Incident Report: MR-10308-PowershellScriptAnalysis

Date: 10-14-2021

Executive summary:

I was tasked with analyzing a PowerShell script that was thought to be dangerous. The tool I used for this story was HashMyFiles.

Conclusion:

As stated earlier, I was tasked with analyzing a PowerShell script that was thought to be suspicious. Turns out it was. I found out that it was a keylogger. With a keylogger, an attacker can capture all of your keystrokes and potentially retrieve sensitive information such as your email and password to your bank account, social media, etc.

1. **What is the SHA256 hash value for this script?**
    a. 2b432ca2f03d4250736f92e09c7075d9fe597cf6bb2b7410f206b83ab2cf09fc
2. **What email was used to send and receive emails?**
    a. chaudariparth454@gmail.com
3. **What is the password for this account?**
    a. ujgfdafsd546562
4. **What port is the script using for SMTP?**
    a. 587
5. **What DLL is imported to help record user keystrokes?**
    a. user32.dll
6. **What folder is the generated text file put in?**
    a. keylogger.txt