Citrix MetaFrame Remote Access Exploit

A French-Canadian man name Gabriel had a knack for tinkering with technology since he was 15, from playing games to hacking from the local PC café. One of his hobbies included looking up information on possible, mostly for fun targets online. He found an online list of IPs (<https://www.flumps.org/ip/>) and went through it looking for words like “gov” and “bank” and be able to find their netblocks.

Two softwares utilised by him were Spy Lantern Keylogger – used to keylog a targets computer while being undetected, and Citrix MetaFrame – a supervision software used to keep track of employee work and can even be used to take control of a system.

After figuring out the target utilised Citrix in its work and realising that most such systems were shipped with poor passwords and rarely changed, he targeted systems with the relevant port 1494 (Microsoft VPN Services) open and simply searched it for “password” and found the password to the bank’s firewall in time.

Given the network’s flat structure it gave him access to all systems in the organisation. He found a gold mine in the form of a security consultancy report which listed all the vulnerabilities in the system.

With the Keylogger and the incredibly poor and weak passwords (Administrator password was only 4 letters), he quickly gained access to the forms used to begin fund transfers and also how to use them all on a manual stored on the same system.

This showed a failure to understand proper security threats, they had some very beefed up physical security, but failed to have basic safety etiquette. From a single layered structure to incredibly lax password security.

The Confidentiality and Integrity were highly affected as the attacker could access and modify the systems for an extended period without any detection.

Possible control measures would be to audit all logins while working with sensitive information, better password requirements and an overall better trained staff in terms of security.