



6-1 Discussion: Securing External Scripts



Listen

[Back to Topic](#)

I like to MoveIT, Move... NOOOOO!!!!

Andrew Yon IV posted Aug 6, 2024 18:04

[Subscribe](#)

By now I am sure many of you may have already forgotten about the MOVEit attacks that took the news agencies by storm last year, when C10p promised not to release any data they stole from the governments but would not hesitate to do so from the thousands of businesses that they farmed with the assistance of the automated backup software MOVEit.

<https://www.lepide.com/blog/the-moveit-attack-explained/>

Directly from that article: "Some of the IoCs associated with the MOVEit attack include:

- Scripts or webshells uploaded to the C:\\MOVEit Transfer\\wwwroot\\ folder, such as backup.aspx, backup.aspx.cs, backup.aspx.designer.cs, backup.aspx.resx, download.aspx, download.aspx.cs, download.aspx.designer.cs, download.aspx.resx."

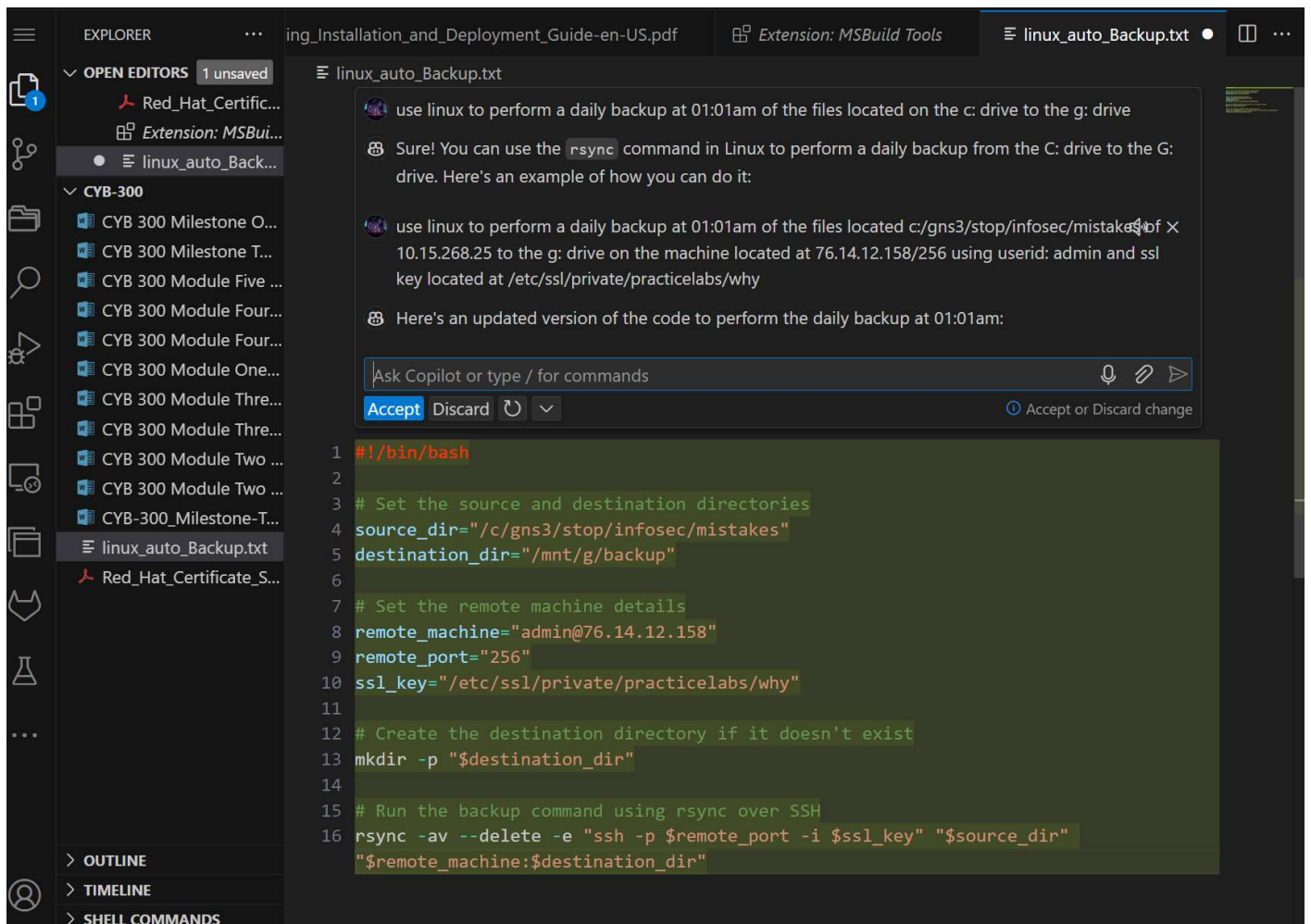
So they were marketing a bunch of automated scripts with a fancy interface as a backup solution. I understand it is hard to get good IT personnel for small to mid-sized businesses, but this was huge companies like BBC, British Airways, THE US GOVERNMENT. Surely they could afford to pay an intern to sit there and watch the percentage bar on a backup reach completion before hitting a mouse button

to start the next step. It wasn't like these companies went out and downloaded some untested script from github and got whacked, they were using an NSA approved application that was supposed to be providing secure transfer of their data to a secured backup service. Umm, next time give me the IP address and folder name to place my own backups. You know what, I will just have the helpdesk guy at my remote office monitor the backup servers at his location thank you very much.

If you feel the need to save a few hours of script writing with a few hours of googling and then copy and pasting code into your software, make sure to vet your source. If you can't do that, make sure to go through the code thoroughly and make sure that it doesn't have any unintended destinations built into it. Get a copy of VS Code, SNYK, and an IDE for whatever language (Linux, Java, Python, HTML, C++, Cobol, etc) that you are writing your code in and have it checked using the SNYK AI to verify that it isn't placing vulnerabilities in the software that you are creating, **HEY THEY ARE ALL FREE TOO**. Chat AI can write good code if worded correctly, Chat AI can write bad code if worded correctly, Chat AI will put vulnerabilities into your code if you don't know what you are doing.... You have been warned. VS Code has it's own AI for coding assistance and it works pretty good, add SNYK to it and SNYK will prevent it from being stupid. However, it has one issue where if you perfectly describe something that is already commercially available it will not duplicate that code.

<https://snyk.io/blog/top-5-vs-code-extensions-security/>

I was attending a bootcamp for full stack development and can highly recommend SNYK. It makes life so much easier. VS Code takes a little getting used to but if you are developing (typing) a lot of code, it can make life a lot easier once you get used to it. Like MS Word it will underline error in red, mark suggested corrections in blue, and even through up little light bulbs next to the line numbers where it thinks you might be able to right click and simplify your code to improve functionality.



Happy coding y'all.

image.png

(330.35 KB)

Reply to Thread

Filter by: **All Posts** ▼ | Clear filters

Show: **Threaded**

There are no replies in this thread


Reply to Thread

 Reflect in ePortfolio



Activity Details

Task: Reply to this topic

 Available on Aug 3, 2024 20:59. **Submission restricted before availability starts.**

Assessment



Discussion Rubric:
Undergraduate