



Data Vulnerability Presentation

Ransomware Attack at PRAMP's 842-B Station

Alberta Airsheds Council - Technical Committee Meeting

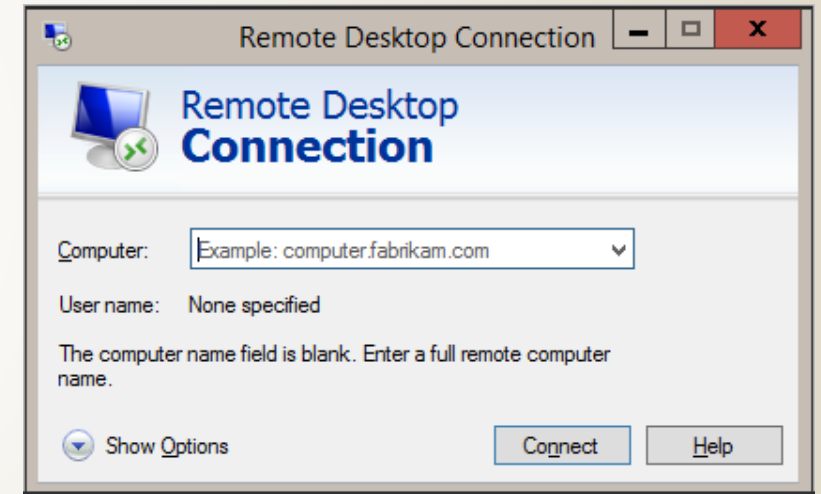
Tuesday, January 10, 2023



Events

Legitimate Access

- In early July 2022, a legitimate remote access was made to an Ultimate Logger by a technician using Window's Remote Desktop Protocol (RDP).
- To allow this, a port was opened on the modem's firewall (port 3389, the standard RDP port)



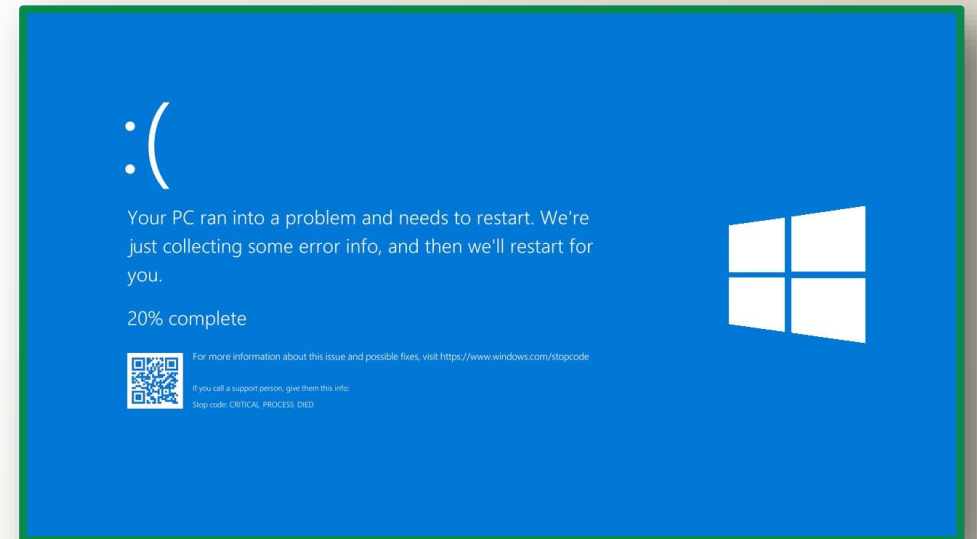
Modem Firewall Procedure

- On completion of such connections, it is necessary to both close the port and reboot the modem.
- Prior testing had shown that, without the reboot, active connections prevent the modem (Bluetree 6800-series) from closing the port - even though it reports it as closed.



Something Went Wrong

- On July 26, the data link with the station was lost.
- On arrival at the station the next day, the PC was found to be infected with ransomware. The machine was physically disconnected from all networks and turned off.





Investigation

The security system was “off” ...

- It is known that, when open, port 3389 attracts malicious log-in attempts within minutes - thus active connections are virtually guaranteed.
- The port closing/reboot was not performed correctly once the tech had finished with the remote connection. This left port 3389 open to the internet.



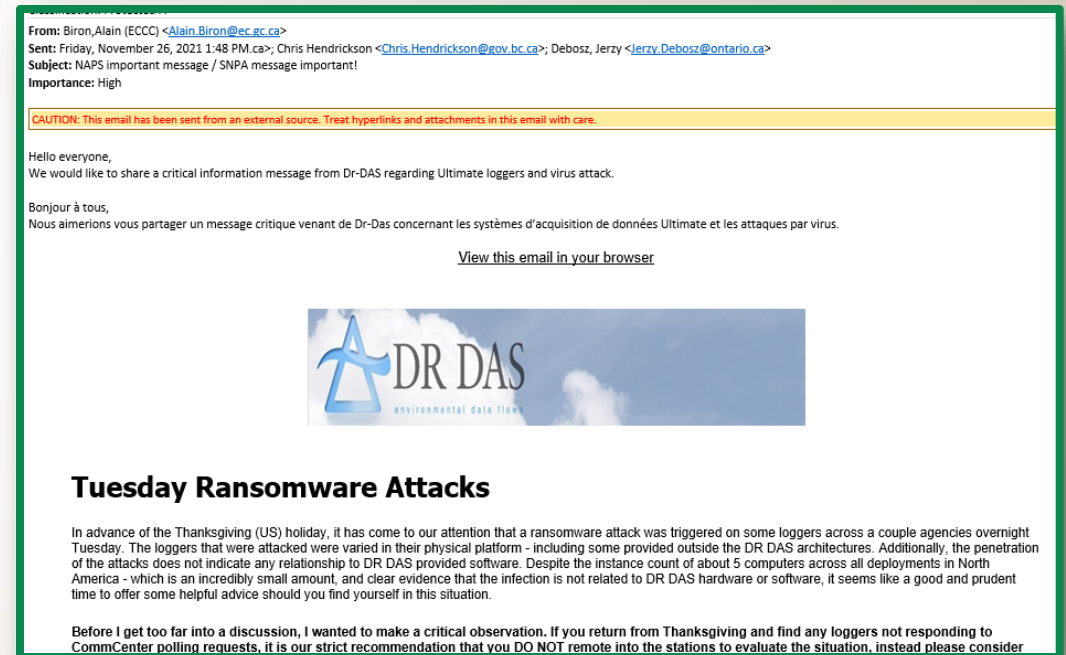
... and they had the key to the front door!

- With the port left open, the PC would have been subjected to continuous log-in attempts from bots running known combinations of usernames and passwords.
- The Ultimate machine was using the default DR DAS user/password combination



How did the bot/virus/ransomware obtain the default username and password?

- Not entirely sure.
- There have been known attacks on DR DAS systems and Ultimate loggers.
- One of the first things bots do when a system is compromised is scour for other access information and security credentials.



Consequence

- Approximately 3 days of ambient monitoring data from PRAMP's 842 monitoring station were lost.
- Removed the data-logger from the station and replace with a back-up unit since the compromised Ultimate could not be restored in the field.



Response

Improvements Made on PRAMP (& LICA) Servers

- DR DAS default user/password was immediately changed on every Ultimate machine to something unique.
- Remote connections are now principally made via a VPN connection removing the need to manually open/close firewall ports.
- More sophisticated anti-virus software was installed on all machines (now Cybereason)
- Bluetree modems are being replaced by something more up-to-date.

Advice from DR DAS

- Install anti-virus.
- Remote access passwords need to be strong.
- Consider changing the port (if using Ultra-VNC, Remote Desktop, etc).
- The remote modem should only accept incoming connections from the known public static IPs.
- Activity on the Ultimate should be restricted to accessing what is necessary on the machine (ie, don't check email or browse the internet).
- Avoid use of USB thumb drives.



Final Thoughts

- Establish a good sense of security.
 - Understand vulnerabilities and limitations of hardware and software (firewalls, ports, passwords, MFA, 2FA), their lifecycles and update frequency needs.
 - Follow manufacturer advice, recommendations, bulletins.
 - Cyber security complacency is a common catalyst for breaches.
 - *“Complacency is especially insidious in moments of seeming internal quiet or when cyber security incidents seem like distant statistics.”*



Thank You

- Acknowledgment: Input from Chris Wesson at Bureau Veritas