RDP WILL EXPLOITED AROUND THE GLOBE.

Every day around the world, we are seeing many news about how the “attackers” trying to break into corporate networks.

Couple weeks ago a new vulnerability was release (CVE-2019-0708) Remote Desktop Services Remote Code Execution Vulnerability Aka **BlueKeep**, when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

What is RDP?

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 are familiar with. Software clients connect to computers running RDS using RDP (the Remote Desktop Protocol).

Why this is interesting?

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.

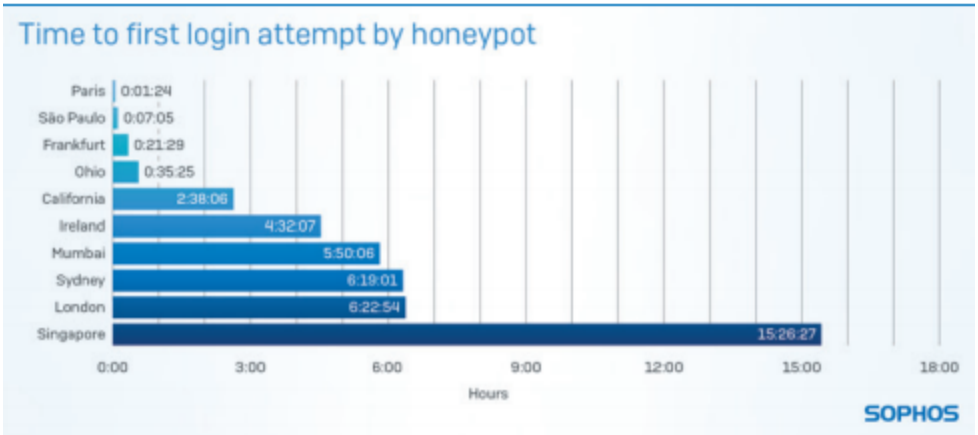
The expectations were eventually a BlueKeep exploit will be used to self-replication malware, the predictions were correct. We are seeing new ransomware attacks using BlueKeep for self-replication.

A new research for ShophosLabs, they shows how will increase the attacks and search for RDP protocol on internet.

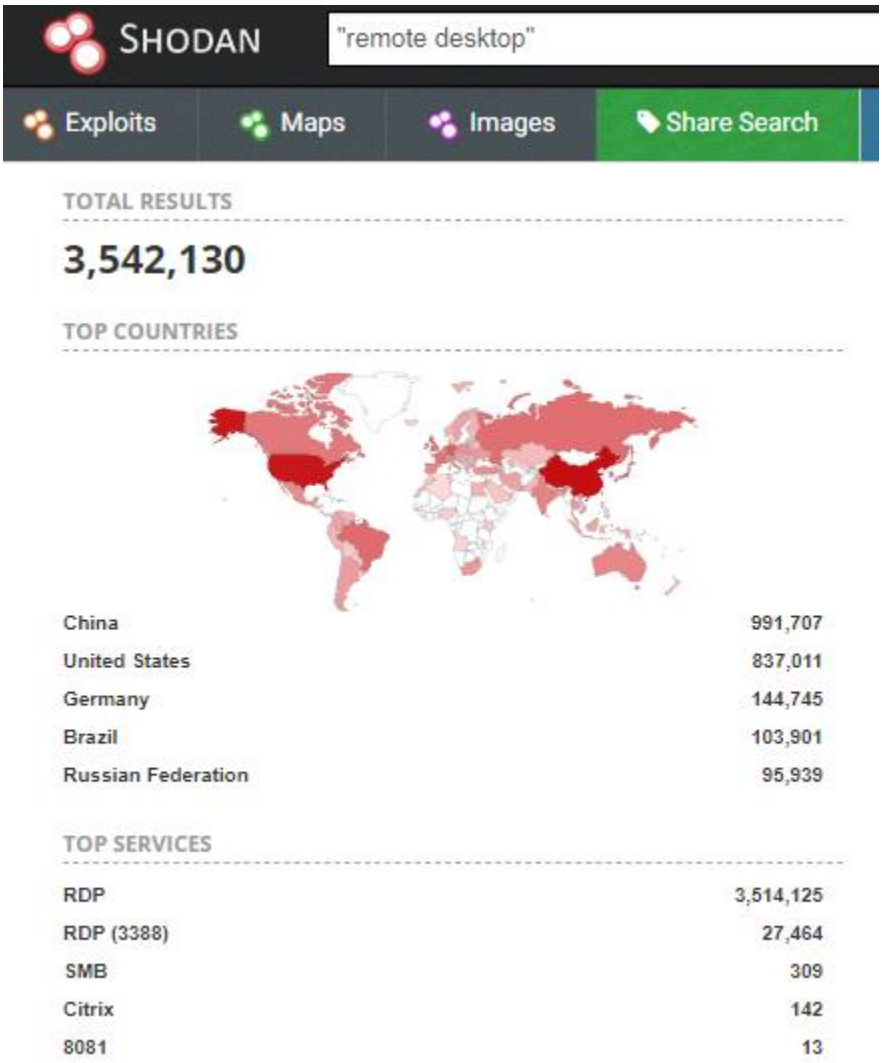
Honeypots

They were set up a couple honeypots on Amazone EC2 windows devices running windows server 2019, they have deployed in a different regional data centers.

The first honeypot to be discovered was found just one minute and twenty-four seconds after it was switched on. The last was found in just a little over 15 hours



A lot of more business is using RDP and they exposed this weak protocol to internet. On my last searched. I found this 3,542,130 devices connect to internet.



What to do?

- Disable RDP if you don't need it.
- Patch your server with the last version.
- Avoid use weak passwords for your admin accounts.
- Two-factor authentication.
- Make RDP accessible only via a VPN.

Conclusion.

This is not a new technic. It's only a combination between brute force password and a vulnerability on RDP, 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.

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.

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

Full Shophos Research Here

Official vendor vulnerability site Here

Exploit Here