Understanding Remote Desktop Protocol Threats

Devolutions

WHAT IS SURPRISING IS THAT SO MANY COMPANIES REMAIN UNAWARE OF THE RISKS THAT COME WITH POTENTIALLY EXPOSING RDP OVER THE INTERNET

The recently reported hack of LabCorp – one of the largest blood testing labs in the U.S. – has raised some legitimate questions about the defense strategies of corporations in an era when **cyber attacks can happen at any time**.

While there are probably many factors that led to the attack, it's worth focusing on Windows Remote Desktop Protocol (RDP).

https://www.youtube.com/watch?time_continue=2&v=tEmAl3JKWaY

Targeting RDP

It's not surprising that the hackers went after RDP. Windows services are very attractive as they are bound to an Active Directory domain for authentication. If multiple Active Directory domain trusts are badly configured, hackers can confirm credentials for internal and other restricted domains.

However, what IS surprising is that **so many companies remain unaware** of the risks that come with potentially exposing RDP over the Internet. Once hackers breach RDP, they can validate user accounts, guess passwords, and then infect multiple systems with ransomware like SamSam — which is what happened at LabCorp.

Brute Force and Password Spraying

Furthermore, it is not as if the risks of using RDP are hidden. There are many articles on the web that warn companies about various types of attacks. These include a brute force method, in which **automated software** is used to generate a large number of password (or PIN) guesses, as well as password spraying, in which a strategically-chosen password is used to attempt logins across multiple accounts. Password spraying also allows hackers to attempt many logins without locking out users. The list of potential victims is often built from publicly available sources of information such as **Google, LinkedIn, and Facebook**.

Overconfidence in RDP

RDP, just like any other service, is a piece of software. If exposed on the Internet, it can be breached and exploited. Have we forgotten EternalBlue from the Microsoft security bulletin MS17-010 last year? A remote code execution vulnerability on Windows systems — discovered and kept secret by the NSA — was leaked publicly, and weaponized by hackers months later.

I'm not saying that RDP doesn't have its uses. But the overconfidence that some companies place in this service continues to amaze me. **Assuming that RDP can be breached should be part of the overall security strategy.**

RDP + MFA = Not Bulletproof

As many have pointed out, RDP should never be exposed directly to an untrusted environment such as the Internet. And some people recommend only multi-factor authentication (MFA) for added security. I strongly disagree. Here is why: to be truly effective, MFA must be uniformly applied to the perimeter. In a penetration test two years ago, I witnessed a company expose a VPN enforcing 2FA, but the mail service OWA was exposed without 2FA!

As you might expect, the penetration tester did indeed successfully guess a valid pair of credentials (using the password spraying technique described above), and accessed the victim's mailbox. Configuration procedures and the secret for the second factor (a soft token) were sent by email to the compromised employee when he got hired. From there, it was just a matter of following the procedures in the email to install the second factor on the penetration tester's own phone, and obtain unauthorized access to the corporate VPN.

I admit that in this scenario, there were other problems besides the use of **2FA (such as 2FA information sent in cleartext via email, email retention policy, etc.)**. But it still makes the point that hackers can be creative to circumvent defense measures.

TL;DR

Many companies don't clearly understand how the cyber security kill chain works, or the various modus operandi of hackers. The overconfidence in RDP (and other Windows services) makes companies vulnerable. RDP services should be hidden behind a 2FA enforced VPN at all times, and every system on the perimeter that may leak information about users should also have 2FA uniformly enforced. A strong password policy is also vital!