Remote Desktop Protocol (RDP): Balancing Convenience with Security

By Lisa Traina, Partner, and Allison Davis, Senior Manager

RDP**:** three letters that create significant debate among network administrators, security experts, and analysts. Remote desktop protocol (RDP) provides a graphical interface when used to connect to another computer over a network connection for remote administration. It is often used for working remotely and providing IT support.

Yet while RDP provides convenience and efficiency to many organizations, it also has many security implications. It's too useful to give up, but is it too dangerous to keep? Before we can evaluate the solutions for securing this type of remote access, we need to understand what RDP is and why it has become a popular target for cyber criminals.

The History of RDP

Microsoft created RDP over 20 years ago and it has been widely adopted for its simple graphical interface and ease of use when connecting to other computers. The protocol is built into the majority of Windows operating systems as a server, and the client required for access is available on most operating systems, including Windows, macOS, UNIX, and Linux. As a result, RDP provides the ability for a user to remote into another computer via a known port from anywhere, with hardly any setup on the user side.

Third-party software that allows a user to remote into another computer has since been introduced, including LogMeIn, TeamViewer, and join.me. While this software offers more features than a regular RDP client, the use of RDP — which is built into existing systems and free — has not declined. RDP continues to be easy and cost-effective for organizations.

In September 2018, the FBI's Internet Crime Complaint Center (IC3) released an announcement about cyber criminals increasingly exploiting RDP and ongoing attacks against devices with the port open to the Internet. IC3 encouraged organizations to evaluate their use of RDP and the controls in place to secure it.

As noted above, RDP is not a new service. So how is it still being so heavily exploited after its initial release?

RDP Exploits

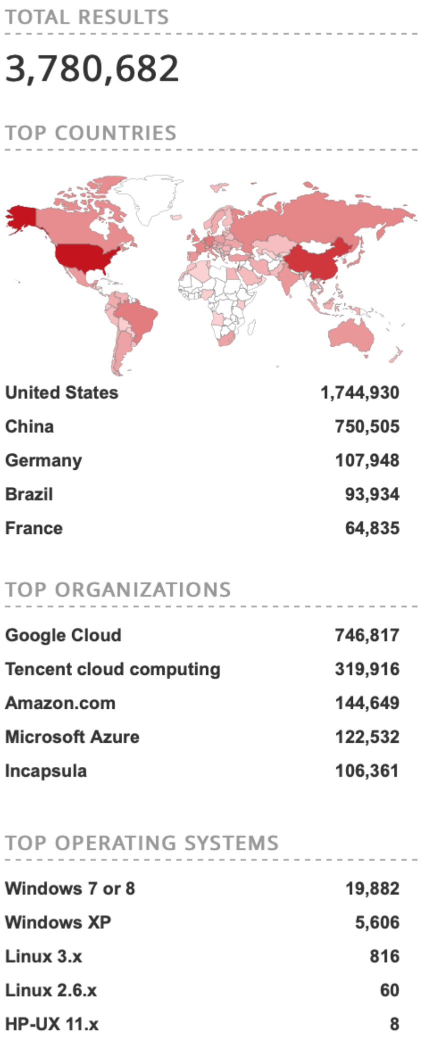
As with any piece of software, bugs arise sooner or later. A critical security exploit allowing a man-in-the-middle-style attack was discovered in RDP version 5.2. In 2012, another critical vulnerability was discovered to allow a Windows computer to be compromised by unauthenticated clients. Version 6.1, found in Windows Server 2008, revealed a critical exploit that harvested user credentials. And more recently, an exploit discovered in March 2018 allowed remote code execution attack and another credential-harvesting scenario.

At the same time, hackers are well aware of the extensive use of RDP within organizations. As a result, they are now targeting RDP as a method to proliferate their attacks. The evolution of ransomware is a prime example. Ransomware has proven to be a very lucrative form of cyber attack, and hackers have begun to target RDP to spread this form of malware within organizations.

Similarly, capturing and selling RDP credentials on the dark web has also proven to be a money-making scheme for hackers. RDP credentials sell on dark markets for about $3 apiece, on average. One set of credentials allows you complete control via RDP, and some dark web sites have thousands of compromised credentials for sale.

Human error has also contributed to the exploitation of RDP. Overworked, stressed, or novice network administrators often feel that they need to respond quickly to users seeking an easy and efficient method of remote access. Since RDP is built into operating systems, many network administrators failed to consider the implications of exposing RDP to the public Internet. And once third-party software became the norm, RDP became a backup solution and an afterthought. It was essentially out of sight, out of mind.

At this point, the risk associated with RDP sessions is inarguable, but RDP usage hasn't declined. On the contrary, it has increased rapidly as more organizations use remote locations, rely on cloud computing, and decrease the use of physical hardware with emerging technologies such as virtualization. A query on Shodan, a search engine used to scan specific types of computers that populate the entire Internet, shows just how extensively RDP is used. This screen capture, taken in January 2019, is a real-time view of how many computers have the default RDP port (port 3389) active and open for attack on the Internet.



TOTAL RESULTS

3,780,682

TOP COUNTRIES

United States	1,744,930
China	750,505
Germany	107,948
Brazil	93,934
France	64,835

TOP ORGANIZATIONS

Google Cloud	746,817
Tencent cloud computing	319,916
Amazon.com	144,649
Microsoft Azure	122,532
Incapsula	106,361

TOP OPERATING SYSTEMS

Windows 7 or 8	19,882
Windows XP	5,606
Linux 3.x	816
Linux 2.6.x	60
HP-UX 11.x	8

How to Secure RDP

Until Microsoft disables the RDP client-server feature in all past, current, and future iterations of the Windows operating system, RDP will always be used. The macOS operating system also uses Microsoft's branded RDP client. And with the release of Microsoft's new HTML5 version of the RDP client, it is now entirely browser-based. This form of remote access is too convenient to discontinue fully. So what do we do?

Fortunately, you can secure RDP through layered controls. While this list is not exhaustive, it provides some basic guidelines for securing RDP in your organization:

- Disable any RDP connection to the open Internet. If nothing else, this will reduce the risk of hackers scanning your network and limit your susceptibility to brute force attacks.
- Change the default listening port from 3389.
- Update and apply patches regularly.
- Enable complex passwords and a conservative account lockout policy. Consider customizing a more stringent policy for RDP.
- Configure multi-factor authentication (MFA).
- Limit and reduce access via RDP and consider disabling all administrative access via RDP.
- Enable logging and monitoring capabilities to alert personnel of suspicious activity.
- Ensure self-signed certificates are in place.
- Enable the following on workstations and servers that use RDP:
    - Network Level Authentication
    - TLS 1.2
    - FIPS compliance

While it may be difficult to stop using RDP, it's crucial to take steps to secure it. Please contact us at capintech.com with any questions.

This article was originally published in The Nonprofit Times.

Fortunately, you can secure RDP through layered controls.

About the Authors

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

Allison Davis, Senior Manager
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA