

Report

# The dark market report — A new economy

**rackspace**  
technology™

**ARMOR™**



# Table of contents

<b>Armor 2020 dark market report</b> .....	<b>3</b>
About the report .....	3
Why dark web threat intelligence? .....	3
What's new on the dark web?.....	3
<b>Price list for hackers goods and services</b> .....	<b>4</b>
<b>Cybercrime services</b> .....	<b>5</b>
A turnkey, eCommerce service for dark web vendors.....	5
Cybercrime-as-a-Service: destroy a business and DDoS.....	5
Bulletproof web hosting services .....	6
Commercial software for rent .....	6
<b>Underground Marketplace products</b> .....	<b>7</b>
Hackers add business fullz to their repertoire .....	7
Tools of cybercrime trade .....	7
Remote desktop protocol credentials .....	8
Get your degree at Hacker University.....	9
Ransomware evolves to be more heinous.....	9
<b>Conclusion</b> .....	<b>10</b>
<b>How Rackspace Technology helps</b> .....	<b>11</b>
Take our Cybersecurity Risk Self-Assessment .....	11

# Armor 2020 dark market report: a new economy

In times of war, natural disaster or political turmoil, underground economies often thrive. In 2020, COVID-19 took the world by storm.

And while COVID-19 has wreaked havoc on economies around the world, it also, unfortunately, seems to have created new opportunities for underground cyber markets. This comes at a time when the tools and communication vehicles for cybercriminals are becoming more innovative, inexpensive and readily available.

Today, the underground economy — comprised of stolen credentials, malicious software and tools for financial fraud — continues to grow across hundreds of dark web markets, some of which claim to have as many as one million monthly visitors.

## About the report

This report from Armor, a Rackspace Technology™ partner, was created by Armor's security research team, the Threat Resistance Unit (TRU). Between October 2019 and June 2020 the TRU team investigated 15 markets and a variety of underground hacker forums, news sites and open repositories, to understand the state of what continues to be a growing and innovative ecosystem.

## Why dark web threat intelligence?

Why is threat intelligence important, and how does it benefit organizations to know what is currently happening on the dark web?

In general, threat intelligence provides more information so you can make better security decisions. By knowing more about the tools and techniques of an adversary, organizations can better protect themselves. Finally, threat intelligence provides context for your complete security posture.

Threat intelligence pertaining to dark web marketplaces and forums is also important because of what you might discover at any time. On dark markets, threat researchers may see the sale or trade of malicious software, zero-day exploits, large data dumps or the sale of intellectual property. It is here in the dark web — in marketplaces and private forums — where threat researchers often first hear of the latest malware and cybercrime services.

## What's new on the dark web?

- Turnkey, ecommerce service for setting up illicit, digital storefronts on underground markets
- Full identity packets on businesses for sale (a.k.a. business fullz)
- A Hacker University opens its doors
- Stolen financial loan applications for sale — chock full of personal identifiable information (PII)
- Dark web advertising, news and hacker reviews

Throughout the digital storefronts of these dark markets, Armor's security researchers found that many of the illicit products and services outlined in the 2018 and 2019 reports remain staples in these criminal markets. They include Remote Desktop Protocol (RDP) credentials and an array of malware. Popular cybercrime services continue to be advertised, such as offers to take down a competitor's website using a distributed denial of service (DDoS) attack or the availability of ransomware-as-a-service (RaaS).

There are several products and services that the TRU team spotted this year that are quite notable. The first was an offer to have a hacker "destroy a competitor's business." And, as if there are not already enough cybercriminals participating in illegal activities, there is a turnkey ecommerce service that provides fraudsters with everything they need to set up their own shops in an underground market.

Also, for the newbies just breaking into the cybercrime business, the TRU team discovered a growing ecosystem of advertisers, news sources and shady services catering to underground buyers. One of the most worrisome items the TRU team saw this year was an array of business fullz for sale. Business fullz are data files containing everything a criminal needs to appear as if they are a corporate officer of an actual business.

There are also SMS bombing services and commercial software for rent. And if newbies are looking for a "formal" cybercrime education, they can now attend Hacker University. For \$125, to be paid in bitcoin or monero, the criminal group behind this online university claims that it will teach attendees everything from operational security and Wi-Fi hacking to network attacks and carding.

# Price list for hackers, goods and services

Here are examples of the fees for popular hacking services available on the dark web:

Business Fullz data	
Includes: bank acct numbers, employee identification number (ein), certificate of business, corporate officers' names, birth dates, SSN.)	\$35-60

Ransomware	
Various generic ransomware	\$1.99-6.50

Unhacked remote desktop protocol servers	
Unhacked RDP servers worldwide	\$9.99-25 per server

Degree from Hacker University	
Hacker University degree	\$125

Various Malware	
Type	Average
Various virus packs	\$2.68-4.99
Remote Access Trojan (RAT)	\$.99-12
Cryptex Crypter	\$.99
TinyNuke bank botnet source code	\$75
Mirai botnet source code	\$6
Drupal exploit	\$80
(SMS stealer)	\$4.99-9.99

DDoS Attack	
DDoS a small website	\$100
DDoS a medium website	\$250

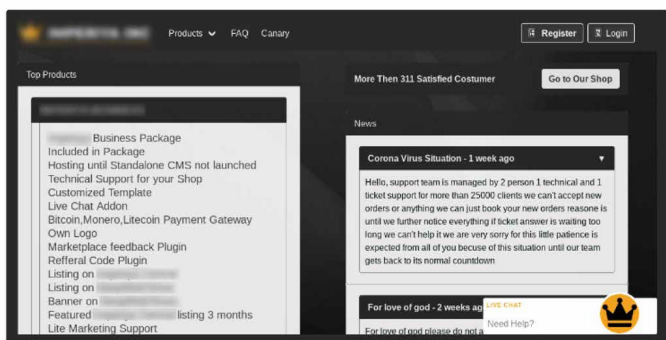


# Cybercrime Services

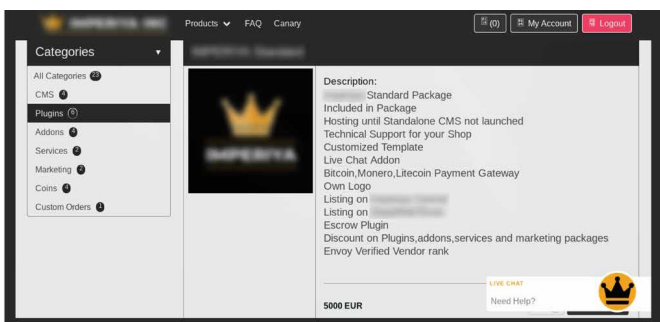
## A turnkey, eCommerce service for dark web vendors

One of the most interesting services spotted is a complete turnkey eCommerce service that allows dark web sellers to establish their own digital shop on an underground marketplace. The vendor, who boasts 240 customers, offers four levels of services: standard, business, plus and ultimate.

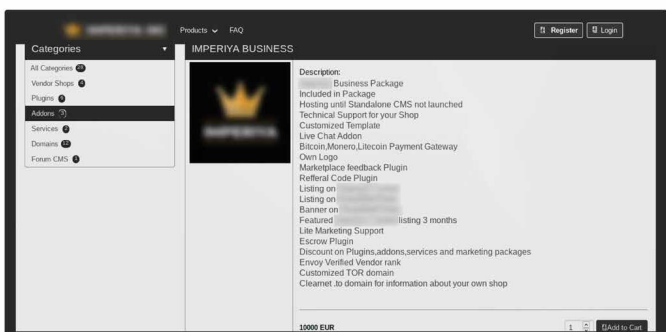
The standard package includes website hosting services, technical support, an escrow plug-in and cryptocurrency payment gateways for €5,000 (euro). The second level is a business package for €10,000 that includes light marketing support that packages together a banner ad, a featured listing on dark web news sites and a verified vendor rank. In addition, vendors can purchase plug-ins for features such as a lottery wheel. The plus package includes medium-grade marketing support, while the ultimate package provides services “at the highest priority.” The all-in-one service is similar to those offered by legitimate eCommerce agencies.



A dark web, turnkey, eCommerce services vendor provides cybercriminals with the key elements needed to set up a dark market shop online.



The vendor package for €5,000 includes web hosting, payment gateways, technical support, and an escrow plug-in.

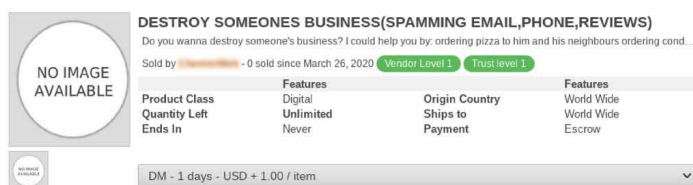


Business package for €10,000 includes standard features, support and promotions.

## Cybercrime-as-a-Service: destroy a business and DDoS

As the TRU team saw last year, there continues to be heavy rotation of advertisements from hackers offering a list of eyebrow-raising, illegal services such as offers to destroy a business or carry out DDoS attacks. This illustrates a significant development in the dark market: that cybercrime-as-a-service allows those with limited technical skills to participate in very lucrative hacking schemes.

With professionally designed websites, easy-to-use tools and customer service functions such as live chats and video tutorials, cybercriminals have developed effective models to expand their business. There are even underground markets that allow potential employers to leave money in escrow for use in recruiting other hackers.



The hacker sells this service for only \$185 and brags that “after 2 days of doing these type of things, his business will be ruined!”

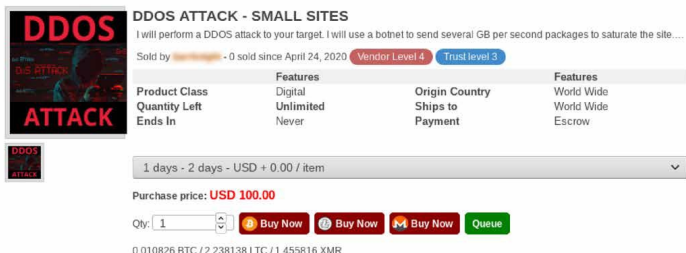
## Destroy a business

One of the most alarming services the TRU team discovered on the dark web is a vendor offering to destroy an individual’s business by hitting them with a barrage of spam emails and phone calls, shipping unwanted items to the victim’s business and including their business phone number in advertisements.

## DDoS services

DDoS services continue to be popular. One vendor advertises that he will DDoS a small website for \$100 and medium websites for \$250. He even brags that his DDoS tools can bypass the DDoS protection offered by the web security companies Cloudflare® and BlazingFast.

DDoS services, email spamming and ransomware-as-a-service continue to be offered by organized cybercriminal organizations on dark net markets.



**DDOS ATTACK - SMALL SITES**  
I will perform a DDOS attack to your target. I will use a botnet to send several GB per second packages to saturate the site...

Sold by [Vendor Level 4] - 0 sold since April 24, 2020 [Trust level 3]

	Features	Origin Country	Features
Product Class	Digital	World Wide	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

1 days - 2 days - USD + 0.00 / item

Purchase price: **USD 100.00**

Qty: 1 [Buy Now] [Buy Now] [Buy Now] [Queue]

0.010826 BTC / 2.238138 LTC / 1.455816 XMR

DDoS attacks are offered by size and duration of attack.



**DDOS ATTACK - MEDIUM SITES**  
NEW PRICES!!!! I will perform a DDOS attack to your target. I will use a botnet to send several GB per second packages to...

Sold by [Vendor Level 4] - 0 sold since March 03, 2020 [Trust level 3]

	Features	Origin Country	Features
Product Class	Digital	World Wide	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

1 days - 3 days - USD + 0.00 / item

Purchase price: **USD 250.00**

Qty: 1 [Buy Now] [Buy Now] [Buy Now] [Queue]

0.027066 BTC / 5.595345 LTC / 3.639540 XMR

DDoS services offer to send “several GB per second packages to saturate the target site.”

## Bulletproof web hosting services

Just as threat actors need software to conduct business, they also need reliable IT infrastructure in which to host their malware, botnets, spam and phishing sites, among other things. Where do they go to rent this infrastructure? They typically look for web hosting companies that don't mind working with criminals — those involved in everything from cybercrime to online gambling. Naturally, the criminals don't want to be asked questions about what they are hosting on the servers, and they want to feel confident that their IT infrastructure will stay online and will not be taken down by the hosting provider should the company receive an abuse report.

This type of hosting service is referred to as “bulletproof hosting” for the way it can largely withstand scrutiny. The cost of services can range between \$4 and \$19 per month, and bulletproof hosting companies can be found in any country. However, many of them are located in China, Russia and many of the countries that formerly made up the Soviet Union and now part of the Commonwealth of Independent States (CIS), such as Ukraine and Belarus.

## Commercial software for rent

Looking to rent expensive software for a specific project? Look no further. The TRU team saw cybercriminals mimicking the offerings of many legitimate software-as-a-service providers, but at a much lower rate. One vendor is selling a license for one user to the 2019 version of Adobe® Premiere Pro (a program for video editing) for \$5.67, and another vendor is selling a single-user license to Adobe Creative Suite Master Collection CS6 with 18 different popular Adobe products.

Several other threat actors are advertising that they will sell access to popular software applications for \$250 per day and up to \$1,000 for three months of access. However, one threat actor does not list the specific applications, but rather requests that interested buyers send a private message to find out the types of software available.

- \$250 for 1 week of activation
- \$500 for 1 month of activation
- \$1,000 for 3 months of activation

# Underground marketplace products

When it comes to the variety and the amount of illicit goods on the underground markets, Armor's findings illustrate that the cybercriminals participating in these businesses are resilient, innovative and agile. They are constantly coming up with creative ways to sell their goods and to monetize any type of data.

## Hackers add business fullz to their repertoire

While personal fullz continue to be one of the most popular items on the dark market, recently hackers have added "business fullz" to their repertoire.

For comparison, personal fullz are packets of information about individuals. They contain all kinds of Personal Identifiable Information (PII) on an individual. Personal fullz typically contain the victim's full name, social security number, date of birth, phone number, address, driver's license and mother's maiden name — everything a criminal needs to commit identity theft.

Similarly, business fullz contain everything a criminal needs to appear as if they are a corporate officer of an actual business. One vendor states that his business fullz contains a corporate officer's credit score (promised to be in a range from 700 to 850), certificate of business, bank account numbers, and Employee Identification Number (EIN), also known as a Tax Identification Number. An EIN is a unique, nine-digit number assigned by the IRS to business entities operating in the U.S. for the purposes of opening a bank account or filing tax returns.

The business fullz also come with background report and the Social Security Numbers (SSN), full names and birthdays of the corporate officers. The seller also promises that the businesses do not have credit locks. Business fullz cost between \$35 and \$60 depending on the seller.

What can a cybercriminal do with this packet of valuable business documents? As billions of dollars in small business loans flowed to organizations during the COVID-19 crisis, the TRU team believes this type of information potentially helped criminals apply for these small business loans, as well as standard business loans, lines of credit and high-limit credit cards. Cybercriminals can also use this information to help stage business email compromise schemes and open business bank accounts, enabling them to move larger amounts of money into and out of the accounts, without drawing unwanted attention to their activities.



**\*UPDATE\* High Quality Business Fullz fulls w/ bank account #s and documents**  
NEW UPDATE! Information included: Company name address owner owner phone email tax exempt # Federal ID numbe...  
Sold by [redacted] - 408 sold since November 27, 2018 Vendor Level 5 Trust level 5  
12 items available for auto-dispatch

Product Class	Features	Origin Country	Features
Digital	Digital	United States	United States
Quantity Left	16	Ships to	World Wide
Ends In	Never	Payment	Escrow

Bulk Discount	Bulk Discounts	Price	
Bulk Discount	From qty 5 to 9	USD 25.00	0.00270543 BTC
Bulk Discount	From qty 10 to 79	USD 20.00	0.00216435 BTC

default - 1 day - USD + 0.00

Purchase price: **USD 35.00**

Underground criminals advertise business fullz, a packet of key, identifying information about a business and its owner(s) or corporate officers, so that scammers can commit fraud against the business, such as applying for bank loans, setting up money mule accounts, etc.

## Tools of cybercrime trade:

### Crypters, remote access trojans (RATs) and exploit kits

On marketplaces and in forums, malicious software is one of the key items being sold along with access to hijacked servers, botnets and individual computers. Among the most popular tools of the cybercrime trade are remote access trojans (RATs), exploit kits and crypters. A crypter is software that can encrypt and obfuscate malware, making it undetectable to some antivirus programs. RATs continue to be popular because they can give cybercriminals complete access to a victim's computer, just as if they had physical access to the device. With this access, the cybercriminal can access the victim's files, their camera and even turn on or off their device. The TRU team saw a variety of RATs advertised on the underground markets ranging from \$1 to \$12.

Exploit kits used to be very popular in the underground. An exploit kit is a type of toolkit packaged with exploits that cybercriminals use to attack vulnerabilities in commonly installed software, such as Internet Explorer and Adobe Flash Player. Their goal is to successfully compromise the computer system so they can distribute malware onto the device. Exploit kits are typically designed to be modular and are updated to add newer exploits to replace the older exploits. Some threat actors sell complete kits outright, while others rent their kits on weekly or monthly terms. These rental fees can range from \$800 to \$2,000 per month. The TRU team is also seeing threat actors sell individual exploits. One cybercriminal is offering to sell an exploit for the popular Drupal content management system for \$80. He claims it can successfully exploit Drupal version 7 and 8.



## Remote desktop protocol credentials – get ‘em while they’re hot!

One of the ways cybercriminals are infecting organizations with ransomware and other malware is by targeting open Remote Desktop Protocol (RDP) servers. These hackers will scan the internet for “open” internet-facing servers that are running the RDP service. An RDP service is commonly used by organizations so that employees can log into office computers remotely. The service also allows IT administrators to perform software installations, PC maintenance, computer troubleshooting, printer setup and email setup, among other activities.

When cybercriminals detect open RDP servers, they will utilize a brute-force, password-spray attack in an attempt to log into the server using common or default usernames such as “administrator,” along with multiple, commonly used passwords. Once the threat actors have obtained working credentials, they simply use it as a pivot point for lateral movement into other areas of the network, and proceed to steal data and install ransomware or other malware onto targeted machines.

As in 2019, the TRU team found cybercriminals offering to sell credentials to publicly available RDP servers. These credentials have grown widely popular, and there are countless dark market vendors selling them with an average price of between \$16 and \$25 apiece.

**+++ Super RDP | USA | EU +++ Not hacked !**  
 HM Super RDP Service Hello everybody! We are selling new RDP | Proxy | socks5 for 1 month ( you can renew it later if y...  
 Sold by [Vendor] - 25 sold since February 01, 2019 Vendor Level 4 Trust level 3 D 9400 4.82

	Features	Origin Country	Features
Product Class	Digital	World Wide	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Silver RDP Regular RDP with admin access - 1 days - USD + 1.00 / item

Purchase price: **USD 16.00**

Qty: 1 Buy Now Buy Now Buy Now Queue

0.001733 BTC / 0.370456 LTC / 0.249454 XMR

**--- RDP with Admin Access - WORLDWIDE ---**  
 =====WELCOME===== Have worldwide RDPs which are very useful for different carding method...  
 Sold by [Vendor] - 379 sold since March 28, 2018 Vendor Level 5 Trust level 4

	Features	Origin Country	Features
Product Class	Digital	World Wide	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Rdp with admin access RANDOM COUNTRY LEAVE NOTE EMPTY NO USA - 1 days - USD + 0.00 / it▼

Purchase price: **USD 9.99**

Qty: 1 Buy Now Buy Now Buy Now Queue

0.001083 BTC / 0.231304 LTC / 0.155948 XMR

**Atlanta, GA - Non hacked RDP Service or VPS. RDP server**  
 BIGGEST RDP VENDOR SINCE ALPHABAY! PLEASE SPECIFY IN THE ORDER NOTES IF YOU WANT WINDOWS 7, WI...  
 Sold by [Vendor] - 5 sold since April 23, 2019 Vendor Level 2 Trust level 1

	Features	Origin Country	Features
Product Class	Digital	World Wide	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Linux GUI - 1 days - USD + 10.00 / item

Purchase price: **USD 25.00**

Qty: 1 Buy Now Buy Now Buy Now Queue

0.002710 BTC / 0.578838 LTC / 0.390259 XMR

**Non-hacked RDP credentials, guaranteed not to have been used previously, are advertised for the U.S., Europe and other parts of the world.**



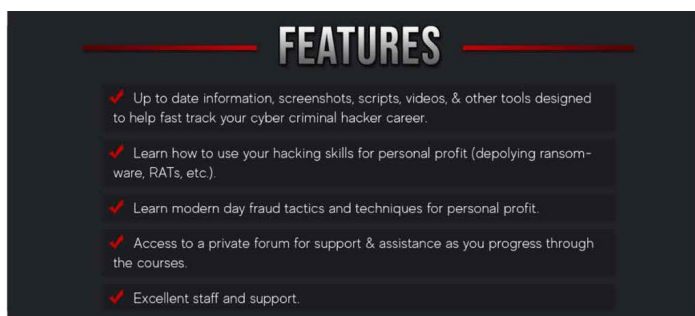
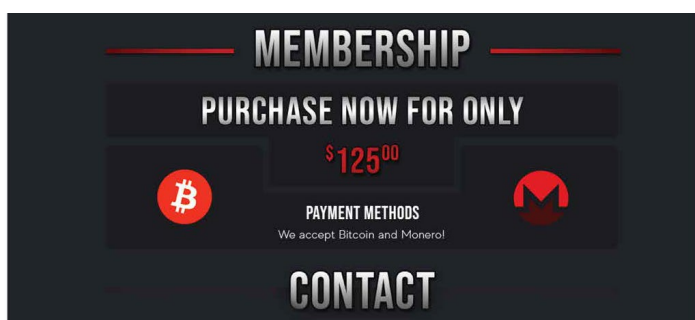
## Get your degree at Hacker University

Video tutorials and instruction guides on how to commit an array of different kinds of cybercrime, from PayPal cashouts to creating bank drops and identity fraud, continue to be peddled on the underground for only \$10 each. One seller boasts in their ad: “Earn \$1,000s every day. We have guides on just about EVERYTHING!!!”

However, one criminal group is offering a much better option than do-it-yourself instruction guides. They have established what they call “Hacker University.” They are selling memberships for \$125, to be paid in bitcoin or monero.

For this one low fee, Hacker University purportedly offers members courses on everything from operational security and Wi-Fi hacking to network attacks and carding.

Creators of the site advertise that they want to “teach people about cybercrime and how to become a professional cybercriminal. By taking the course offered you will gain the knowledge and skills needed to hack an individual or company successfully with whatever malware you have at your disposal.” They offer training to those who want to become “hackers, fraudsters, dark market vendors and people who want to remain anonymous online.”



Hacker University courses include Wi-Fi hacking, network attacks and carding.

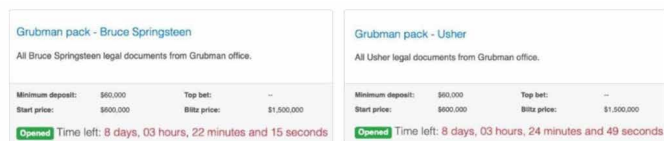
## Hacker University advertises topics such as:

- How to access the router admin panel
- How to find proper targets once in the network
- Router exploitation
- Printer exploitation
- How to brute force a router admin panel
- Getting up-to-date on current MITM attacks
- How to perform MITM attacks
- All scripts and programs provided

There is also a planned section where members will be able to purchase malware including: ransomware, remote access trojans (RATs), crypters, password stealers and keyloggers.

## Ransomware evolves to be more heinous

Throughout 2019 and the first half of 2020, Armor identified more than 380 publicly reported ransomware attacks on public U.S. organizations.



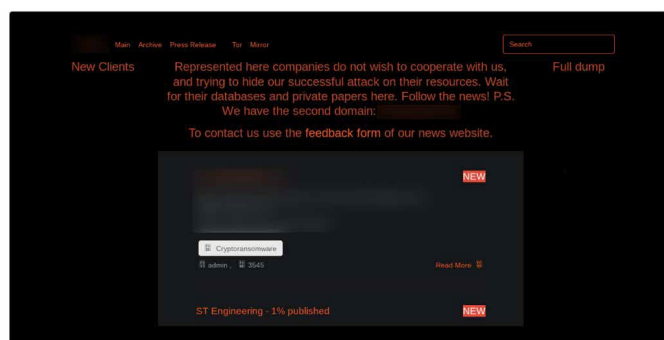
Grubman pack - Bruce Springsteen		Grubman pack - Usher	
All Bruce Springsteen legal documents from Grubman office.		All Usher legal documents from Grubman office.	
Minimum deposit: \$50,000	Top bid: --	Minimum deposit: \$50,000	Top bid: --
Start price: \$500,000	Bidder price: \$1,500,000	Start price: \$500,000	Bidder price: \$1,500,000
Opened	Time left: 8 days, 03 hours, 22 minutes and 15 seconds	Opened	Time left: 8 days, 03 hours, 24 minutes and 49 seconds

Ransomware data was offered for sale on the Sodin website on July 10, 2020.

In November 2019, cybercriminals added yet another lethal element to their ransomware schemes, causing ransomware attacks to become an even bigger problem for its victims.

Threat actors began creating copies of each victim organization's data before encrypting it. Next, they threatened to publish portions of the data and sell it to other criminals or simply give it away if the ransom wasn't paid. Security staffing firm Allied Universal was the first organization to experience this additional form of extortion. The ransomware attackers demanded \$3.8 million after Allied missed two payment deadlines. The threat actors did release some of Allied's data on the internet and threatened to give all of it to WikiLeaks.

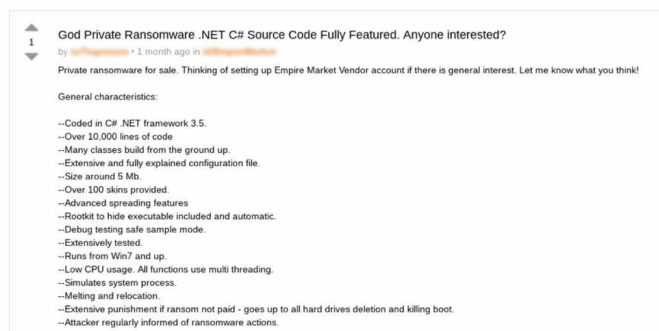
By May 2020, a ransomware attack using this approach had demanded a record \$42 million ransom payment from celebrity law firm Grubman Shire Meiselas & Sacks. There have been no public reports about whether or not the law firm paid the ransom. The threat actors behind the attack, called Sodin, reported that it was holding thousands of the law firm's documents hostage — allegedly including private information on Lady Gaga, Madonna, Nicki Minaj, Bruce Springsteen, Mary J. Blige, Christina Aguilera and Mariah Carey. The digital kidnappers increased their demand for payment to \$42 million — double their initial \$21 million ask — when the firm failed to respond. The group also threatened to publicly release more data if it wasn't paid within a week. On July 10, 2020, the ransomware gang kicked off a week-long auction of items purportedly containing data of Springsteen, Usher, Minaj, Carey, Jessica Simpson and LeBron James with a "buy now price" of \$1.5 million for each cache.



The Maze website lists its purported victims and samples of each victim's data.

Ransomware groups such as Sodin, Maze, Nemty, Lockbit and Doppelpaymer have all openly taken part in this new extortion tactic. The group behind Maze hosts a website that announces its latest victims and includes samples of stolen files to show it means business. Regular press releases by the group bully victims into paying. Few victims listed on the site have publicly reported a ransomware attack.

Ransomware itself continues to be offered as a stand-alone software product, and also sold as a service. There are also close-knit ransomware gangs that recruit affiliates who can work with them to launch attacks.



A threat actor provides details on an underground forum about a specific type of ransomware he claims to have developed, and wants to determine the interest level from prospective buyers.

## Conclusion

Dark, underground or shadow economy markets have been in existence for decades. They rise and fall with world events, filling the demand for goods and services that might otherwise be unavailable. Unfortunately, they attract many people who are not interested in earning a legitimate living. Dark web markets are no different, but they present new challenges.

Following the U.S. recession that started in 2007, the U.S. shadow economy grew to an estimated 5.4% of Gross Domestic Product (GDP) — or \$2.7 trillion. Following times of economic turmoil, including recessions, wars or natural disasters, shadow economies thrive.

Armor and Rackspace Technology believe this will hold true for dark web markets as cybercriminals are motivated by economic uncertainty, emboldened by the success of recent cyberattacks and obscured by the chaos of a global pandemic. Thus, it is more important than ever for organizations and individuals to implement proven and comprehensive security practices.

# How Rackspace Technology helps

When it comes to navigating the dark market, you don't have to go it alone. At Rackspace Technology, we work as an extension of your security team, helping you stay ahead of cybersecurity threats before they impact your business with 24x7x365 support from certified security analysts in our global Security Operations Centers (SOC). Our global team of 400+ network and security experts has earned 500+ industry certifications — including CCNAs and GIACs in cyber defense, penetration testing, digital forensics and incident response.

We partner with you every step of the way in your cloud security journey. We start by assessing your current posture against industry benchmarks and then design, build, manage and optimize a defense-in-depth architecture for unified protection across your multicloud environments. Our offerings include:

- **SOC-as-a-Service:** Reduce your risk with security experts who monitor the security posture of your multicloud environments, and provide rapid detection and response of threats before they impact your business.
- **Global SOC presence:** Our modern, full-service SOCs are located in San Antonio and London, with GIAC Certified Incident Handlers (GCIH) available around-the-clock.
- **Zero trust and network security:** Secure your infrastructure stack from malicious intrusion and unauthorized access — providing granular protection and control from the cloud to the network, application and data layers.
- **Application security:** Protect and improve the performance of your web and mobile applications, and DevSecOps solutions by building security and speed into the development of your cloud-native apps from the start.
- **Professional Services:** To help you identify security gaps, we offer a range of assessments to identify risks in your environment and to provide recommended actions to meet the security and compliance mandates that are important to your business, such as FFIEC, GLBA, PCIDSS, HIPAA, HITECH, FedRAMP, FISMA, DFARS, ISO and SOC2.

Rackspace Technology remains dedicated to being a leader in helping our customers protect their digital investments, while helping to ensure security resiliency and compliance, enabling more predictable business outcomes and underwriting transformation benefits.

## Take our cybersecurity risk self-assessment

Did you know that 52% of organizations have experienced security breaches in the past 12 months? On average, 206 days pass before a breach is detected. And the average cost to address the breach? \$3.2 million.<sup>1</sup>

Take our 15-question Cybersecurity Risk Self-Assessment to help identify some common security gaps in your environment that you may not be aware of. After completing the assessment, you'll receive a professional consultation with a cloud expert. They will review your results and make best-practice recommendations on how you can address any security gaps in your business.

### Take your assessment today.

Visit [www.rackspace.com/security](http://www.rackspace.com/security) or call 1-800-961-2888 today.

1. 2019 Forrester Analytics Global Business Technographics® Security Survey

© 2021 Rackspace US, Inc. :: Rackspace®, Fanatical Support®, Fanatical Experience™ and other Rackspace marks are either service marks or registered service marks of Rackspace US, Inc. in the United States and other countries. All other trademarks, service marks, images, products and brands remain the sole property of their respective holders and do not imply endorsement or sponsorship.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS A GENERAL INTRODUCTION TO RACKSPACE TECHNOLOGY SERVICES AND DOES NOT INCLUDE ANY LEGAL COMMITMENT ON THE PART OF RACKSPACE TECHNOLOGY.

You should not rely solely on this document to decide whether to purchase the service. Rackspace Technology detailed services descriptions and legal commitments are stated in its services agreements. Rackspace Technology services' features and benefits depend on system configuration and may require enabled hardware, software or additional service activation.

Except as set forth in Rackspace Technology general terms and conditions, cloud terms of service and/or other agreement you sign with Rackspace Technology, Rackspace Technology assumes no liability whatsoever, and disclaims any express or implied warranty, relating to its services including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, and noninfringement.

Although part of the document explains how Rackspace Technology services may work with third party products, the information contained in the document is not designed to work with all scenarios. any use or changes to third party products and/or configurations should be made at the discretion of your administrators and subject to the applicable terms and conditions of such third party. Rackspace Technology does not provide technical support for third party products, other than specified in your hosting services or other agreement you have with Rackspace Technology and Rackspace Technology accepts no responsibility for third-party products.

Rackspace Technology cannot guarantee the accuracy of any information presented after the date of publication.

Rackspace-Report-Dark-Market-Report-A-New-Economy-SEC-TSK-4330 :: April 16, 2021