REMOTE CONTROL

Chris Morales *discusses the potential risks involved in remote desktop protocol and reveals measures to keep your organisation safe*

Being able to control a computer or range of computers remotely is definitely a useful business tool, however it is also a dream come true for threat actors as it enables them to more easily carry out key elements of an attack. Remote Desktop Access (RDP) is a popular administrative tool used by IT system administrators to centrally control their remote systems with the same functionality as if they were local. It's also valuable for normal users who want access to their computer when away from their normal work location. That is why accessing an organisation's Remote Desktop Protocol is such an attractive target, with recent Vectra research showing that nine out of 10 organisations experience some form of malicious RDP behaviour.

The research, conducted on observations made between January and June 2019, highlights those industries and size of organisations with the most RDP detections, along with examples of how RDP is being used by cybercriminals and state-sponsored actors.

Organisations around the world use RDP as a means of creating efficiencies through enabling engineers and technicians to centrally access hundreds or even thousands of connected devices that could be in distant or inaccessible locations. This is highlighted in figures from industrial communications and IoT solutions supplier HMS Networks, which show that sending out an engineer to fix an issue with a machine or device can cost in the region of $2,200. Given that, according to Machine Design, 60 to 70 percent of machine issues can be resolved remotely through a system upgrade or changing settings, it is hardly surprising that businesses are opting for RDP. Why would they want to go to the expense of paying for an engineer to travel to wherever the issue is, simply to push a few buttons that could be done in a few minutes by one in an operations centre?

Furthermore, the time saved resolving these issues remotely, along with the ability to cover an entire network from one room, means that one engineer can do the work of a whole team. This enables an organisation to further streamline costs.

APT40 has targeted organisations involved in the development and production of naval technologies across a range of sectors including defence, engineering and transportation

Picture credit: Getty

WREAKING HAVOC

Yet with all the benefits it brings, RDP can be an Achilles' heel when it comes to securing a corporate network. If a threat actor manages to gain access to RDP, they can wreak havoc almost completely undetected. Unfortunately, this can be surprisingly simple for a threat actor to achieve, particularly if a system uses default passwords and settings. Worse yet, Microsoft recently revealed four critical RDP vulnerabilities affecting Windows 7, Windows 8 and, the latest version, Windows 10 that could be executed without the need for credentials. Therefore, as organisations upgrade their systems to try to make them more efficient and secure, they will still be affected by these vulnerabilities.

As cybercriminals usually choose the easiest root to accessing a network, it is no wonder that RDP attacks are increasingly popular. Indeed, the FBI has warned that such activity "has been on the rise since mid-late 2016".

The sectors most targeted with malicious RDP behaviours observed during our six-month research period were manufacturing, finance and retail. These accounted for half of the incidents recorded for nine sectors in total.

Regarding the size of organisation being attacked, small and medium businesses experienced a higher proportion of RDP detections than larger firms. Medium organisations experienced 6.9 RDP detections per 10,000 workloads or devices, small organisations had 6.5, while large businesses had 4.5. The reason for this difference between small/medium organisations and large organisations, is that large businesses are more likely to have a greater number of employees assigned to cybersecurity and threat hunting, as well as bigger budgets to invest into IT security.

When looking at size and sector together, the most RDP detections were seen in medium manufacturers, medium retailers and small financial institutions. The only large organisation type that appears in the top 10 is manufacturing.

It is worth noting that the size of the company, or rather the number of staff it employs, is not always indicative of the number of devices. Businesses in the manufacturing sector for instance are likely to have significantly more devices or machines than staff. RDP enables a small team to conduct the necessary close monitoring and frequent modifications manufacturing machinery requires, significantly reducing operational costs while improving productivity.

To gain greater insight into the attack methods used by threat actors, as part of the research we used our own platform to split the RDP detections into RDP Recon and Suspicious Remote Desktop. RDP Recon is an early stage attack behaviour detection activated when repeated failed attempts to establish an RDP connection to a workload or host are detected, which can occur when a threat actor tries various default log-in combinations to access a system or they are looking to identify active accounts. The three top industries we observed for RDP Recon were manufacturing, government and education.

Suspicious Remote Desktop detections on the other hand are activated when unusual characteristics are detected following a successful RDP connection. This could be because an RDP server that is usually logged into using English keyboard inputs is accessed by someone using a French keyboard, for instance. Again, organisations within the manufacturing sector showed the most RDP detections followed by retail and insurance.

ORGANISATIONS MUST DRAW THEIR FOCUS TO THE WHO, WHAT, WHERE AND WHEN OF RDP ACCESS

Furthermore, detections of RDP Recon and Suspicious Remote Desktop combined varied from sector to sector. For example, while retail businesses had one of the lowest rates of RDP Recon behaviours, they experienced some of the highest levels of Suspicious Remote Desktop. While on the other hand, Government organisations were victims of half the amount of Suspicious Remote Desktops connections compared with RDP Recon detections.

Probably the most well-known campaign in which cybercriminals used RDP to facilitate their attacks was SamSam, which saw more than 200 organisations being infected with ransomware over a three-year period.

GAINING ACCESS

RDP enabled threat actors to gain persistent access to the networks of critical infrastructure, hospitals and Government agencies around the world. Once in, SamSam actors could move around on the network completely unknown to their victims, escalating privileges, infecting servers with malware and running an executable file. Unlike other ransomware campaigns where the victim must perform an action such as opening an email attachment, SamSam could be executed with no need for the victim to be involved at all, thanks to RDP. The US Department of Justice believes that SamSam perpetrators made more than $6-million in ransom payments and caused a further $30-million in damage.

Aside from cybercriminals looking to exploit RDP for financial gain, the protocol is also leveraged by state-sponsored threat actors looking to commit espionage. For example, news surfaced of a tracked threat actor group which was labelled APT40 that is working to support the modernisation of China's Navy. As part of its clandestine operations, APT40 has targeted organisations involved in the development

and production of naval technologies across a range of sectors including defence, engineering and transportation. For example, it has tried to infiltrate universities involved in maritime research, such as Penn State and Duke in the US, impersonating a manufacturer of unmanned underwater vehicles.

WHY PAY FOR AN ENGINEER TO TRAVEL TO FIX THE ISSUE WHEN THE PROBLEM CAN BE SORTED REMOTELY?

In many of these attacks APT40 uses RDP to laterally move through a network performing actions such as stealing data, reconnaissance and malware execution. Elsewhere a cyber-espionage gang with links to Iran has been conducting attacks on telecommunications, travel and high-tech industries, as well as Government organisations. While its main focus appears to be the Middle East, APT39 has targeted victims in Europe and the United States. As the two largest economies in the Arabian Gulf, Saudi Arabia and The United Arab Emirates are likely to increasingly become targets as Iran seeks to gain more prominence in the region.

RDP is used by APT39 not only to facilitate lateral movement throughout a network, but also to maintain persistence within it. This is reflective of an increasing trend among state-sponsored cyber-espionage groups of no longer just simply committing a 'smash and grab' to steal data, but instead being able to harvest information and cause sabotage on a long-term basis.

As demonstrated by our findings, as well as warnings from law enforcement, there are clearly significant risks posed by threat actors potentially gaining access to an organisation's network through the malicious use of RDP. Nevertheless, businesses still see RDP as an invaluable tool, with many believing that the benefits of using it outweigh the security risks associated. Therefore, as a consequence of businesses continuing to use RDP, it will carry on representing a significant risk as an exposed attack surface. As such, actions must be taken that mitigate these risks as much as possible.

REDUCING RISK

Limiting access to only those that need to use RDP is essential along with strong authentication processes, which includes ensuring that the same credentials are not used by more than one person. Furthermore, organisations must assume compromise is possible and draw their focus to the who, what, where and when of remote desktop access. Doing this not only reduces the chance of credentials being accidentally shared with unauthorised persons, but also limits the scope of an investigation following a cyberattack as to who might be the source.

In addition to access controls, it is also vital that organisations increase their ability to detect a cyber attacker on the network. With this in mind, it is advised that they implement tools that can automatically monitor, detect and respond to remote access behaviours at speed and scale to determine whether they represent those of a cyber attacker infiltrating the network.

By taking steps towards secure and monitored RDP use, companies can continue to benefit from the value it delivers without having to weigh up the risks it poses ●

Chris Morales Head of Security Analytics at Vectra, has over 20 years of experience in cybersecurity consultancy, sales and research roles. He is a widely respected expert on cybersecurity issues and technologies.

SamSam perpetrators made more than $6-million in ransom payments and caused $30-million in damages