AVALON Cyber

Remote Desktop Protocol (RDP) Attacks

RDP attacks are **up 330%** since the start of the **COVID-19 pandemic.***

The Headlines

"Iranian Hackers Attack Exposed RDP Servers to Deploy Dharma Ransomware"

Low-skilled hackers…find victims by scanning IP address ranges on the internet for exposed remote desktop connections…

"Millions of Brute-Force Attacks Hit Remote Desktop Accounts"

A rash of brute-forcing attempts aimed at users of Microsoft's proprietary Remote Desktop Protocol (RDP) has come to light, striking millions per week…

"Zerologon Attacks Against Microsoft's DCs Snowball in a Week"

…researchers from Cisco Talos warned that cybercriminals are redoubling their efforts to trigger the elevation-of-privilege bug in the Netlogon Remote Protocol...

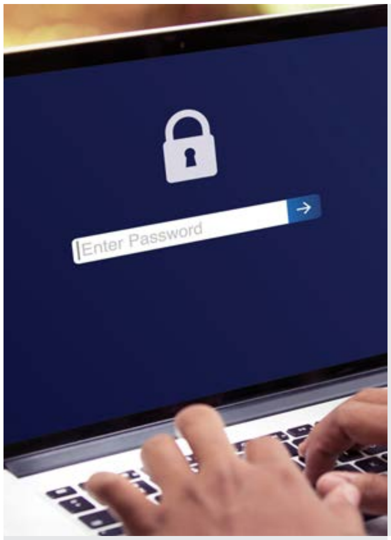
The Situation

With the recent rise in remote workers due to COVID-19, Remote Desktop Protocol, or RDP, (i.e. Microsoft's proprietary protocol, which allows employees to access Windows from outside their company's network) has been making headlines on a regular basis. The reason? The number of internet-connected RDP ports jumped from 3 million in January 2020 to 4.5 million by the end of March.

Unfortunately, many businesses don't take the right precautions and leave their RDP ports open, i.e. unsecured, allowing anyone – including cybercriminals – to access their network. McAfee, an international computer security company, recently reported that the U.S. and China have the most exposed systems, at around 1.3 million each. As you can probably guess, the number of attacks targeting open RDP ports in the U.S. more than tripled in March and April.

So how do the bad guys get in? Well, since some RDPs aren't even password protected, they just "walk" straight into the network. If the RDP does require a password, the most common way an adversary gains access is through a "brute-force attack," a terrifying name for the process of attempting numerous password options over and over until a legitimate password is revealed. Which is why strong passwords are crucial to securing your network (see sidebar on next page).

Once accessed, adversaries use a company's network to spread spam and malware, collect personally identifiable information (PII), and carry out other nefarious activities. Luckily, there are several steps you can take to protect your business's RDP.



Really Dumb Passwords

It's hard to believe that it still happens, but people continue to use passwords like 123456, qwerty, test123, and the "uncrackable" P@ssw0rd123. That's why another acronym security peeps use for RDP is "Really Dumb Passwords."

If your employees are using passwords like this, consider yourself breached. Strong passwords should be required for any and all systems, programs, and sites your team uses for work, including your RDP.

To avoid the usage of Really Dumb Passwords, you may want to consider a password management tool like LastPass to make it easier for your employees and safer for your business.

"With the increasing sophistication of adversaries' attacks and the **growing number of remote workforces,** the risk landscape is only widening and becoming more complicated.

A **model of Zero Trust is imperative,** to not only detect, but to stop these activities before they start."

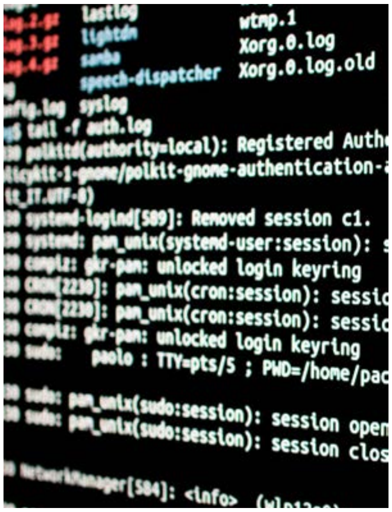
– Kyle Cavalieri,
President,
Avalon Cyber

The Solutions You Can Implement Right Now

First and foremost, establish a virtual private network (VPN) to protect your RDP. That way, your employees have access to your network, but your VPN secures the network by creating a data tunnel that encrypts your data, making it unreadable to outsiders.

In addition to utilizing a VPN, we suggest adopting the following tactics:

- ✓ Do not allow RDP connections over the open internet
- ✓ Use strong passwords
- ✓ Use multi-factor authentication (MFA)
- ✓ Update your software
- ✓ Lock out users and block IPs that have too many failed log-on attempts to prevent brute-force attacks
- ✓ Use an RDP gateway
- ✓ Limit domain admin account access
- ✓ Minimize the number of local admins and ensure that each account is unique
- ✓ Enable restricted admin mode
- ✓ Restrict access via firewalls
- ✓ Enable Network Level Authentication (NLA)
- ✓ Consider placement within the network
- ✓ Consider using an account-naming convention that does not reveal organizational information



```
log.2.gz   lastlog                   wtmp.1
log.3.gz   lightdm                   Xorg.0.log
log.4.gz   samba                     Xorg.0.log.old
           speech-dispatcher
nfig.log   syslog
$ tail -f auth.log
polkitd(authority=local): Registered Auth
olicykit-1-gnome/polkit-gnome-authentication-
(it_IT.UTF-8)
systemd-logind[589]: Removed session c1.
systemd: pam_unix(systemd-user:session): s
compiz: gkr-pam: unlocked login keyring
CRON[2230]: pam_unix(cron:session): sessio
CRON[2230]: pam_unix(cron:session): sessio
compiz: gkr-pam: unlocked login keyring
sudo:    paolo : TTY=pts/5 ; PWD=/home/pac
sudo: pam_unix(sudo:session): session open
sudo: pam_unix(sudo:session): session clos
NetworkManager[584]: <info>
```

In the U.S., between **March 10 and April 15, 2020,** cybercriminals carried out **32,299,662** remote desktop brute-force attacks.

On average, there were **872,964 attacks daily.***

The Solutions Avalon Cyber Can Provide

In addition to securing your RDP, it's a great idea to have a cybersecurity company inspect the health of your network via a few tests – and to have their number on speed dial in case of an emergency.

Vulnerability Assessments

Avalon Cyber's expert engineers conduct internal and/or external scans to identify vulnerabilities and basic misconfigurations in your company's environment. Our team works with you every step of the way to develop a plan to address the most critical weaknesses and provide insights into the best way to implement improvements.

Penetration Tests

Our cybersecurity professionals safely simulate the actions of a cybercriminal targeting your network and attempt to exploit critical systems to access sensitive data. Penetration testing validates the efficiency of your currently deployed security resources and determines how well employees are following existing security policies.

Phishing Simulation and Training

Avalon Cyber partnered with the world's largest security awareness training and simulated phishing platform to help our clients manage the ongoing problem of social engineering. Our innovative phishing simulation and training program allows your security team to launch best-in-class, fully automated simulated phishing attacks and run comprehensive security awareness training campaigns to help educate your employees and stakeholders.

Managed Detection and Response (MDR)

Our KnightVision MDR service is a robust endpoint monitoring solution that screens malicious behavior at the endpoint level, allowing our team of experts to alert you and take immediate action to shut down a potential threat.

SIEM and Managed SOC

Our KnightVision CAM (which stands for Compliance, Alerting, and Monitoring) combines a Security Information and Event Management (SIEM) platform, which collects, aggregates, and analyzes security event log data, and a managed Security Operations Center (SOC), i.e., a team of cybersecurity experts who respond to detected threats immediately. It's Avalon Cyber's customizable, scalable, affordable solution that addresses a range of cybersecurity challenges, including regulatory compliance, threat detection, and incident response.

The Conclusion

The current work-from-home situation probably won't change for quite a while. Some employees still can't return to the office, while others prefer to work remotely and hope to continue doing so, having proven that staying home and being productive can go hand in hand. That means RDP will be a necessity for many companies for the foreseeable future, so securing it through the simple steps listed here will allow your employees to access what they need to succeed, while keeping cybercriminals out.

About Avalon Cyber

Avalon Cyber offers a full suite of cyber services, including vulnerability assessments, penetration tests, managed detection and response (MDR), and KnightVision CAM (compliance, alerting, monitoring), our opensource SIEM/MSOC solution, developed to assist small and medium-sized businesses with regulatory compliance, threat hunting, alert detection, and incident response.

The men and women who support our managed security services have decades of experience in information security, have or previously have held top secret government clearances, and possess key industry certifications including: CISSP, OSCP, GPEN, CISM, CISA, CRISC, CCNA, CCE, CFCE, EnCE, and ACE.

Avalon Cyber is proud to work with clients in industries that include financial services, legal, healthcare, manufacturing, and telecommunications, who seek a greater level of data security – and we stand ready to assist with your cybersecurity needs too.

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

*https://atlasvpn.com/blog/rdp-attacks-surged-by-330-in-the-us-amid-pandemic

AVALON Cyber

QUESTIONS?

For more information on any of our services, please contact:

Ian Gattie
Director of Marketing
ian.gattie@teamavalon.com