SOPHOS

RDP Exposed - The Threat That's Already at Your Door

By **Matt Boddy**, **Ben Jones**, and **Mark Stockley**

Contents

Executive summary 2

Introduction 3

- The targeted ransomware playbook 4

Methodology 4

Findings 5

- Time to first login attempt 5
- Volume and frequency of login attempts 5
- A detection avoidance strategy? 7
- Source of attacks 9
- Login attempts and IP addresses by region 9
- Login attempts and IP addresses by country 9
- Types of attacks 10
- What's in a name? 13
- Top 5 usernames used in all failed login attempts 13
- Login attempts for localised versions of Administrator 14

Impact of Shodan 15

Conclusions 16

Appendix A 18

- Login attempts and IP addresses by country 18

Appendix B 18

- Top 15 usernames (all honeypots) 18

Appendix C 19

- Top 15 usernames (Ireland) 19

Appendix D 19

- Top 15 usernames (Ohio) 19

Appendix E 20

- Top 15 usernames (Frankfurt) 20

Appendix F 20

- Top 15 usernames (London) 20

Appendix G 21

- Top 15 usernames (Paris) 21

Appendix H 21

- Top 15 usernames (California) 21

Appendix I 22

- Top 15 usernames (Sao Paulo) 22

Appendix J 22

- Top 15 usernames (Sydney) 22

Appendix K 23

- Top 15 usernames (Mumbai) 23

Appendix L 23

- Top 15 usernames (Singapore) 23

Executive summary

RDP is the latest source of sleepless nights for sysadmins because of BlueKeep (CVE-2019-0708), a vulnerability so serious it could be used to trigger a ransomware outbreak spreading around the world and running through corporate networks in hours, like WannaCry.

But while companies race to patch BlueKeep in the expectation that criminals will eventually find a way to exploit it, another wolf is already at the door. RDP is already being abused, every day, to devastating effect.

Gangs of criminal hackers are using off-the-shelf software to find internet-connected computers running RDP, and then brute force guessing the passwords that allow them to walk into corporate networks and conduct crippling ransomware attacks. It's an approach that's so successful that the criminal gangs who conduct targeted ransomware attacks have almost entirely abandoned alternative methods of network entry.

Every day, the news carries fresh stories of enterprises, hospitals, factories, utilities, and city administrations brought to their knees by ransomware that found its target because of a cracked RDP password.

The research presented here sets out to quantify the global threat of RDP brute forcing by using a network of ten geographically diverse honeypots. By recording login attempts, the honeypots captured how quickly an unknown RDP server can be found by attackers, and how relentlessly those attackers will rattle its locks.

It shows that organizations that connect RDP-enabled computers to the internet can expect to be found within minutes, and subjected to an escalating number of simultaneous attacks from multiple attackers using a variety of tactics.

Between them, the honeypots received 4.3 million login attempts at rate that steadily increased through the 30 day research period. The first honeypot to be discovered was found in just one minute and twenty four seconds, the last in just 15 hours. They were visited by fly-by-night attackers looking for an opportunistic win, and by attackers settling in for the long haul, determined to crack an elusive administrator password.

For networks exposed to the internet via RDP there is no rest and no hiding place. BlueKeep may be around the corner but RDP password attacks are at your door, right now.

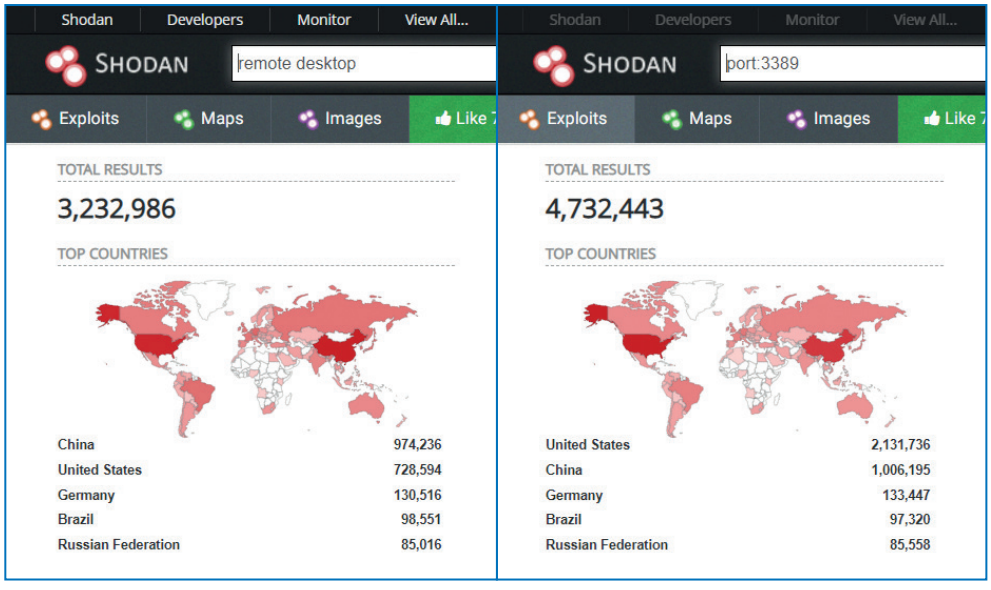
Introduction

RDS (Remote Desktop Services) is a Microsoft thin-client technology that allows remote users to access a computer over a network and control it using the Windows graphical user interface they're familiar with. Software clients connect to computers running RDS using RDP (the Remote Desktop Protocol).

RDS is a keystone technology for organizations that allows administrators to reach computers on remote networks or in the cloud and facilitates remote working for end users.

RDP doesn't have to be used over the internet, but it often is. At the time of writing, the Shodan search engine, which indexes online devices and their services, lists over three million results in a search for "remote desktop" and closer to five million when searching for devices accessible over port 3389. It's likely that the larger figure includes firewalls with port 3389 open but no active RDP server. The smaller figure may include RDP servers listening on ports other than port 3389, as well as any other services that return the string "remote desktop." Between them, the two searches suggest that the number of potential targets for RDP password guessing is in the millions.

Because attackers use compromised RDP servers as bridgeheads to invade entire networks, the total number of computers made vulnerable by the millions of internet-connected RDP servers is likely to be far higher.



This abundance of computers accessible via RDP, and the stubborn popularity of weak passwords, has made RDP a favorite point of entry for criminal hackers looking to break into corporate networks. In turn, this has fueled the development of a criminal market in stolen RDP credentials.

In recent years, criminals deploying targeted ransomware like BitPaymer, Ryuk, Matrix, and SamSam have almost completely abandoned other methods of network ingress in favor of using RDP. Gangs like these have the choice cracking passwords themselves using tools like NLBrute, buying passwords cracked by others, or buying accounts on compromised RDP servers.

The targeted ransomware playbook

	SAMSAM	DHARMA	MATRIX	BITPAYMER	RYUK
First appeared	2015	2016	2016	2017	2018
Active	No	Yes	Yes	Yes	Yes
Infection vector	RDP	RDP	RDP	RDP	RDP

It is likely therefore that any computer exposed to the internet via RDP is of interest to criminal hackers and the subject of frequent attacks.

This research attempts to quantify the danger, looking at the volume and frequency of attacks, and some of the different tactics employed in attempting to guess RDP passwords.

Methodology

Building on previous research into attacks on SSH servers, this research used ten geographically dispersed, low-interaction honeypots.

The honeypots were Amazon EC2 instances running Windows Server 2019 with an unmodified, out-of-the-box configuration that enables RDP by default. Each EC2 instance was deployed in a different regional data center. Attackers were prevented from logging on to the machines by a prohibitively strong password. Failed login events (event ID 4625, which captures usernames but not passwords) on all instances were captured in a centralized database over a 30-day period between April 18 and May 19, 2019.

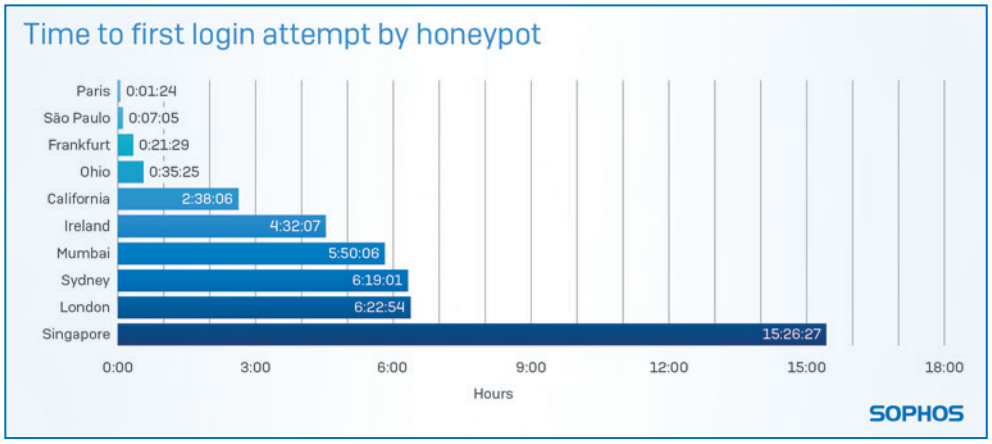
Separately, a computer script monitored Shodan search results for RDP to see how long it took the honeypots to appear in its index.

Findings

Time to first login attempt

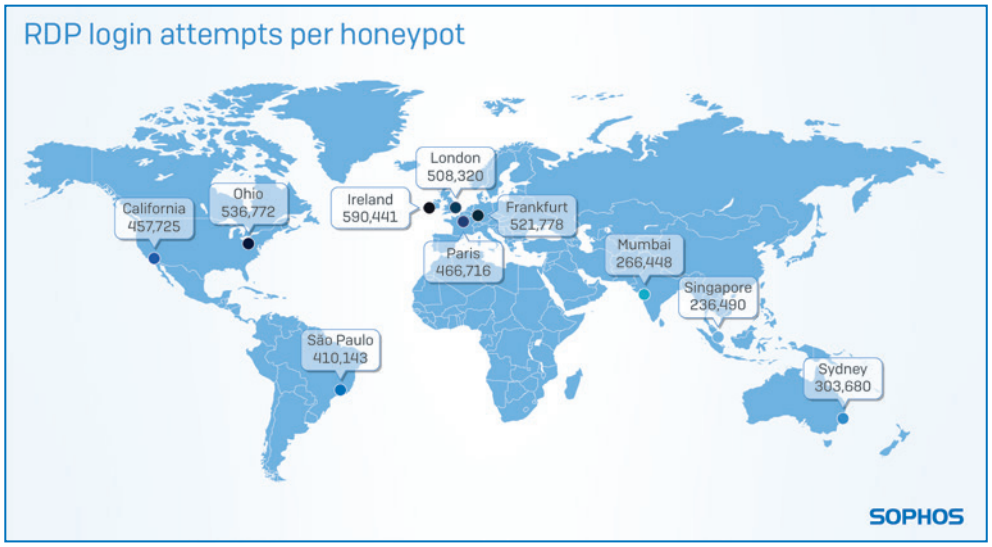
All ten of the honeypots received their first RDP login attempt on day one. The first to receive a visitor was Paris, which had been online for just 1 minute and 24 seconds, and the last to log a first failed login was Singapore, which had to wait for a little over 15 hours. The median average time to first login across all the data centers was 3 hours and 35 minutes. There is not enough evidence to suggest that geography played a part in how quickly the servers were discovered.

All the honeypots, which were known only to the researchers, were discovered within a few hours, simply because they were exposed to the internet via RDP. From a threat modelling perspective, the difference in discovery times is irrelevant – if you use RDP you will be a target, as good as instantly. It is of utmost importance therefore that RDP is hardened against attack and configured correctly before it is exposed to the world.

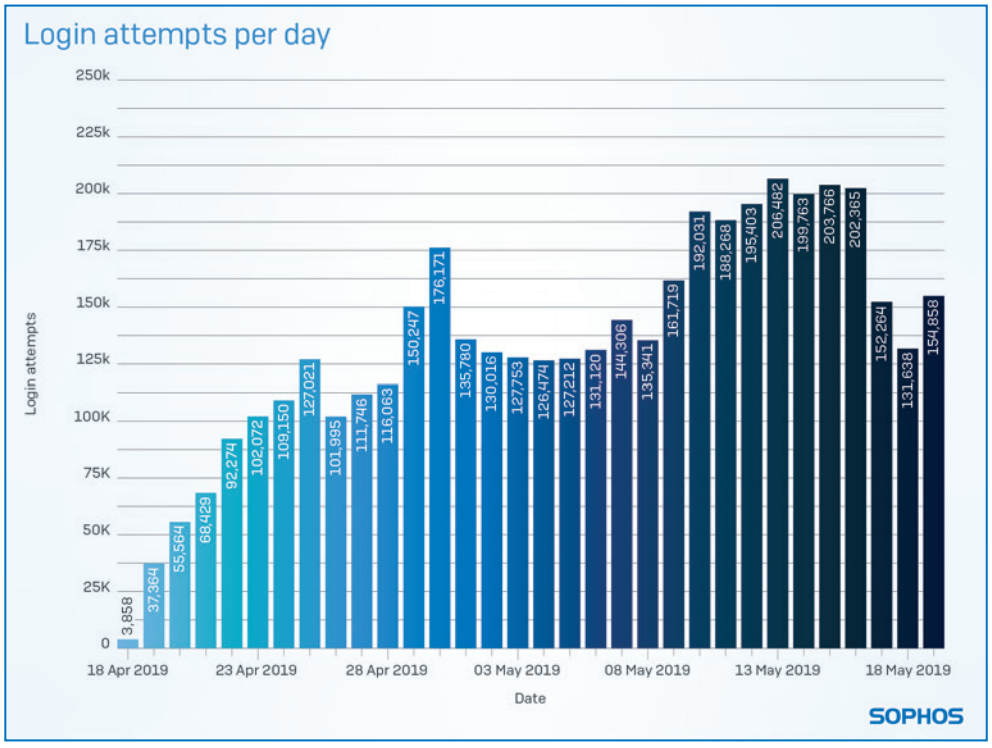


Volume and frequency of login attempts

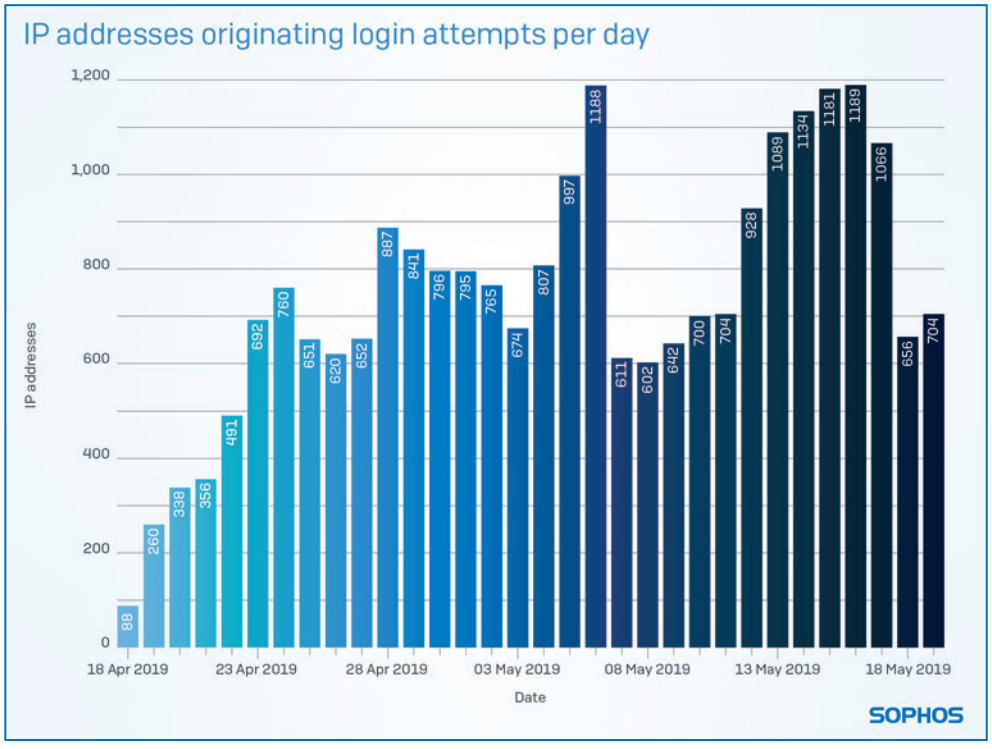
The ten RDP honeypots logged a combined 4,298,513 failed login attempts over a 30-day period at a median average of 467,000 attempts per data center – about 600 login attempts per hour, per data center. For contrast, research in 2012 by Brett Huston measured two login attempts per hour.



After the initial failed login, the honeypots were subjected to an escalating frequency of login attempts for the remainder of the research period.



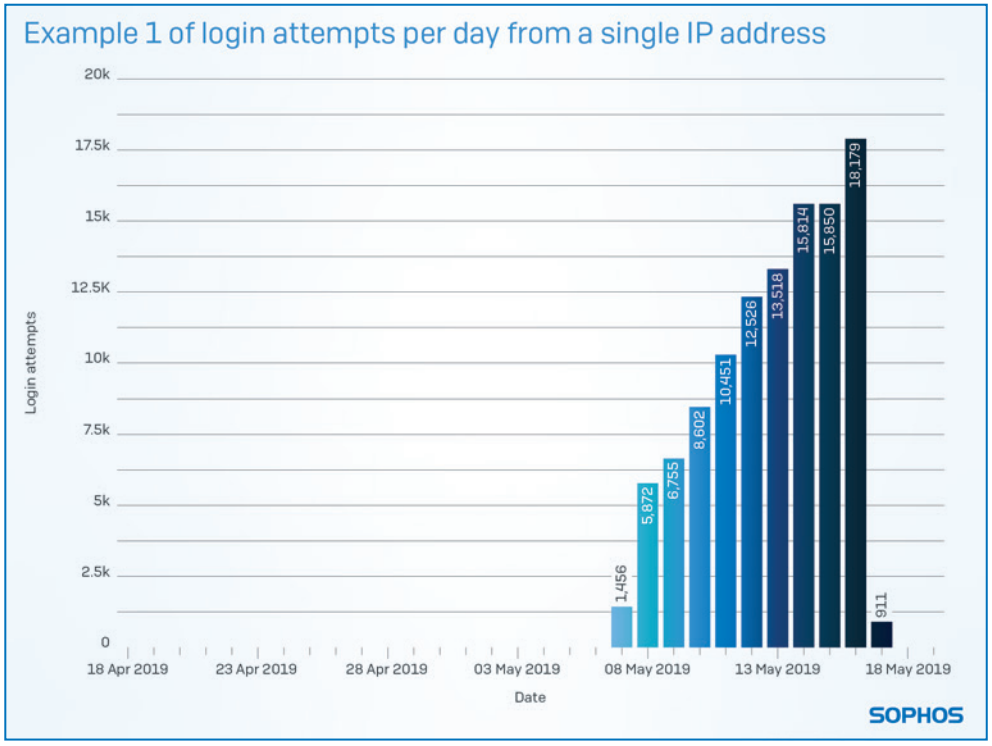
The escalating number of attacks has two causes. The number of IP addresses triggering failed login attempts increases over time, as more people discover the honeypots. In many cases, the number of login attempts per IP address increases over time too.

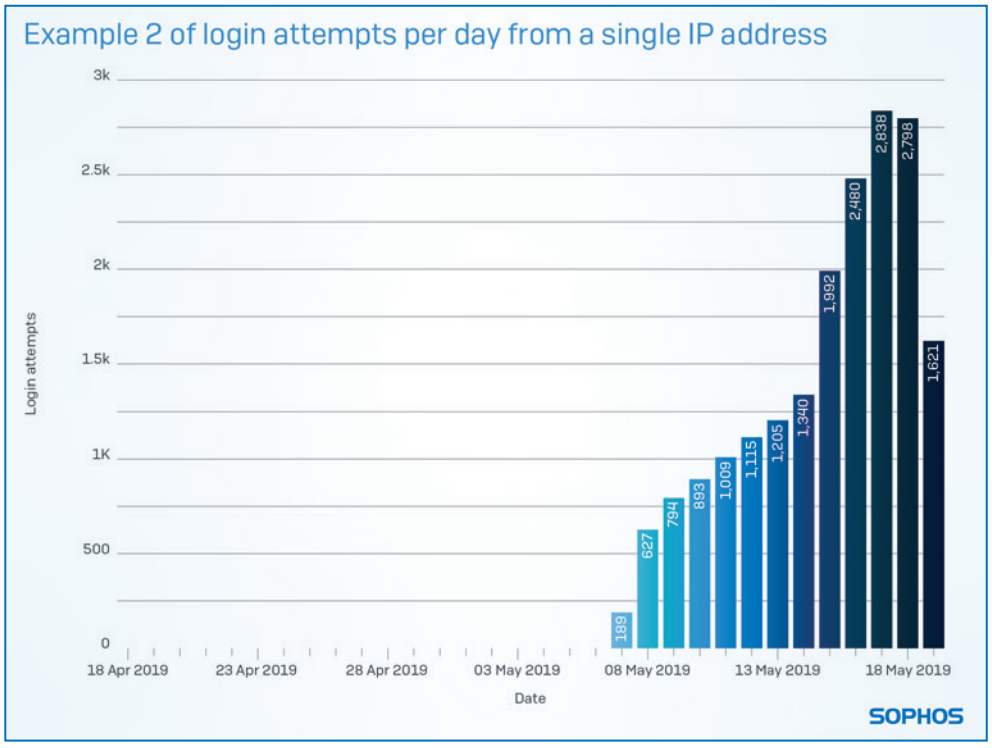


A detection avoidance strategy?

It is possible that in cases where the number of failed logins from a single IP increases over time, multiple attackers are using the same IP address.

By looking at the timing of attacks and the frequency of the username Administrator, which is used by almost every attacker, it is possible to identify attacks where a single IP address appears to represent a single attacker. By isolating individual attackers it's possible to see that in some attacks lasting several days, the number of login attempts per day increases over time.





This pattern is intriguing because, superficially, it's to an attacker's advantage to make password attempts at the maximum rate allowed by their infrastructure, before the target is taken offline. However, there are some reasons why it may be deliberate:

1. Rate-limit discovery

A common password hardening technique is rate-limiting, which locks users out for a penalty period if they have too many consecutive failed logins. By slowly increasing the frequency of attacks until a rate limit is triggered, attackers can discover what the limit is, and ensure they stay below it thereafter.

2. Target acclimatization

The attacker may be trying to acclimatize network monitoring systems to their presence, to prevent anomalous behavior detection alarms from going off (if you get five knocks a day on your front door then an extra knock each day might not strike you as odd, but an extra thirty would immediately command your full attention).

Source of attacks

Because the IP addresses used on the internet are allocated geographically, it's possible to discover where in the world the login attempts made on the honeypots came from.

To avoid detection, it's common for attackers to use compromised computers that can be operated from anywhere in the globe. As such, the location of the IP addresses used to make login attempts is unlikely to reveal anything about where the attackers were located, but it can indicate where the compromised computers they used were.

Login attempts and IP addresses by region

	TOTAL LOGIN ATTEMPTS	SHARE OF LOGIN ATTEMPTS	TOTAL IP ADDRESSES	SHARE OF IP ADDRESSES
Europe	1,801,252	41.91%	952	30.14%
North America	1,136,947	26.45%	806	25.51%
Asia	1,050,811	24.45%	1054	33.36%
Africa	157,599	3.67%	103	3.26%
South America	141,497	3.29%	212	6.71%
Oceania	9,949	0.23%	32	1.01%

The U.S. has the biggest share of IP addresses by far, with about 35% of all IP addresses allocated. The next largest share goes to China, with about 10%. It's no surprise then that both should feature in the top five countries originating login attempts.

The other countries in the top five – Russia, the Netherlands, and Vietnam – are all overrepresented relative to their internet IP address allocation (about 1.5%, 1%, and 0.5% respectively).

Login attempts and IP addresses by country (see Appendix A for a longer list)

	TOTAL LOGIN ATTEMPTS	SHARE OF LOGIN ATTEMPTS	TOTAL IP ADDRESSES	SHARE OF IP ADDRESSES
United States	960,668	25.03%	659	26.37%
Russia	589,252	15.35%	220	8.80%
China	293,833	7.66%	285	11.40%
Netherlands	235,875	6.15%	134	5.36%
Vietnam	160,595	4.18%	120	4.80%

Types of attacks

RDP attackers must choose a strategy that balances a number of variables, each with millions of possible values.

They must choose which targets to attack and how many to attack simultaneously. They must decide on a password guessing rate that's high enough to be effective without raising an alarm. Then they must select the usernames and passwords they'll use from an almost endless number of possibilities.

They must also decide how much effort they're prepared to spend trying to compromise abundant, low privileged user accounts and how much on rarer, more highly privileged (and likely more secure) administrator accounts.

For example, some attackers appear to make just three login attempts on each honeypot, presumably before moving on to another target. Such a brief attack prioritizes reaching the maximum number of targets in the smallest possible time above exhaustive and time consuming exploration of username or password lists. This may be an attempt to avoid a limit of three failed login attempts per IP address imposed by some administrators. It's also possible that the IP addresses in these attacks are part of a botnet using multiple computers to conduct a single, coordinated attack.

The research uncovered a number of different cracking strategies, three of which are explained below. This is not an exhaustive list, but illustrates how different attackers optimize their attacks for different variables.

The ram

The attacker who tried hardest to crack one of our honeypot passwords used a strategy designed to uncover an administrator password. Over the course of 10 days an attacker made 109,934 login attempts at our Irish honeypot, using just three usernames.

The attacker made 37,623 login attempts with the username Administrator, followed by another 37,623 attempts with the username Admin and then 34,688 thousand attempts with the username Riarthóir, the Irish word for administrator.

Although it's possible that the attacker is trying a short list of passwords many times over, it seems more likely that the attacker was using a relatively long password list.

If an attacker is aiming to crack open an administrator accounts then focusing on making tens of thousands of password guesses at the expense of a slow turnover of usernames makes sense. Administrators are likely to have stronger passwords than regular users and a small number of usernames are very common.

The swarm

This attack began on the Paris data center just before midnight on April 23. The attacker tries the username ABrown nine times over the course of 14 minutes. That's followed by nine attempts with the username BBrown, nine more with CBrown then nine with DBrown. Each username is tried nine times at unpredictable intervals, with each interval lasting anything from a few seconds to tens of minutes.

The attacker continues, advancing the first letter of the username through the alphabet and making nine attempts with each username until, at 8:15 p.m. the following evening, nine attempts with the username YBrown are followed by nine with A.Mohamed (the attacker skips ZBrown).

A.Mohamed gives way to B.Mohamed, then C.Mohamed, and so on, through the alphabet until Z.Mohamed gives way to 26 permutations of *.Muhammad (with a dot between the initial and the name), 26 permutations of *.Ali, then 26 of *Smith* (with the letter either side of Smith changing in unison e.g. ASmithA, BSmithB etc). Permutations of *Smith* are followed by permutations of *Müller, then *Simmons and a laundry list of other last names prefixed by A - Z.

Early on the morning of May 4, the attacker makes nine attempts to login to the Paris honeypot with the username ZSimmons.

Around the same time, attacks from the same IP address begin on the Ohio, London, Ireland, and Frankfurt honeypots. Intriguingly, the attacker doesn't begin their attack on the newly discovered targets with the username ABrown, as they did against Paris 12 days before. Instead, all five honeypots, including Paris, receive nine login attempts with the same username: AWashington. These are followed by nine attempts with BWashington, nine each with CWashington and so on.

The attacker continues their relentless and unrepeating strategy against all five honeypots until the honeypots are decommissioned.

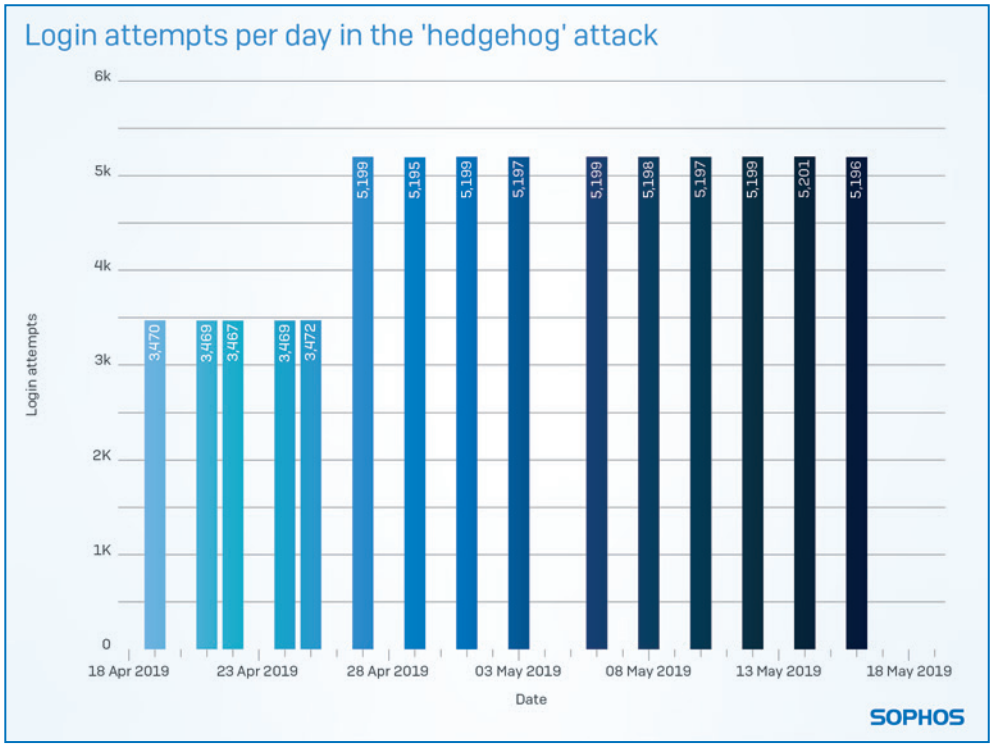
The attacker appears to be working through a long list of usernames and simply includes new targets in their attack at whatever point in the list of usernames they've reached. Perhaps the attack doesn't use a list at all and relies on an algorithm to generate an endless sequence of usernames. However it works, the attacker seems to believe that one username is as likely to produce a result as any other and that, unlike passwords, there is no best first guess.

We assume that the nine guesses per username use nine different passwords (presumably worst common list perennials like "123456" and "password").

The long list of usernames and the short list of passwords makes this nagging, persistent, and unflagging swarm attack the reverse of the ram. Not unreasonably, this attacker seems to think their most likely foothold on a victim's network will come via a regular user with a poor password rather than via an administrator.

The hedgehog

This spikey attack against the Sao Paulo honeypot is characterized by bursts of activity followed by longer periods of inactivity. Each spike is generated by one IP address, lasts approximately four hours and consists of between 3,369 and 5,199 password guesses. Although the spikes are all a similar size and duration, they are not the same size, and neither are the pauses between them as you might expect from a scripted attack. This may be because the attacker is deliberately introducing some randomness into their attack so it doesn't follow a predictable pattern, or perhaps it's an artefact of some constraint we can't see.



This attack is another attempt to discover administrator credentials and only uses the usernames Administrator and SSM-User.

Twelve other IP addresses perform similar short bursts of login attempts against the Sao Paulo data center, using the same pair of usernames and roughly the same number of attempts in each burst. Most of those IP addresses make a single flurry of password guesses and one sustains the repeating pattern of spikes for the entire duration of the test. Given the rarity of the username and the idiosyncratic pattern of the login attempts it seems likely that all 13 IP addresses are under the control of a single attacker.

It isn't known if the attacker's bursts are self-contained and simply cycling through the same password list in each attack, or using each burst to make a little more progress through a larger password list.

What's in a name?

SSM-User

An account with the username Administrator is setup by default on a Windows Server. It's unsurprising then, that username Administrator is by far the most popular with attackers and was used 2.6 million times against our honeypots (about 60% of all the failed login attempts).

Some attackers don't bother with any other usernames at all, and the majority of attackers who try with more than one username include Administrator somewhere in their list.

Top 5 usernames used in all failed login attempts

USERNAME	FAILED LOGIN ATTEMPTS
administrator	2,647,428
admin	376,206
user	79,384
ssm-user	53,447
test	42,117

One of the top five usernames is used in about 75% of all the failed login attempts and the list represents a snapshot of what attackers think will work most effectively.

A surprising entry in the top five usernames was SSM-User. SSM-User is pre-installed by default on a number of Amazon Machine Images (AMIs) and is the default service account used to update, manage, and configure the operating system on those AMIs.

Despite its presence in the top five for all data centers combined, SSM-User is only used in login attempts against the Sao Paulo honeypot. Thirteen IP addresses attempt to login to Sao Paulo with that username, with 66% coming from just one (the "hedgehog" attack).

Given the popularity of AWS, and the fact that RDP is enabled by default on AWS, SSM-User might represent a reasonable guess at an administrator-level username on any exposed RDP connection. However, its presence in our top five appears to be the result of a single attack using just two usernames that accounted for a quarter of all login attempts on the Sao Paulo honeypot. We assume that the attacker knew they were trying to access servers running on AWS and tuned their attack accordingly.

Jessica and David

Found among Administrator, Test, User1, Support and the other techy, functional, entries in our top 25 usernames is David at #20, which stands out as the only name on the list you might actually use to address another person.

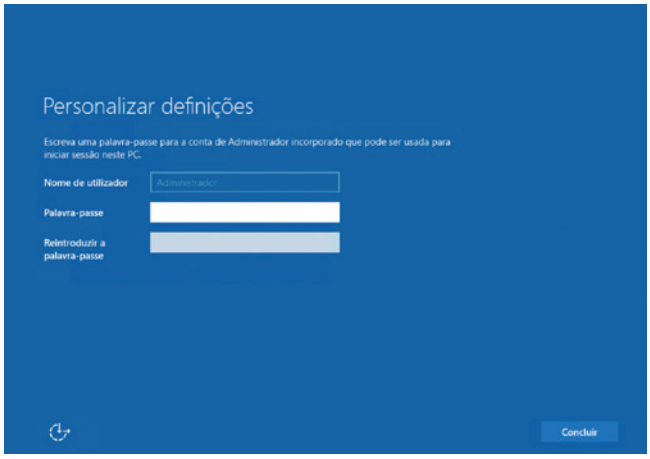
Since the attackers are looking to gain access to a Windows server, they're presumably hoping that the server is domain joined, which many servers indeed are, and they can strike it lucky guessing a regular user's password.

David is used against all the data centers from a wide range of different IP addresses, but 40% of login attempts using David come from one IP address. And that IP address uses Jessica just as often.

Why did the attacker choose these two names? Presumably they're betting on these being popular names amongst the working age population. The U.S. Social Security website suggests they're right: Jessica enters the top five names for females in 1977 and isn't out of the top two between 1981 and 1997. David is rarely the most popular male name but only spends three years outside the top five between 1948 and 1989.

Localization

According to Microsoft, eight languages have a localized word for administrator. If you install a localized version of Windows that uses one of those eight languages, then the name of the default administrator account will use the localized form of administrator.



Most of those localized names for Administrator were used against our honeypots.

Login attempts for localised versions of Administrator

LANGUAGE	TRANSLATION	LOGIN ATTEMPTS
Finnish	Järjestelmänvalvoja	0
French	Administrateur	2,888
Hungarian	Rendszergazda	4
Spanish **Portuguese (Brazil)** **Portuguese (Portugal)**	Administrador	20,079
Russian	Администратор	802
Swedish	Administratör	14,593

Perhaps surprisingly, all of the localized forms of Administrator that were popular were used against all of the data centers. There does not appear to be any correlation between the choice of localization and the geographic location of the data center. Administratör was as popular in Mumbai as it was in Frankfurt for example, while Administrador was four times as popular in London as it was in Sao Paulo.

One translation of the word Administrator did correlate with a data center's location, although it isn't on Microsoft's list of default localized Administrator account names. Riarthóir is an Irish translation of Administrator and was used in more failed login attempts than any other translation of administrator – 34,688 times. All of them came from a single IP address and all of them occurred at the Irish data center.

The Irish language version of Windows does not create an Administrator account called Riarthóir but it does use Riarthóir as the default administrator account's display name.

Impact of Shodan

Shodan is a search engine that discovers and indexes internet-connected devices and presents them in an easy-to-use graphical interface. It makes finding servers of a particular type, such as Windows machines running RDP, or devices with particular ports open, such as the port most commonly used by RDP – 3389 – very easy. It can be used by attackers to discover targets or by organizations trying to discover how they appear to potential attackers.

This research set out to discover if Shodan played a role in how people find RDP-enabled computers. This was done by observing whether the rate of attacks against the honeypots increased after they appeared in the search engine's index.

A Python script monitored Shodan continuously throughout the test period, looking to see if the honeypot's IP addresses were listed, and if they were identified as running RDP.

None of the honeypots appeared in the Shodan index during the test period and so the monitoring didn't reveal anything about whether or not hackers use Shodan, or what difference a Shodan listing might make to the number of attackers.

What the monitoring does make clear is that a computer that isn't listed on Shodan is still a target. Potential attackers are able to find RDP-enabled devices almost as soon as they appear on the internet and organizations should not rely upon Shodan to assess how they appear to potential attackers.

Conclusions

Just before the end of the research testing period Microsoft issued an advisory for CVE-2019-0708, a remote code execution flaw in RDP nicknamed BlueKeep. The vulnerability requires no authentication and is regarded as 'wormable,' meaning that if it were successfully exploited it could be used by self-replicating malware to spread across the internet rapidly (WannaCry and NotPetya used a similarly wormable flaw in Microsoft's SMB v1 to spread around the globe in a matter of hours).

But securing RDP goes far beyond patching systems against CVE-2019-0708.

While system owners rightly race to secure their machines against BlueKeep, cybercriminals are busy probing computers exposed by RDP, using password guessing attacks, 24 hours a day.

Sophos first warned about automated attacks against RDP passwords in 2011, when the Morto worm used nothing more than a short list of common passwords to spread via RDP.

The risks of RDP were highlighted once more in 2017 as it became clear that multiple ransomware operators were using it as the entry point for a new form of ransomware attack.

Some criminals were abandoning untargeted malware delivery approaches, such as email campaigns, in favor of a more considered and targeted approach. With network access gained via an RDP foothold, the groups behind malware like BitPaymer and SamSam could hold entire companies to ransom and demand vast, five- or six-figure ransoms.

Targeted ransomware attacks have continued to represent a major threat to organizations ever since. Targets are selected on the basis of their vulnerability to RDP brute forcing, and, as this research clearly demonstrates, discovering vulnerable RDP servers has become a lucrative, industrial scale activity.

When Sophos wrote about Brett Huston's attempts to measure RDP password guessing attempts in 2012, his honeypots received two probes per hour. The honeypots in this research measured 600.

Some attackers make fleeting visits, trying just a few usernames and passwords before moving on to the next target. A smaller number show far more persistence, trying tens of thousands of passwords or more, hoping to hit the jackpot and login as an administrator. Others simply grind away, patiently exploring every corner of your address book.

The intransigence of weak passwords in the face of decades of user education suggests that the number of RDP servers vulnerable to brute force attacks is unlikely to be reduced by a sudden and dramatic improvement in users' password choices.

Changing this situation therefore requires action from either administrators, cloud computing vendors, or Microsoft, RDP's progenitor.

Microsoft controls the design of RDP and could significantly improve resistance to password guessing by making two-factor authentication mandatory, or by switching to another form of authentication entirely, such as public key authentication. Given the RDP installed base, and the hostility that has greeted previous mandatory updates by Microsoft, any such switch would likely be highly disruptive.

Cloud computing vendors like Amazon offer turnkey servers and could influence vast numbers of computers by modifying the default configurations in their standard machine images. For example, Amazon EC2 instances running Windows, such as those used in this research, are administered remotely via RDP. Switching to an alternative means of remote administration, or some form of alternative authentication scheme, would remove a large number of potential targets from attackers' sights.

Until RDP is replaced or improved, the buck stops with administrators though. They can lessen their company's exposure to attack by using Remote Desktop Gateway and enabling multi-factor authentication. While effective against credential harvesting, this still leaves RDP servers exposed to zero-day exploits or unpatched vulnerabilities such as BlueKeep.

Administrators can further harden their machines against credential harvesting by not allowing domain administrators to log in via RDP; enabling RDP for only the people who need it; securing idle accounts; rate-limiting or capping the number of password retries each user is allowed; and strength testing users' passwords.

It is the researchers' contention though that computers running RDP represent such a high-value target that they should not be accessible from the internet at all. Where possible, RDP should be disabled. Where it's required, it should be shielded from exploits and credential harvesting by controlling access to it with a Virtual Private Network (VPN).

Appendix A

Login attempts and IP addresses by country

	TOTAL LOGIN ATTEMPTS	SHARE OF LOGIN ATTEMPTS	TOTAL IP ADDRESSES	SHARE OF IP ADDRESSES
United States	960,668	25.03%	659	26.37%
Russia	589,252	15.35%	220	8.80%
China	293,833	7.66%	285	11.40%
Netherlands	235,875	6.15%	134	5.36%
Vietnam	160,595	4.18%	120	4.80%
India	153,831	4.01%	140	5.60%
France	148,215	3.86%	101	4.04%
Ireland	118,463	3.09%	40	1.60%
Latvia	118,140	3.08%	16	0.64%
United Kingdom	116,528	3.04%	76	3.04%
Germany	114,166	2.97%	127	5.08%
Canada	9,6903	2.52%	77	3.08%
Ukraine	91,337	2.38%	42	1.68%
South Africa	78,825	2.05%	46	1.84%
Poland	76,065	1.98%	22	0.88%
Brazil	75,579	1.97%	107	4.28%
South Korea	69,434	1.81%	53	2.12%
Italy	65,953	1.72%	37	1.48%
Singapore	55,154	1.44%	73	2.92%
Bangladesh	51,293	1.34%	21	0.84%
Indonesia	43,338	1.13%	18	0.72%
Japan	38,293	1.00%	24	0.96%

Appendix B

Top 15 usernames (all honeypots)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	2,647,367
admin	376,206
user	79,384
ssm-user	53,447
test	45,289
riarthóir	34,653
administrador	18,196
admin1	17,700
guest	17,023
administratör	14,277
user1	13,802
server	13,788
support	11,485
ec2amaz	8,564
root	7,533

Appendix C

Top 15 usernames (Ireland)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	372,269
admin	76,465
riarthóir	34,688
user	9,785
test	3,173
user1	1,898
admin1	1,855
administrador	998
server	807
guest	710
tempadmin	498
test1	489
support	462
temp	444
david	314

Appendix D

Top 15 usernames (Ohio)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	333,146
admin	50,700
user	10,688
test	6,764
server	5,731
guest	3,749
administrador	3,379
support	3,086
user1	3,048
admin1	3,037
root	2,787
sql	2,334
david	1,852
administratör	1,839
sqlserver	1,542

Appendix E

Top 15 usernames (Frankfurt)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	317,402
admin	41,610
user	11,855
test	4,756
administratör	1,395
guest	1,131
administrador	1,014
support	971
server	966
admin1	955
user1	743
backup	714
root	639
temp	576
reception	511

Appendix F

Top 15 usernames (London)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	314,652
admin	47,558
user	9,644
administrador	7,544
test	5,462
guest	2,202
support	1,828
administratör	1,816
server	1,669
admin1	1,336
пользователь	1,316
user1	1,132
root	995
david	723
backup	690

Appendix G

Top 15 usernames (Paris)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	264,076
admin	29,240
user	8,674
ec2amaz	8,564
admin1	3,754
test	3,277
guest	871
support	746
administrador	724
administratör	666
kevin	664
ec2amaz-gi6fja	469
user1	445
server	436
test1	346

Appendix H

Top 15 usernames (California)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	306,698
admin	38,431
user	5,608
test	4,782
administratör	1,664
administrador	1,286
guest	1,158
support	1,139
user1	971
admin1	851
server	653
test1	646
temp	615
root	444
administrtor	388

Appendix I

Top 15 usernames (Sao Paulo)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	260,341
ssm-user	53,671
admin	23,540
user	7,491
test	4,591
administrador	1,789
estoque1	1,300
administratör	1,144
support	719
user1	539
guest	529
spfarm	522
adm	521
admin1	504
server	459

Appendix J

Top 15 usernames (Sydney)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	191,805
admin	19,992
user	5,479
test	4,833
guest	1,796
admin1	1,390
user1	1,246
server	1,159
support	1,149
administratör	926
root	884
asp.net	736
mypc	617
administrador	565
test1	557

Appendix K

Top 15 usernames (Mumbai)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	152,317
admin	26,235
user	5,200
test	3,374
admin1	2,799
administratör	2,594
priyanka	1,028
aditya	950
user1	878
server	798
guest	773
support	750
deepak	605
test1	517
david	417

Appendix L

Top 15 usernames (Singapore)

USERNAME	FAILED LOGIN ATTEMPTS
administrator	133,797
admin	24,393
user	8,122
test	5,083
guest	4,080
user1	2,474
administratör	2,226
admin1	1,153
user001	914
server	677
remote	625
backup	588
root	574
administrador	525
test1	506

sophos.com

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

19-07-15 WP-EN (DD)

SOPHOS