premium for documents such as passports.

As for pricing, scans (digitally scanned copies sent to a buyer with their information inputted) are at the low end, while U.S. passport templates

(a PSD template allowing the buyer to input their information) are the most common offering. This can easily be offered across multiple marketplaces and the pricing is relatively low, but there is a variance depending on the country or location.

Physical passports are the most difficult to produce from scratch and are typically priced at the highest end of the spectrum. It is worth noting that the more expensive physical passports usually include other substantiating documents in the price, such as a driver's license, Social Security Number, and/or birth certificate. These primary documents can also be used to open bank accounts in various countries or locations.

In our 2017 survey, scanned passports typically ranged in price from \$5 to \$65 USD, passport templates typically ranged in price from \$29 to \$89 USD, and physical passports typically ranged in price from \$2,980 to \$5,000 USD.

## REPRESENTATIVE SAMPLE OF 2019 IDENTIFICATION DOCUMENTS AND PRICES IN USD

U.S. passport PSD template	\$18
Driver's license template, passport, certificates	\$1,000
UK driving license, passport pack, PSD photo	\$3-\$26
Australian passport PSD template	\$18
Canadian passport PSD template	\$26-\$46
France passport PSD template	\$45
Germany passport PSD template	\$46
Netherlands passport PSD template	\$50
Spain passport PSD template	\$45
Sweden passport PSD template	\$5
Turkey passport PSD template (fully editable)	\$45

<sup>2</sup> <https://www.flashpoint-intel.com/blog/fake-id-fabrication-in-race-with-anti-fraud-measures>

### DDOS-FOR-HIRE-SERVICES

DDoS-for-hire pricing depends on many factors and similarly does not have a clear pricing trend in cybercrime communities. For example, the pricing of a DDoS botnet—a network of infected machines leveraged by botnet operators to carry out DDoS attacks—ranges from \$1 to \$100 USD and varies upon bandwidth and duration. This pricing is noticeably higher than 2017 when the high end of the range was \$27.

Several changes to the overall operating environment have had an effect on DDoS-for-hire pricing. The rates for taking down bigger websites are custom crafted due to different forms of DDoS protection and ways to bypass them. Many websites use DDoS protection or a Content Distribution Network (CDN), so taking them down is usually beyond the capabilities of almost all bot herders. However, there are instances where threat actors can successfully target larger websites, such as the takedown of Wikipedia via a DDoS attack in September 2019<sup>3</sup>. The threat actor targeted everything to a single data center, which was beyond the scope of Wikipedia’s prior stress testing. This tactic is outside the norm, however, and most attacks remain focused on video game cheating and personal harassment.

Additionally, booters—web-based services that perform DDoS-for-hire attacks—are priced depending on bandwidth and duration. Threat actors also offer DDoS-for-hire attack services by the minute and the hour. These prices range depending on the threat actor and the type of targeted website.

In 2017, most booters ranged from \$5 to \$30 USD for the most basic account, yet would only push between 1 and 20 Gigabits per second (Gbps), with the vast majority only pushing between 1 and 5 Gbps of malicious traffic. However, premium accounts with longer boot times and more concurrent attacks are sold for a higher price.

Furthermore, threat actors also offer DDoS-for-hire services by the hour. These prices range depending on the threat actor and the type of targeted website. For example, a DDoS attack on a regular website is typically \$10 USD per hour, whereas an attack on a protected website is typically \$25 USD per hour. The most expensive per hour DDoS attack rates include attacks on government, military, or bank websites; the costs for such services typically range from \$100 to \$150 USD per hour.

### REPRESENTATIVE SAMPLE OF 2019 DDOS-FOR-HIRE SERVICES PRICED IN USD

DDoS attack service	\$165
Rent HTTP DDoS IoT botnet (unprotected) 1 day	\$25
Rent HTTP DDoS IoT botnet (unprotected) 10 minutes	\$0.35
Rent HTTP DDoS Windows botnet (protected) 1 day	\$50
Rent HTTP DDoS Windows botnet (protected) 10 minutes	\$0.35
Rent UDP DDoS layer 4 botnet (servers) 1 day	\$100
Rent UDP DDoS layer 4 botnet (servers) 10 minutes	\$1.45
Booter website remote root exploit report error	\$60
“I will ddos attack any site you wish (5 hours)”	\$250
3 Hours DDoS Botnet Attack (~ 200k Requests / Sec)	\$35

<sup>3</sup> <https://www.bleepingcomputer.com/news/security/wikipedia-ddos-attacks-prompt-ncsc-to-remind-of-dos-mitigation>

## EXPLOIT KITS

Not so many years ago, exploit kits were the de facto means of large-scale web-based compromises spreading all manner of malware, from click-fraud attacks to ransomware. Exploit kits are automated attack tools that first compromise websites, and then exploit vulnerable browsers of site visitors in order to spread malware or carry out other attacks. A number of high-profile arrests put some popular exploit kits on the sidelines<sup>4</sup>, but they still maintain a viability within illicit communities.

Flashpoint’s analysis determined that exploit kits are still rented out, with different pricing options for daily, weekly, and monthly rentals; functionality often determines pricing, as does the exclusivity of the kit. These kits are rarely sold. Prices have also remained relatively stagnant between 2017 and 2019, Flashpoint analysts learned.

### AVERAGE PRICES

Daily rental	\$80-\$100
Weekly rental	\$500-\$700
Monthly rental	\$1,400-\$2,000

There are exploit kits currently being offered on cybercrime marketplaces, however the credibility and reliability of these services decreases on these sources. For example, vendors on markets regularly advertise “blackhat” exploit kits, such as Bleeding Life (2.0) and Black Hole, for \$5 to \$15.

<sup>4</sup> <https://threatpost.com/inside-the-demise-of-the-angler-exploit-kit/120222>

### RDP ACCESS

Remote Desktop Protocol (RDP) is Microsoft’s proprietary protocol used by most often system administrators to remotely connect to other machines over the network for updates and other support tasks. RDP clients are available for other operating systems beyond Windows, including Linux, Unix, Mac OS X, iOS and Android. RDP server software exists for Windows, Unix, and Mac OS X.

As in most cases where threat actors find a way to leverage legitimate services for malicious purposes, RDP is no exception. A number of DDW markets offer RDP server access and criminals leverage this access to facilitate account takeover attacks, deliver spam, carding, fraud, or hide in plain sight from law enforcement and security researchers.

The xDedic<sup>6</sup> market was considered by many to be the most thriving underground shop selling RDP access before it was shut down in January by a joint international law enforcement action to seize its servers. Cybercriminals typically purchase RDP access to servers that have already been breached via large marketplaces such as the former xDedic. Following its takedown, threat actors migrated toward cybercrime marketplaces that can provide general RDP services, as well as more specialized shops.

DDW marketplaces selling access to compromised RDP servers have become increasingly popular in the cybercriminal ecosystem in the past several years, as the listings are less specialized but serve a wider audience. Flashpoint analysts detected different categories of RDPs:

- Country specific
- Operating system specific
- Administrator access
- Residential
- Hacked
- Patched
- Carding
- Bank Drops

As with exploit kits, pricing has remained largely stagnant since 2017.

### REPRESENTATIVE SAMPLE OF 2019 RDP PRICES IN USD

Any country RDP	\$26
Hacked RDP	\$35
U.S. RDP hacked and patched	\$15
RDP connect 100% carding success	\$5
U.S. bank drop RDP + PayPal	\$575
PayPal with debit card + fullz +RDP	\$250-\$350
RDP with admin access worldwide	\$10

<sup>6</sup> <https://www.flashpoint-intel.com/blog/rdp-access-to-hacked-servers-still-a-thriving-business-on-deep-dark-web> | <sup>6</sup> <https://www.flashpoint-intel.com/blog/cybercrime/xdedic-rdp-targets/>

## PAYMENT CARD DATA

Pricing for cards and card dumps varies greatly and is influenced by a number of factors. The stolen card data is used for fraudulent purchases or to clone physical cards.

Characteristics such as freshness (how recently the data was sourced), country of origin, availability of Track 1 and Track 2 data, expiration date, and other factors can affect pricing.

Flashpoint analysts assess with a moderate degree of confidence in 2019 that the price of cards in card shops likely often ranges between \$2 and \$20 USD. These prices have not changed in the last two years.

Many card shops offer both "cards" and "dumps." Cards, which are often sourced from online, card-not-present (CNP) transactions and include information such as card number, expiration date, and cardholder name. Dumps, on the other hand, are often sourced directly from malware-infected or skimmed point-of-sale (POS) terminals and consist of track data. Dumps— which include Track 1 and Track 2 information and can be used for a wider variety of fraudulent activities than cards—are typically priced higher than cards. Flashpoint analysts assess with a low degree of confidence that a typical pricing range for dumps is likely from \$5 USD to more than \$200 USD.

## BANK LOGS

Access to online bank accounts, often marketed by cybercriminals as bank logs, are often available for sale on cybercriminal marketplaces and forums. These bank logs are priced depending on the balance available in the bank account, as well as the financial institution. As such, accounts with a high balance tend to be more expensive than accounts with low balances.

### REPRESENTATIVE SAMPLE OF 2019 BANK LOG PRICING IN USD

U.S. bank log \$10k balance	\$25
U.S. bank log \$5k to \$10k balance	\$62.40
German bank log €7K balance	\$175
U.S. bank log \$3,000 to \$4,000 balance	\$50
U.S. bank log \$3,000 to \$7,000 balance	\$75



## ASSESSMENT

Cybercrime communities continue to thrive and offer products and services that are in demand to threat actors globally. While the development of new and innovative attacks continues among more technically sophisticated threat actors on disparate sources including forums and encrypted communication channels, the pricing of some commodity products and services has remained relatively the same during the past two years.

Flashpoint analysts have observed modest price increases for some offerings since their first survey of DDW pricing in 2017. Another thing that remains constant is that it remains unclear what the determinants are for pricing trends within the DDW economy. Prices can vary drastically across the DDW, and the reasons for the discrepancies remain largely unexplained.

Analysts assess with a moderate degree of confidence that the majority of vendors on DDW marketplaces are likely resellers, using a price that has already been established largely by overall market supply and demand. The prices are set by the vendors, and not the administrators of the marketplace. With the fluctuations of marketplaces during the last few years, the price consistency may be an attempt to maintain stability without affecting the demand of fraud-related products and services.

However, monitoring product and price listings should provide a temperature check for the cybercrime climate because a number of listings are catered to the entry-level threat actor. Understanding price listings and future changes should inform how the cybercrime landscape is developing, and how businesses should respond to this threat.

PUBLISHED ON OCT 15, 2019

## CREDITS

The primary author of this report is Ian Gray. Contributors include Maxwell Aliapoulis, Vlad Cuiujuclu, and Allison Nixon. A special thanks to the entire Flashpoint intelligence analyst team for supporting the research and analysis that made this report possible.

## ABOUT FLASHPOINT

Flashpoint delivers Business Risk Intelligence (BRI) to empower organizations worldwide with meaningful intelligence and information that combats threats and adversaries. The company's sophisticated technology, advanced data collections, and human-powered analysis uniquely enables large enterprises and the public sector to bolster cybersecurity, confront fraud, detect insider threats and build insider threat programs, enhance physical security, improve executive protection, and address vendor risk and supply chain integrity.

For more information, visit [www.flashpoint-intel.com](https://www.flashpoint-intel.com) or follow us on Twitter at [@FlashpointIntel](https://twitter.com/FlashpointIntel).