Thursday, October 6th

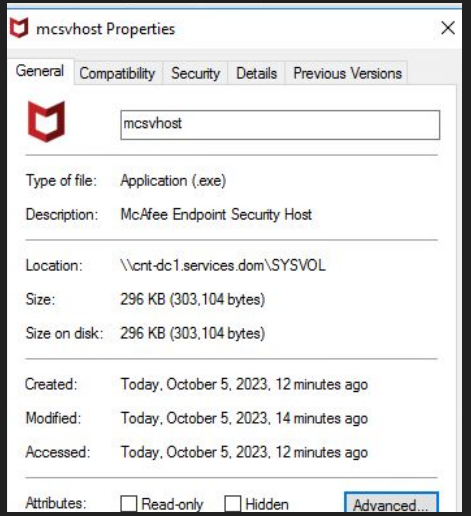
Houston Office Lazaro, Ethan, Chris, Zanovia

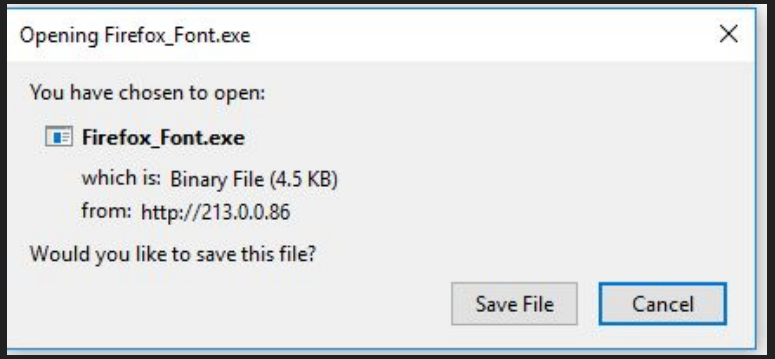
Synopsis

- We have been breached
- Malicious code injected onto tech.com
- Threat actor gained the domain admin’s password
- Startup script was implemented
- Domain controller compromised
- Firefighter or reimage the system

What happened?

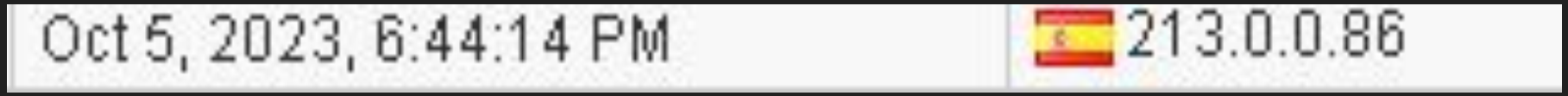
- 18:43 Spanish IP accessed www.tech.com
- 18:50 Injected XSS into company website
  - Pop-up
  - Dropper
- 18:55 User 055 typed in admin password
- 19:00 Accessed Domain controller
- 19:00 Keylogger added into startup script





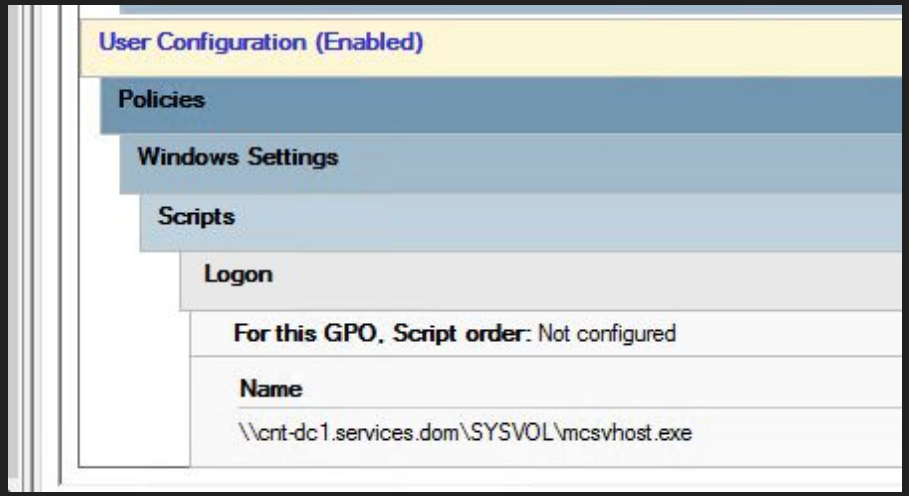
Who caused it?

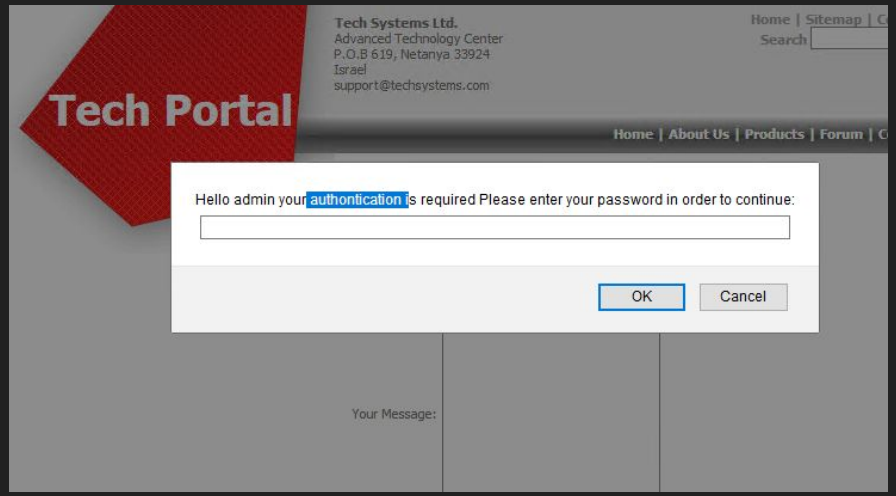
- Threat actor with Spanish IP
- Known nefarious IP address



Why did it happen?

- User055 entered admin password into fake authentication field
- Threat was able to install keylogger
- Lack of website security





Lessoned Learned and Next Steps

- Create group policy for startup script
- Web developer update website
  - Remove XSS
  - Automated vulnerability scanning
  - Implement WAF (Web Application Firewall)
- End user education
  - Update employee passwords
  - See something, say something
- Reimage all systems (known point of entry)