

Unknown actor “Winter Pension” targets several companies

Intelligence Report

April 30, 2024 10:38:39 AM, 19-00006100, Version: 23

Risk Rating: HIGH | Exploitation State: No Known

Introduction

Several of our customers have been targeted by a new adversary, which, as it is currently unknown, has been provisionally named 'Winter Pension'.

Threat Detail

The new actor has used _____(1)(MITRE ATT&CK id) to initially breach into VPNs allowing attackers to connect to the internal enterprise network resources from external locations.

The Username and Password for the malicious VPN connection are the following:

Username: _____(2)

Md5: d344e534ab6289aa48c9f0c7370fe401

Password: _____(3)

Md5: ab961b82aeca81b4ccfac1dcdc1dfca3

After gaining access to the victim's network, the adversary delivered an .exe file called _____(4)

(File hash) Md5: 89edcd028b4cc015a4b8b1b02c854ddd

Once the adversary had full control of the machine, they implemented a C2 server. After analysing one of the compromised machines, we found that the C2 used in this campaign was a modified _____(5) C2 server. This is evidenced by the agent calling the C2 server on port 31337 with a TLS certificate CN = "multiplayer".

The domain name in the C2 server configuration file is encrypted in a strange language, see APPENDIX 1.

This encrypted string, when decrypted, gives the following output: _____(6)

We are continuing to investigate and will provide more information in a follow-up report.

Conclusion

Compose the flag for this challenge by combining one letter from each response:

(4.3) (3.9) (1.1) (2.4) (5.2) (6.13), encoded as (response.letter)

APPENDIX 1

[illegible]