Homeland Security

OFFICE *of* INTELLIGENCE and ANALYSIS

NETWORK DEFENDER BULLETIN

CYBERSECURITY

(U//FOUO) Advanced Persistent Threat Cyber Actors Conduct Password Spray Attack Against US Pharmaceutical and Biotechnology Company

(U//FOUO) ***Scope Note:*** *This* Network Defender Bulletin *provides federal, state, local, tribal, and territorial authorities and private sector network defenders information to help detect and mitigate malicious cyber activity. While I&A considers this network defense information to be credible and actionable, this* Bulletin *is not considered finished intelligence and is being shared for the purpose of informing cybersecurity protection activities.*

(U//FOUO) Advanced Persistent Threat cyber actors on or about 30 December 2020 used an identified German virtual private server IP address to conduct a password spray attack against a US pharmaceutical and biotechnology company, according to defense reporting.

(U//FOUO) **Support to Computer Network Defense**

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Indicators of Compromise	
German IP Address	94[.]130[.]119[.]50

(U) Prepared by the Cyber Mission Center. For questions, contact DHS-SPS-RFI@hq.dhs.gov.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Source, Reference, and Dissemination Information

Definitions	*(U)* **Password Spray Attack:** A type of brute force attack where malicious cyber actors use multiple acquired or commonly used passwords to compromise one or more accounts.
Reporting Suspicious Activity	*(U)* To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form. The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Dissemination	*(U)* Federal, state, local, tribal, and territorial authorities and private sector network defenders.
Warning Notices & Handling Caveats	*(U)* Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* All US person information has been minimized. Should you require US person information on weekends or after normal weekday hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@HQ.DHS.GOV. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov. *(U//FOUO)* This report includes sensitive technical information related to computer network operations that could be used against US Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, e-mail addresses, or user names identified in this document is strictly prohibited.

Homeland Security

Office of Intelligence and Analysis
Customer Feedback Form

Product Title: _____

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: _____ **and function:** _____

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? *(Check all that apply.)*

☐ Drive planning and preparedness efforts, training, and/or emergency response operations
☐ Observe, identify, and/or disrupt threats
☐ Share with partners
☐ Allocate resources (e.g. equipment and personnel)
☐ Reprioritize organizational focus
☐ Author or adjust policies and guidelines
☐ Initiate a law enforcement investigation
☐ Intiate your own regional-specific analysis
☐ Intiate your own topic-specific analysis
☐ Develop long-term homeland security strategies
☐ Do not plan to use
☐ Other: _____

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disgree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name: _____ Position: _____
Organization: _____ State: _____
Contact Number: _____ Email: _____

[Submit Feedback ►]

Privacy Act Statement