Cyber Attack on U.S. Armed Forces & Defense Industry

By cybleinc

Published: 2022-02-25 · Archived: 2026-04-05 21:31:55 UTC

U.S. Armed Forces/Defense Industrial Base Under Cyber Attack

U.S. Armed Forces/Defense Industrial Base Under Cyber Attack

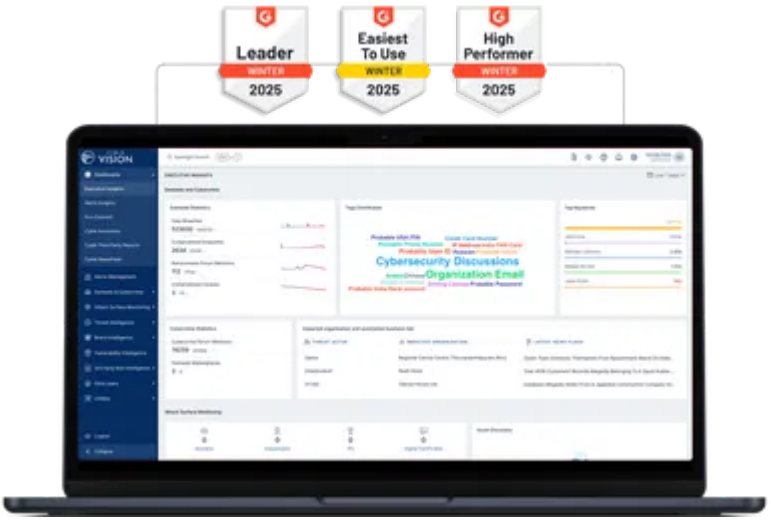
Cyble Research Lab identified a pro-Russian Threat Actor launching a campaign against the US Army and Defense Industrial Base companies.

Introduction

The threat of Russian Advanced Persistence Threat (APT) cyber activities are more imminent and pose a greater danger to the United States (US) as Russian President Putin decided to launch a full-scale attack on Ukraine. As reported by the White House, Russian APT highly likely launched cyber-attacks against Ukraine's Ministry of Defense and bank sector a few days before the open military confrontation with Ukraine. Therefore, it is highly likely that Russian APT cyber-attacks would also extend to Ukraine's allies, such as the US.

The US Intelligence Community (IC) is aware of the Russian APT cyber threat to the Homeland. On February 16, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released an alert on Russian state-sponsored APT cyber activities against cleared Defense contractor networks to obtain sensitive US Defense information and technology. Furthermore, on February 20, the Federal Bureau of Investigation (FBI) released a report to inform the private sector about the threat of Russian state-sponsored APT cyber activities.

Consequently, the Cyble Research Lab (the Lab) identified a pro-Russian Threat Actor (TA) launching a campaign against the US Army and Defense Industrial Base companies, such as Lockheed Martin Corporation. This blog would reveal some details about the TA and the campaign itself.



TA Profile

During our Deepweb search in various forums, security researchers at the Lab identified a prolific TA going by the name NetSec aka ScarFace_TheOne aka Scarfac33 and targeting the U.S. infrastructure. Our research indicated that the TA has been active on the forum for over two years, taking part in various cyberattacks with diverse geographical and dynamic industry footprints. The TA's malicious cyber activities have helped earn an aggressive reputation, besides resulting in the TA being widely endorsed and acclaimed by other notable malicious actors such as Pompompurin, Holistic-K1ller, and IPegFemBoys.

We found several instances wherein the TA has revealed details of malicious cyberattacks targeting the U.S. Department of Defense. For example, on **August 12, 2021**, the TA published a thread named 'Raiding the Army' in which it claimed to have administrator access to some websites of the U.S. Army, as shown in Figure 1, Figure 2, and Figure 3.

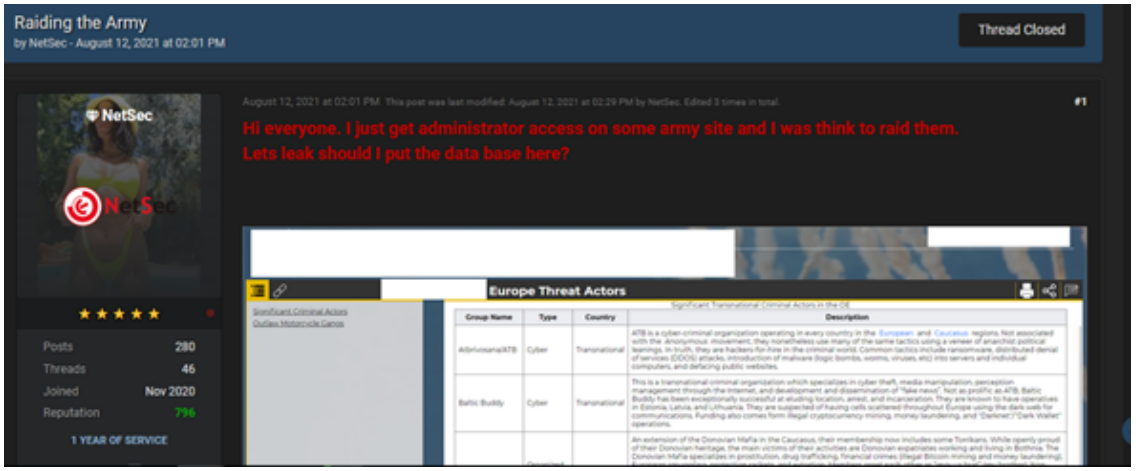


Figure 1: TA claims administrator access to the U.S. website (Part 1)

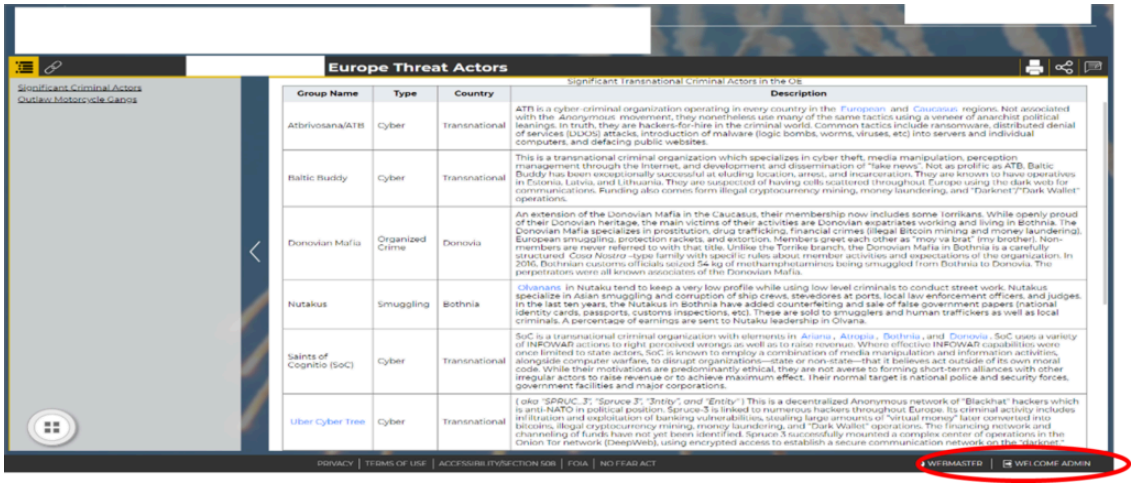


Figure 2: TA claims administrator access to the U.S. website (Part 2)

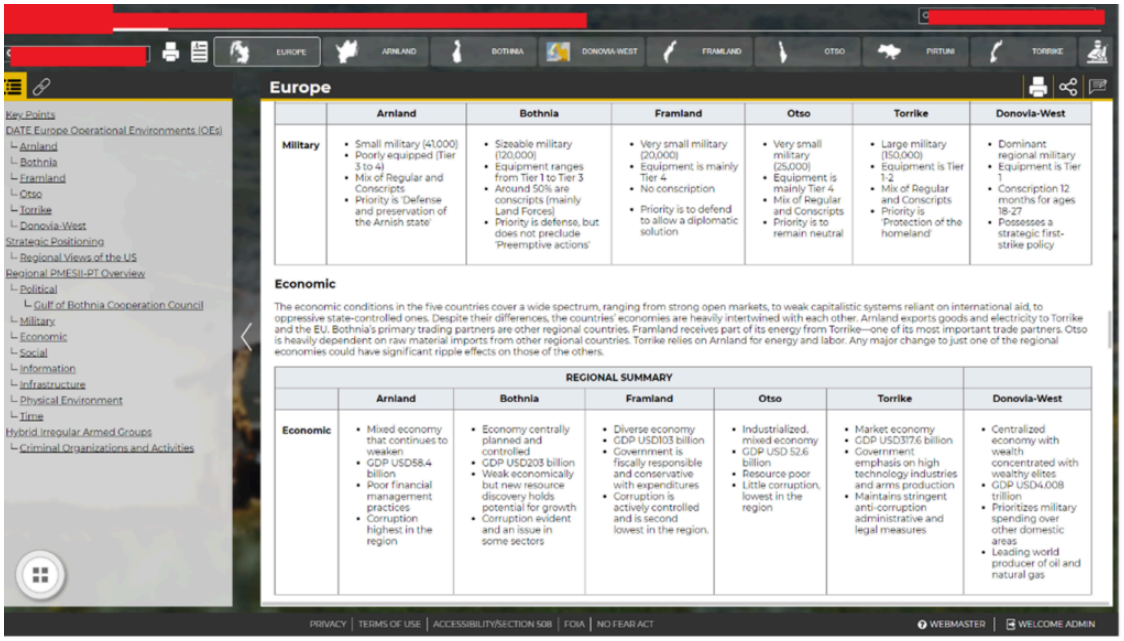


Figure 3: TA claims administrator access to the U.S. website (Part 3)

Our analysis revealed that the TA has also initiated various training threads related to hacking email IDs with an example of fbi.gov example showing attacks like Golden Ticket Attack (a form of Active Directory attack), Remote Code Execution (RCE), SQL injection, etc. Figure 4 shows the training threads.

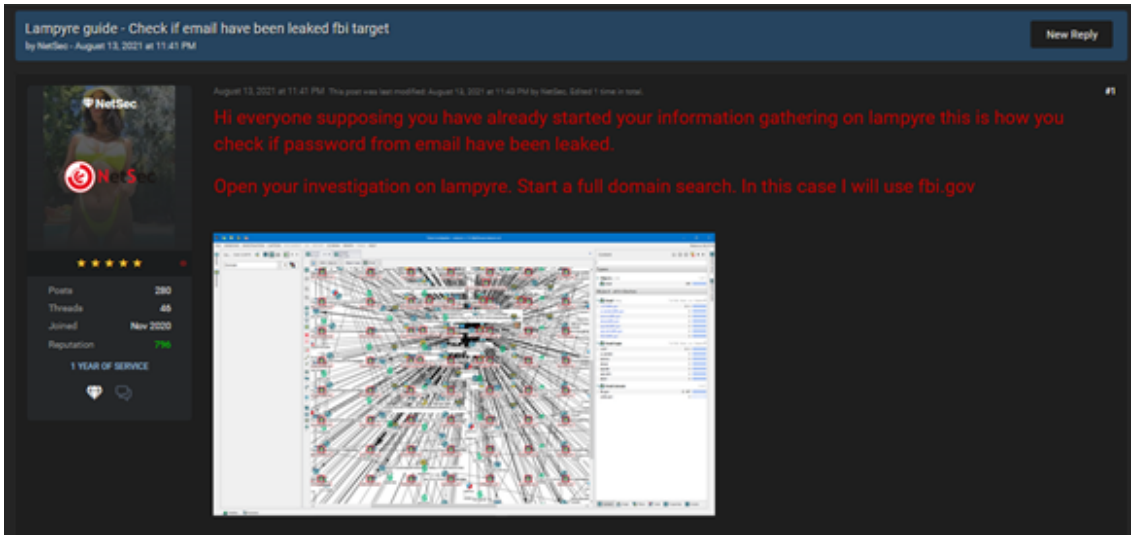


Figure 4: Hacking thread posted by the TA

#RaidAgainstTheUS Campaign

Recently, the TA has been involved in large-scale attacks on the U.S. Department of Defense (DoD), U.S. Army websites, and U.S. Defense manufacturers – such as Lockheed Martin Corporation. The TA has been conducting these attacks under the #RaidAgainstTheUS hashtag.

These attacks most likely lean on the one from August 2021. The TA claims that they coordinated with Russian TAs for over six months and found a 0-day vulnerability in a U.S. enterprise platform deriving from Program Executive Office Enterprise Information Systems (e.g., PEO EIS, eis.army.mil, etc.) to obtain the source codes of the platform. Figure 5 shows the TA's claim.

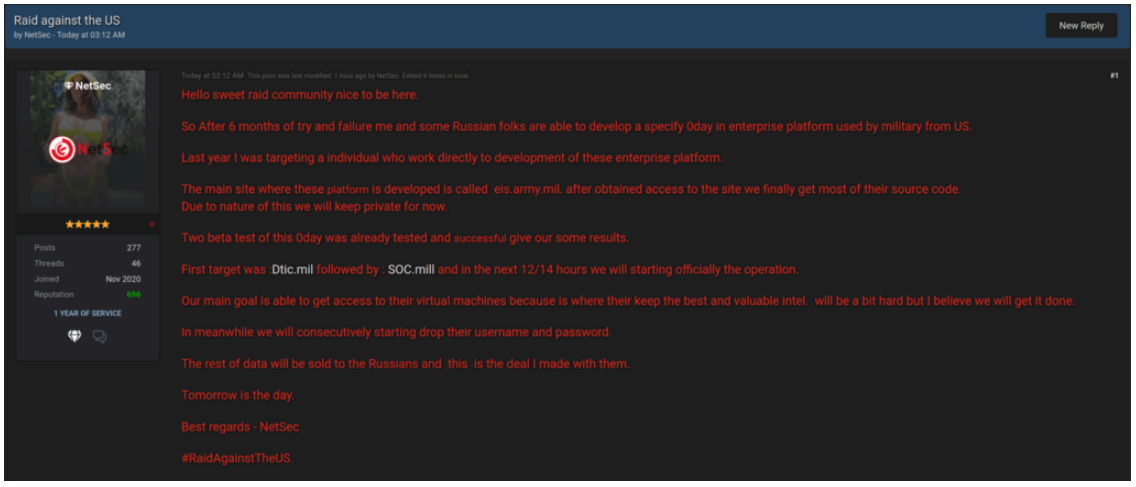


Figure 5: TA's claim finding a Zero-day vulnerability

Program Executive Office Enterprise Information Systems is a critical information systems provider that modernizes and manages the network and enterprise business systems of the U.S. Army. The TA claims to have targeted one of the developers of this enterprise platform in 2021. We suspect that these attacks could have been Beta tests to exploit the U.S. army websites, seemingly paving way for the final attack earlier this week.

Timeline of the #RaidAgainstTheUS Attacks

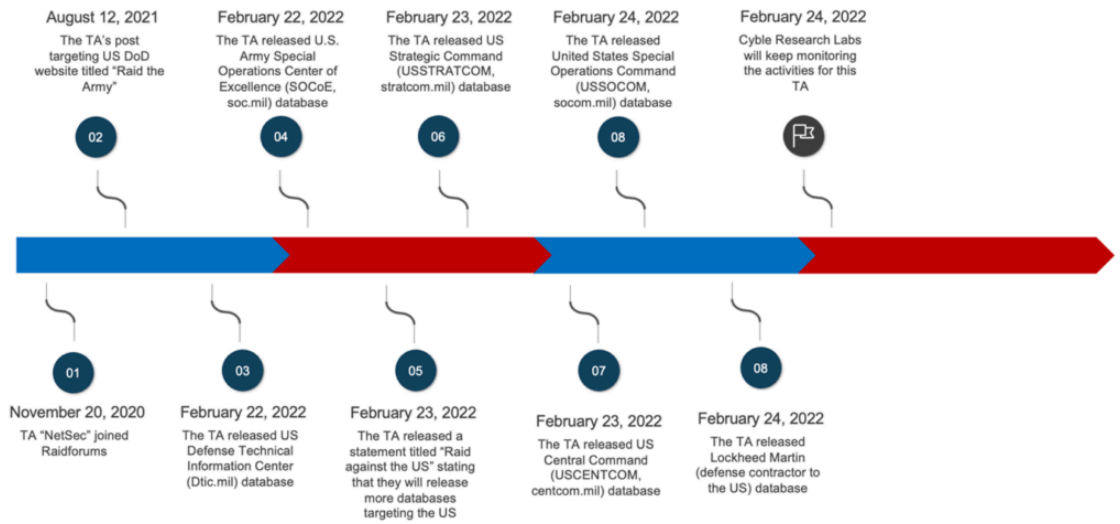


Figure 6: Timeline of the #RaidAgainstTheUS attacks by the TA

On **February 22, 2022**, the TA posted about a data leak from the Defense Technical Information Center (DTIC), as shown in Figure 7.

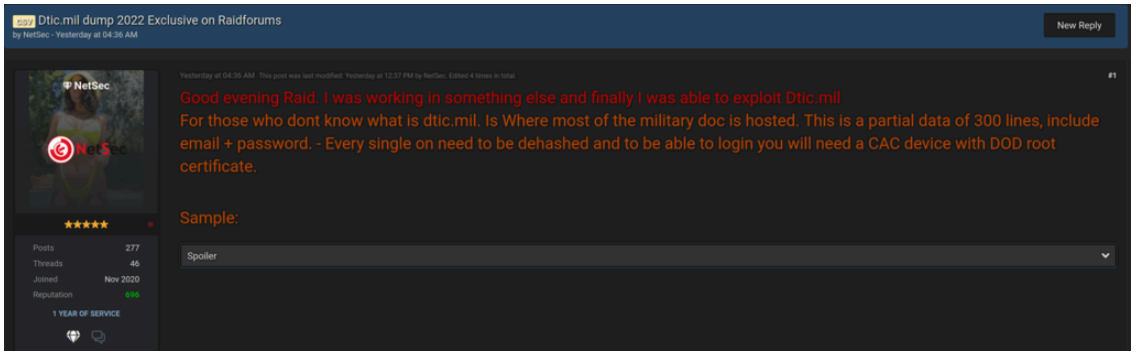


Figure 7: TA's leak from dtic.mil

The data leak consists of emails and hashed passwords belonging to DTIC, Army, and Navy personnel, as shown in Figure 8.

Figure 8: Exposed Emails and Hashed Passwords of the DTIC, Army, and Navy

In its second leak of the day, the TA leaked data from the U.S. Army Special Operations Command (USASOC), as shown in Figure 9.

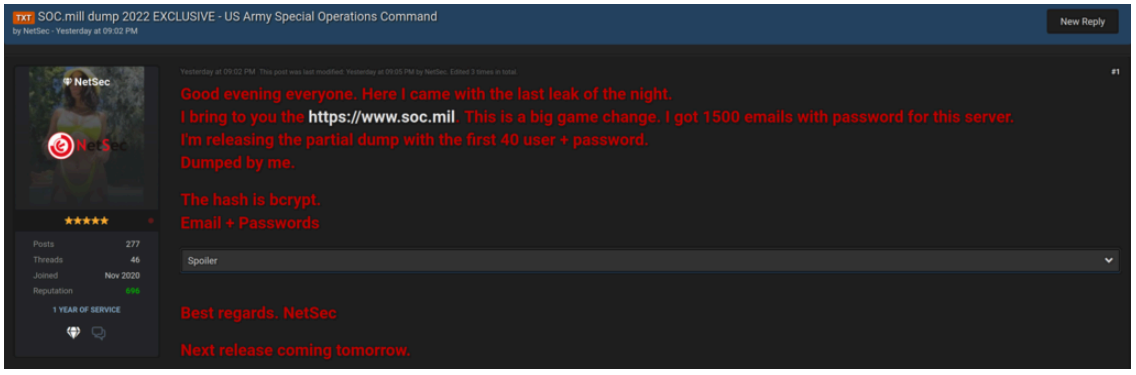


Figure 9: TA' leak from soc.mil

As per our research, the leaked data contains emails and hashed passwords of members of the USASOC, as shown in Figure 10.

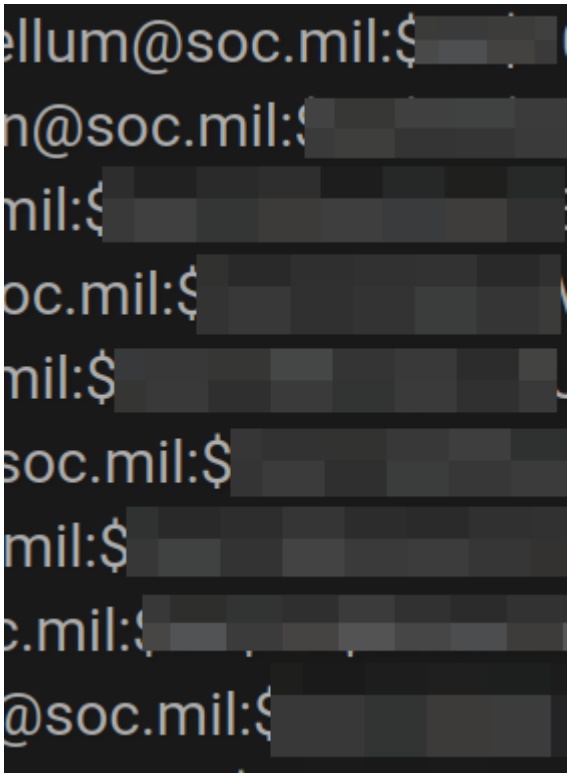


Figure 10: TA' exposed USASOC emails and hashed passwords

On **February 23, 2022**, the TA released two more leaks. First from the U.S. Strategic Command (STRATCOM), and the second from the U.S. Central Command (CENTCOM). Figures 11 and 12 show the TA's post exposing the STRATCOM members' emails and hashed passwords.

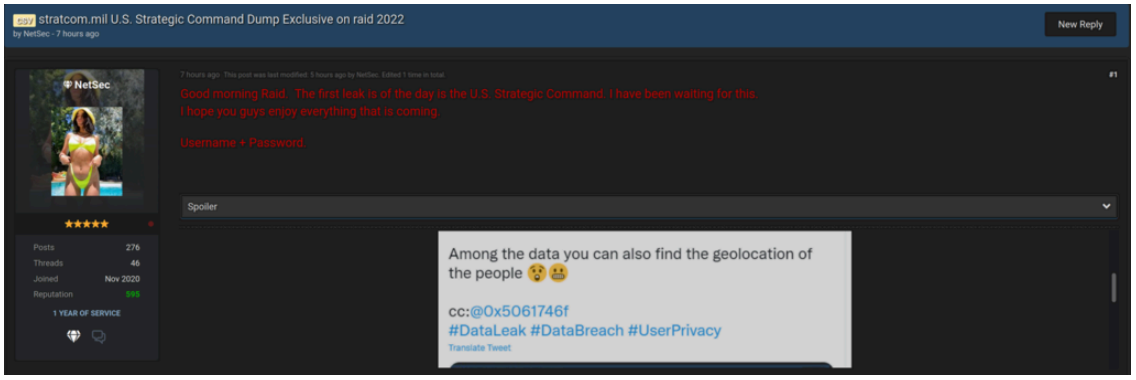


Figure 11: TA' leak from stratcom.mil

Figure 12: TA exposed STRATCOM emails and hashed passwords

Figures 13 and 14 show the TA's post exposing the CENTCOM members' emails and hashed passwords.

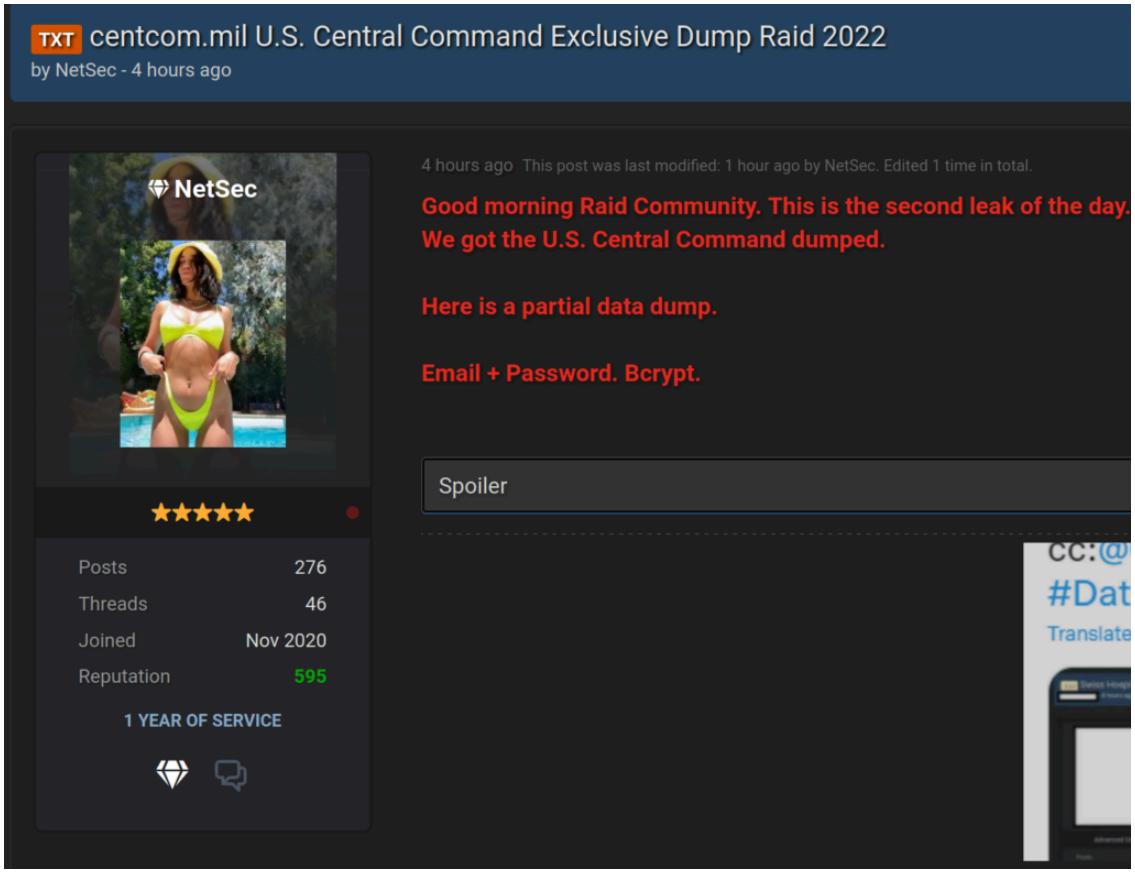


Figure 13: TA' leak from centcom.mil

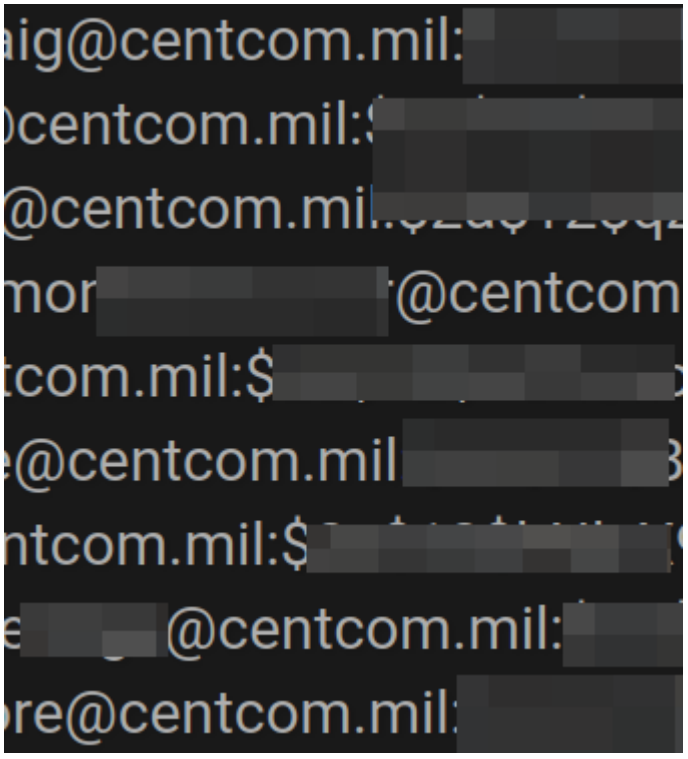


Figure 14: TA exposed CENTCOM emails and hashed passwords

On **February 24, 2022**, the TA released two leaks from the United States Special Operations Command (USSOCOM) and Lockheed Martin Corporation. Figures 15 and 16 show the TA's post exposing the USSOCOM

members' exposed emails and hashed passwords.

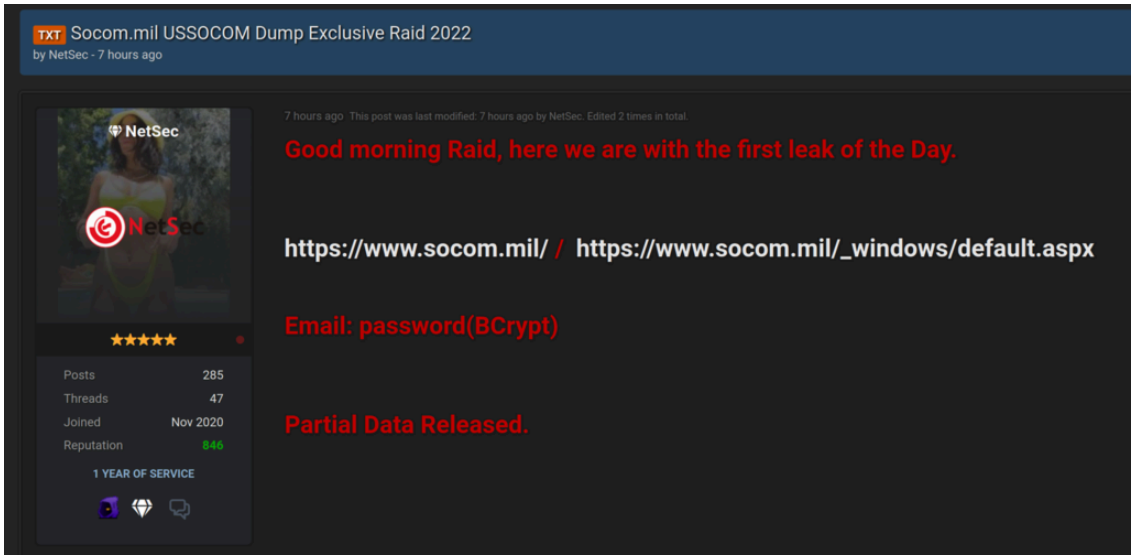


Figure 15: TA' leak from socom.mil

Figure 16: TA exposed USSOCOM emails and hashed password

Lastly, Figures 17 and 18 show the TA's post exposing the exposed emails and hashed passwords of employees of Lockheed Martin Corporation.

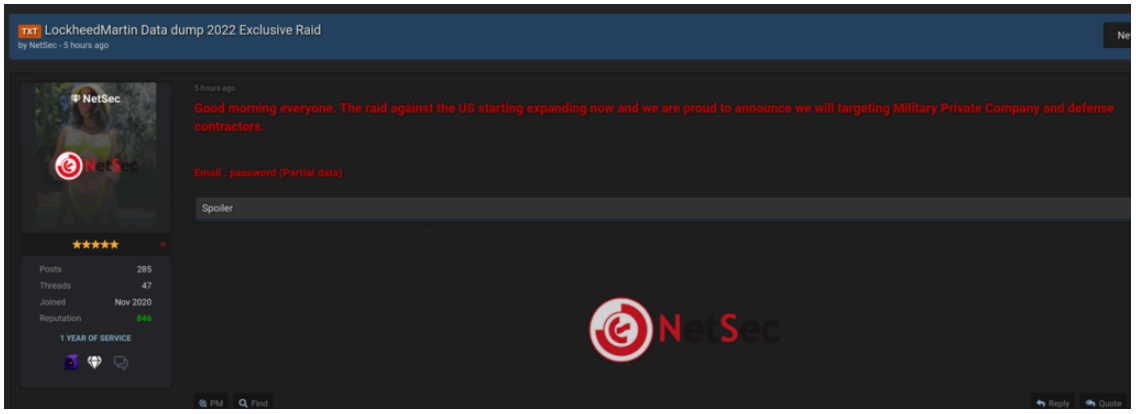


Figure 17: TA's leak from lockheedmartin.com

Figure 18: TA exposed the Lockheed Martin Corporation emails and hashed passwords

Conclusion

Our research suspects that the TA only leaks email IDs and passwords in the cybercrime forums, while a significant part of the leaked data is sold to Russia. The chatter history of the TA indicates that it already possesses data from exposed websites. There is also a likelihood that the TA launched a frontal attack on the websites mentioned above, with Russian APTs launching deeper penetration attacks to exploit the data.

Furthermore, based on the TA's claims, we can suspect that the TA's intrusion tactics are still underway despite eis.army.mil (PEO EIS) being pulled down by the U.S. IC. As a result, we suspect that the TA is likely to exploit more U.S. Armed Forces and private contractors' websites to gain information about U.S. actions and potential plans for retaliation in the case of a protracted Russian full-scale war over Ukraine.

Recommendations

- Keep the operating system and installed software in the system and server updated
- Conduct regular backup practices and maintain backups offline or in a separate network.
- Use security solutions available for Linux and IoT devices
- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Create and save your passwords with password managers.
- Change all internet-connected devices' default passwords.

Source: https://cyble.com/blog/u-s-armed-forces-and-defense-industrial-base-under-cyber-attack/