Logins for 1.3 million Windows RDP servers collected from hacker market

bleepingcomputer.com/news/security/logins-for-13-million-windows-rdp-servers-collected-from-hacker-market/

Lawrence Abrams

By
Lawrence Abrams

- April 21, 2021
- 11:15 AM
- 3

connect to address 192.168.1.1
username: **********
password: ************
Access granted...
exited after 0.006146 seconds with return value
any key to continue . . .

The login names and passwords for 1.3 million current and historically compromised Windows Remote Desktop servers have been leaked by UAS, the largest hacker marketplace for stolen RDP credentials.

With this massive leak of compromised remote access credentials, researchers, for the first time, get a glimpse into a bustling cybercrime economy and can use the data to tie up loose ends on previous cyberattacks.

Network admins will also benefit from a new service launched by cybersecurity firm Advanced Intel called RDPwned that allows organizations to check whether their RDP credentials have been sold in the marketplace.

What's so special about RDP?

Remote Desktop Protocol (RDP) is a Microsoft remote access solution that allows users to remotely access a Windows device's applications and desktop as if they were sitting in front of the computer.

Due to its prevalent use in corporate networks, cybercriminals have built a thriving economy around selling the stolen credentials for RDP servers.

While you may think that access to a corporate network would be expensive, the reality is that threat actors sell remote desktop accounts for as little as $3 and typically not more than $70.

Once a threat actor gains access to a network, they can perform a variety of malicious activities. These activities include spreading further throughout the network, stealing data, installing point-of-sale (POS) malware to harvest credit cards, installing backdoors for further access, or deploy ransomware.

The use of Windows Remote Desktop Services to breach networks is so pervasive that the FBI has stated that RDP is responsible for 70-80% of all network breaches leading to ransomware attacks.

While all ransomware groups utilize RDP to some extent, one ransomware group known as Dharma is known to predominantly use remote desktop to gain a foothold in corporate networks.

UAS, the largest marketplace for RDP credentials

UAS, or 'Ultimate Anonymity Services,' is a marketplace that sells Windows Remote Desktop login credentials, stolen Social Security Numbers, and access to SOCKS proxy servers.

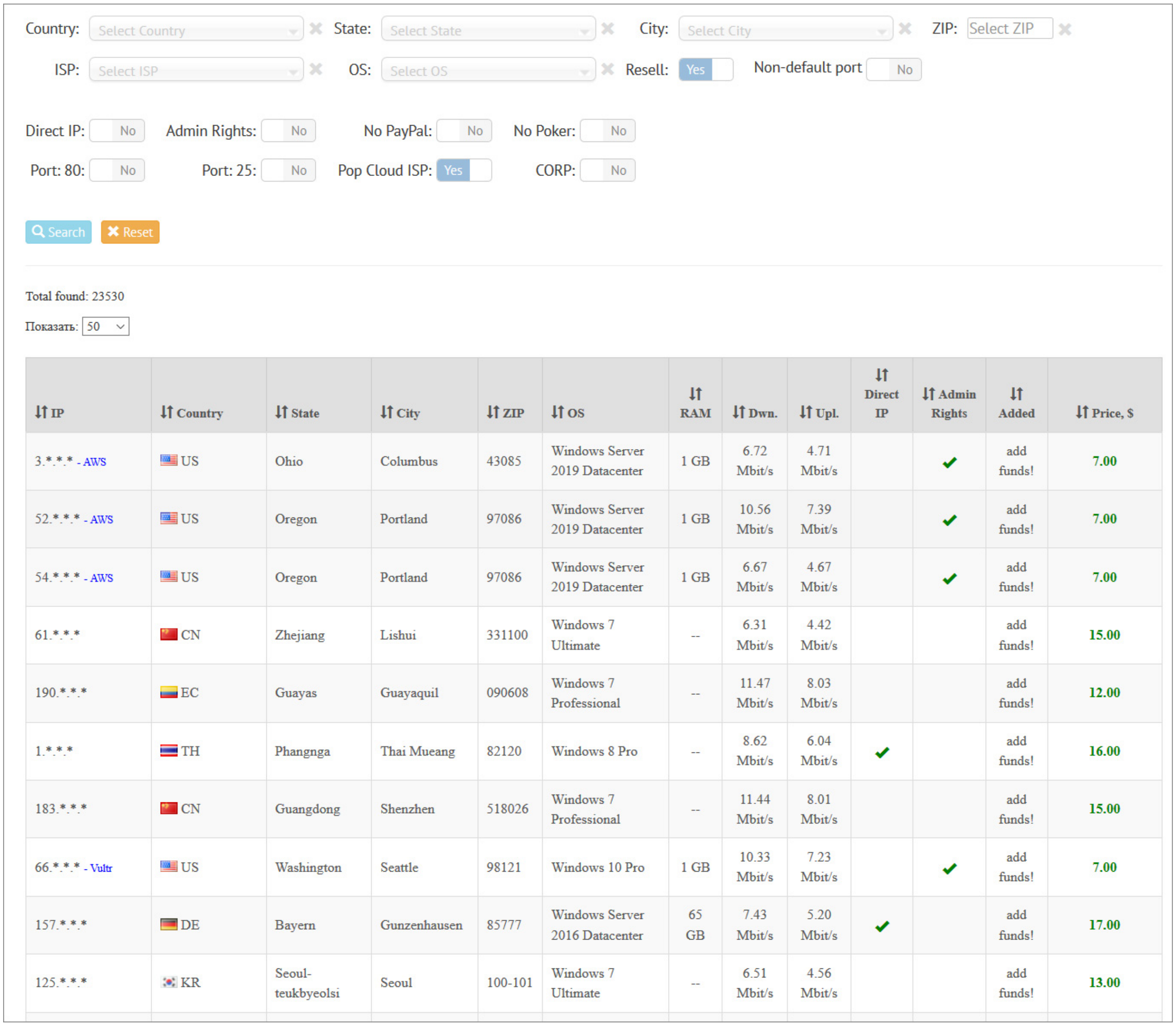
What makes UAS stand out is that it is the largest such marketplace, performs manual verification of sold RDP account credentials, offers customer support, and provides tips on how to retain remote access to a compromised computer.

"The market functions partially like eBay - a number of Suppliers work with the market. They have a separate place to log in and upload the RDPs they hacked. The system will then verify them, collect information about each one (os, admin access? internet speed, cpu, memory etc etc), which is added to the listing."

"The supplier interface provides real time stats for the suppliers (what sold, what didn't, what was sold but a refund was asked for, etc)."

"They also provide support if for some reason what you bought doesn't work. They do take customer support seriously," a security researcher who wishes to remain anonymous told BleepingComputer.

When purchasing stolen RDP accounts, threat actors can search for compromised devices in a particular country, state, city, zip code, ISP, or operating system, allowing them to find the specific server they need.



Country: Select Country ✖ State: Select State ✖ City: Select City ✖ ZIP: Select ZIP ✖

ISP: Select ISP ✖ OS: Select OS ✖ Resell: Yes Non-default port No

Direct IP: No Admin Rights: No No PayPal: No No Poker: No

Port: 80: No Port: 25: No Pop Cloud ISP: Yes CORP: No

Search Reset

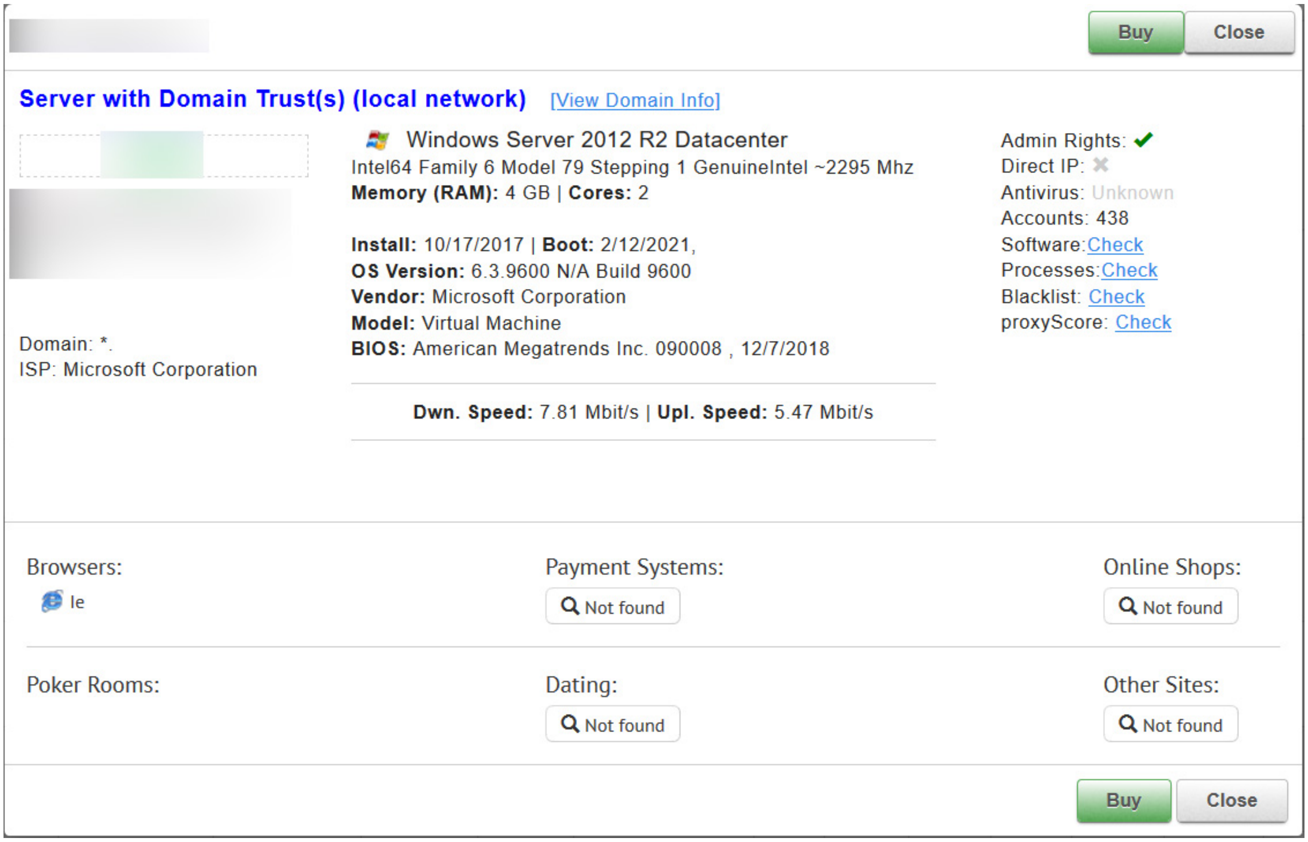
Total found: 23530

Показать: 50

IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
3.*.*.* - AWS	US	Ohio	Columbus	43085	Windows Server 2019 Datacenter	1 GB	6.72 Mbit/s	4.71 Mbit/s		✓	add funds!	7.00
52.*.*.* - AWS	US	Oregon	Portland	97086	Windows Server 2019 Datacenter	1 GB	10.56 Mbit/s	7.39 Mbit/s		✓	add funds!	7.00
54.*.*.* - AWS	US	Oregon	Portland	97086	Windows Server 2019 Datacenter	1 GB	6.67 Mbit/s	4.67 Mbit/s		✓	add funds!	7.00
61.*.*.*	CN	Zhejiang	Lishui	331100	Windows 7 Ultimate	--	6.31 Mbit/s	4.42 Mbit/s			add funds!	15.00
190.*.*.*	EC	Guayas	Guayaquil	090608	Windows 7 Professional	--	11.47 Mbit/s	8.03 Mbit/s			add funds!	12.00
1.*.*.*	TH	Phangnga	Thai Mueang	82120	Windows 8 Pro	--	8.62 Mbit/s	6.04 Mbit/s	✓		add funds!	16.00
183.*.*.*	CN	Guangdong	Shenzhen	518026	Windows 7 Professional	--	11.44 Mbit/s	8.01 Mbit/s			add funds!	15.00
66.*.*.* - Vultr	US	Washington	Seattle	98121	Windows 10 Pro	1 GB	10.33 Mbit/s	7.23 Mbit/s		✓	add funds!	7.00
157.*.*.*	DE	Bayern	Gunzenhausen	85777	Windows Server 2016 Datacenter	65 GB	7.43 Mbit/s	5.20 Mbit/s	✓		add funds!	17.00
125.*.*.*	KR	Seoul-teukbyeolsi	Seoul	100-101	Windows 7 Ultimate	--	6.51 Mbit/s	4.56 Mbit/s			add funds!	13.00

RDP servers currently sold on the UAS marketplace

Potential buyers can dig down deeper on each server to see the number of Windows accounts, the Internet connection speed, the server's hardware, and more, as shown below.



Server with Domain Trust(s) (local network) [View Domain Info]

Windows Server 2012 R2 Datacenter
Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 Mhz
Memory (RAM): 4 GB | **Cores:** 2

Install: 10/17/2017 | **Boot:** 2/12/2021,
OS Version: 6.3.9600 N/A Build 9600
Vendor: Microsoft Corporation
Model: Virtual Machine
BIOS: American Megatrends Inc. 090008 , 12/7/2018

Dwn. Speed: 7.81 Mbit/s | **Upl. Speed:** 5.47 Mbit/s

Admin Rights: ✓
Direct IP: ✗
Antivirus: Unknown
Accounts: 438
Software: Check
Processes: Check
Blacklist: Check
proxyScore: Check

Domain: *.
ISP: Microsoft Corporation

Browsers: Ie
Payment Systems: Not found
Online Shops: Not found
Poker Rooms:
Dating: Not found
Other Sites: Not found

RDP server specs for potential buyers

BleepingComputer was told that the marketplace will not sell any servers located in Russia or a Commonwealth of Independent States (CIS) country and runs a script that automatically removes any that are found.

Even with this filtering of servers, UAS is currently selling a massive 23,706 RDP credentials.

Secretly monitoring the UAS marketplace

Since December 2018, a group of security researchers have had secret access to the database for the UAS marketplace and have been quietly collecting sold RDP credentials for almost three years.

During this time period, the researchers have collected the IP addresses, usernames, and passwords, for 1,379,609 RDP accounts that have been sold at UAS since the end of 2018.

This database had been shared with Advanced Intel's Vitali Kremez, who also shared a redacted copy with BleepingComputer to review.

While we will not be listing any of the companies found in the database, we can say that the listed RDP servers are from all over the world, including government agencies from sixty-three countries, with Brazil, India, and the United States being the top three.

There are also RDPs servers for many well-known, high-profile companies, with many servers from the healthcare industry.

Furthermore, BleepingComputer has found **many** RDP servers in the database that belong to organizations known to have suffered ransomware attacks over the past two years.

After analyzing the 1.3 million accounts in the database, BleepingComputer has pulled out some interesting data that should be useful for all computer users and network admins:

- The top five login names found in the sold RDP servers are '**Administrator**', '**Admin**', '**User**', '**test**', and '**scanner**'.
- The top five passwords used by the RDP servers are '**123456**', '**123**', '**P@ssw0rd**', '**1234**', and '**Password1**'.
- The top five represented countries in the database are **United States**, **China**, **Brazil**, **Germany**, **India**, and the **United Kingdom**.

More complete stats are found at the end of the article.

RDPwned: Checking if your RDP is compromised

Vitali Kremez has launched a new service called RDPwned that allows companies and their admins to check if their servers are listed in the database.

"The marketplace is tied to a number of high-profile breaches and ransomware cases across the globe. A number of ransomware groups are known to purchase initial access on UAS. This treasure trove of adversary-space data provides a lens into the cybercrime ecosystem, and confirm that low hanging fruit, such as poor passwords, and internet-exposed RDP remain one of the leading causes of breaches,"

"RDPwned will also help illuminate old breaches for which they never figured out initial access. For others, it will give them a chance to resolve the security problem before it becomes a breach," Kremez told BleepingComputer.

To use the service, Kremez told BleepingComputer that companies would need to submit contact information from an executive or admin of the company, which Advanced Intel will vet.

Once the user's identity is verified, Advanced Intel will confirm if their company's servers are listed in RDPwned.

Visitors can perform this lookup via reverse DNS, IP addresses, and domain names.

Further statistics

Below are additional statistics showing the top 20 login names, top 20 passwords, and top 10 countries found in the 1.3 million RDP servers that UAS has listed on the marketplace.

Top 20 login names

Used login name	Total accounts
Administrator	303,702
Admin	59,034
User	45,096
test	30,702
scanner	20,876
scan	16,087
Guest	12,923
IME_ADMIN	9,955
user1	8,631
Administrador	8,612
Trader	8,608
postgres	5,853
IME_USER	5,667
Usuario	5,236
user2	4,055
Passv	3,989
testuser	3,969
test1	3,888
server	3,754
student	3,592
reception	3,482
backup	3,356
openpgsvc	3,339
info	3,156

VPN	3,139

Top 20 passwords

Used password	Total accounts
123456	71,639
123	50,449
P@ssw0rd	47,139
1234	34,825
Password1	27,007
1	24,955
password	19,148
12345	16,522
admin	15,587
ffff-ffc0M456x (see note)	15,114
Admin@123	13,572
User	13,437
scanner	13,193
scan	10,409
test	10,169
Aa123456	9,399
Password123	8,756
12345678	8,647
Admin123	8,214
Passw0rd	7,817
admin,.123!@#$%^	7,027
1qaz@WSX	6,248
Welcome1	5,962

P@ssword64	5,522
abc@123	4,958

Note: The 'ffff-ffc0M456x' password appears to be a default password configured by the MailEnable setup program for remote access. Users are advised to change this password to something else.

Top 10 countries

Country	Total Accounts
United States	299,529
China	201,847
Brazil	119,959
Germany	56,225
India	41,588
United Kingdom	37,810
France	32,738
Spain	30,312
Canada	27,347
Hong Kong	24,804

Related Articles:

Microsoft shares mitigation for Windows KrbRelayUp LPE attacks

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Microsoft adds support for WSL2 distros on Windows Server 2022

Microsoft adds Office subscriptions to Windows 11 account settings

Darknet market Versus shuts down after hacker leaks security flaw

- Credentials
- Marketplace
- RDP
- Remote Desktop

- UAS
- Ultimate Anonymity Services
- Windows

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-
  TsVk! - 1 year ago
  -
  -

  All these years later and and people still struggle to make a password that wouldn't be guessed by a 10 year old. Never ceases to amaze.

-
  Wolverine 7 - 1 year ago
  -
  -

  Amazing,..maybe Gurdjieff was right,and everyones asleep,..

-

  Priyanka-agarwal - 2 months ago

  Great work. I think we should question whether is my RDP secure?
  According to Microsoft's research, the one simple action you can take to prevent 99.9% of the attacks on your accounts is to use multi-factor authentication (MFA).
  There are many solution providers in the market like RCDevs security solutions(free up to 40 users), duo, onelogin, etc.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: