Deakin University

Real World Practices for Cyber Security

OnTrack Submission

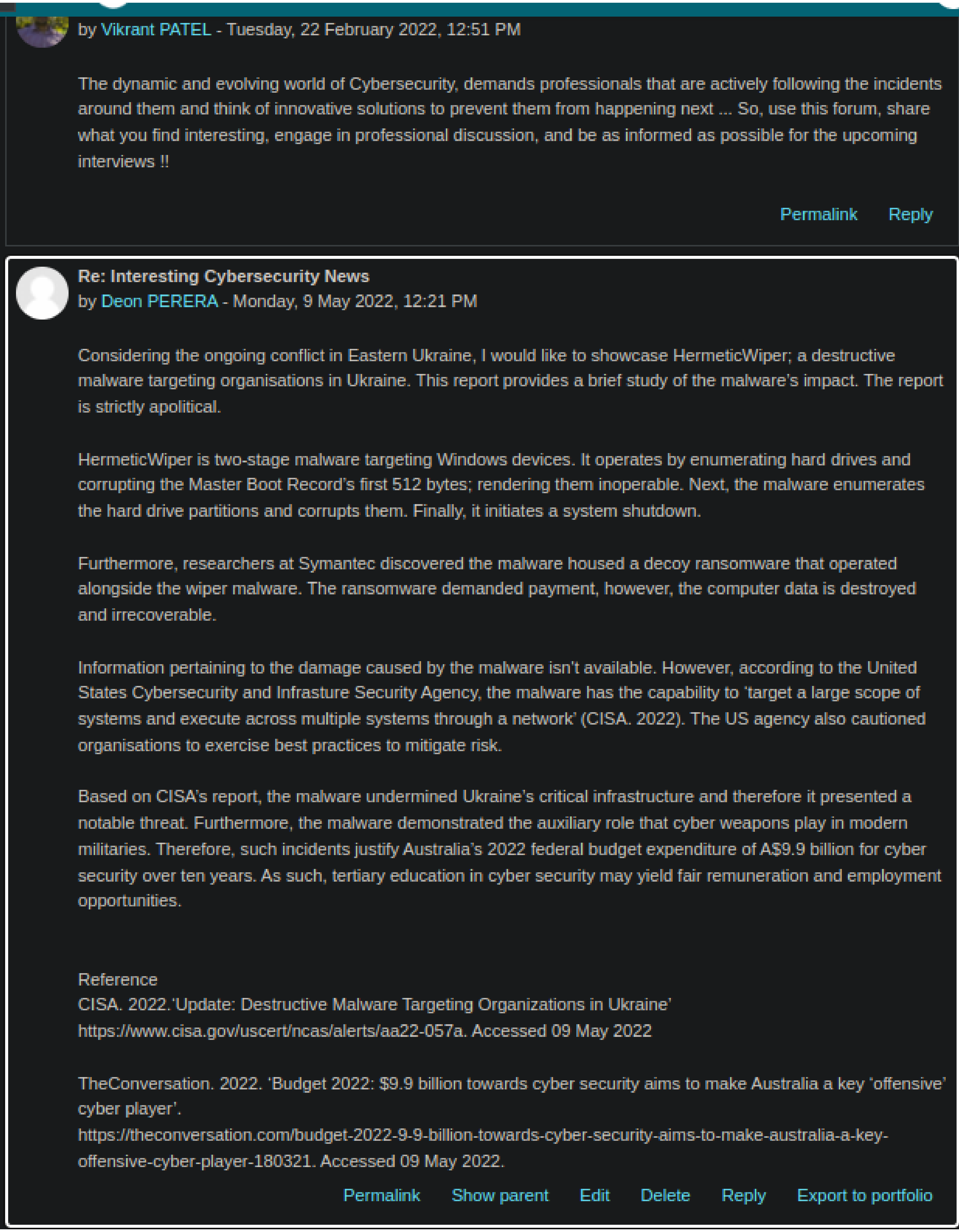
Cybersecurity Incident News

Submitted By:
Deon Perera
pereradе
2022/05/09 12:28

Tutor:
Vikrant Patel

May 9, 2022

Produced by Doubtfire



by Vikrant PATEL - Tuesday, 22 February 2022, 12:51 PM

The dynamic and evolving world of Cybersecurity, demands professionals that are actively following the incidents around them and think of innovative solutions to prevent them from happening next ... So, use this forum, share what you find interesting, engage in professional discussion, and be as informed as possible for the upcoming interviews !!

Re: Interesting Cybersecurity News
by Deon PERERA - Monday, 9 May 2022, 12:21 PM

Considering the ongoing conflict in Eastern Ukraine, I would like to showcase HermeticWiper; a destructive malware targeting organisations in Ukraine. This report provides a brief study of the malware's impact. The report is strictly apolitical.

HermeticWiper is two-stage malware targeting Windows devices. It operates by enumerating hard drives and corrupting the Master Boot Record's first 512 bytes; rendering them inoperable. Next, the malware enumerates the hard drive partitions and corrupts them. Finally, it initiates a system shutdown.

Furthermore, researchers at Symantec discovered the malware housed a decoy ransomware that operated alongside the wiper malware. The ransomware demanded payment, however, the computer data is destroyed and irrecoverable.

Information pertaining to the damage caused by the malware isn't available. However, according to the United States Cybersecurity and Infrasture Security Agency, the malware has the capability to 'target a large scope of systems and execute across multiple systems through a network' (CISA. 2022). The US agency also cautioned organisations to exercise best practices to mitigate risk.

Based on CISA's report, the malware undermined Ukraine's critical infrastructure and therefore it presented a notable threat. Furthermore, the malware demonstrated the auxiliary role that cyber weapons play in modern militaries. Therefore, such incidents justify Australia's 2022 federal budget expenditure of A$9.9 billion for cyber security over ten years. As such, tertiary education in cyber security may yield fair remuneration and employment opportunities.

Reference
CISA. 2022.'Update: Destructive Malware Targeting Organizations in Ukraine'
https://www.cisa.gov/uscert/ncas/alerts/aa22-057a. Accessed 09 May 2022

TheConversation. 2022. 'Budget 2022: $9.9 billion towards cyber security aims to make Australia a key 'offensive' cyber player'.
https://theconversation.com/budget-2022-9-9-billion-towards-cyber-security-aims-to-make-australia-a-key-offensive-cyber-player-180321. Accessed 09 May 2022.