Threat Category: Malware, PlugX

Threat Description: The YARA rule is designed to detect a send tool used in a phishing campaign reported by Area 1 in December 2018. This rule identifies specific code patterns associated with PlugX malware.

The detection mechanism focuses on identifying files that contain at least three of the following code patterns:

8b 0? 56 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? 6a 07 6a ff ff d0 8b f0 85 f6 74 14

8b 4d 08 6a 0c 6a 01 8d 55 f4 52 c7 45 f4 01 00 06 00 c7 45 f8 00 01 00 00 89 4d fc ff d0 85 c0 75 1d

55 8b ec 83 ec 20 0f b7 56 18 8b 46 10 66 8b 4e 14 89 45 e4 8d 44 32 10 66 89 4d f0 0f b7 4e 1a 57 89 45 e8 33 ff 8d 45 e0 8d 54 31 10 50 89 7d e0 89 55 ec c7 45 fa ?? ?? ?? ?? 89 7d f2 89 7d f6 ff 15 1c 43 02 10

0f b6 8d b0 fe ff ff 0f b6 95 b4 fe ff ff 66 c1 e1 08 0f b7 c1 0b c2 3d 02 05 00 00 7f 2c

c7 06 23 01 12 20 c7 46 04 01 90 00 00 89 5e 0c 89 5e 08 e8 51 fb ff ff 8b 4d 08 8b 50 38 68 30 75 00 00 56 51 ff d2

8b 1d ?? ?? ?? ?? 6a 08 50 ff d3 0f b7 56 12 8b c8 0f af ca b8 1f 85 eb 51 f7 e9 c1 fa 05 8b c2 c1 e8 1f 03 c2 89 45 f8 8b 45 f0 6a 0a 50 ff d3 0f b7 56 14 8b c8 0f af ca b8 1f 85 eb 51

Possible Attribution & Use Cases:

The rule detects a tool used in a phishing campaign.

The campaign is attributed to PlugX malware.

PlugX is a remote access trojan (RAT) used by various threat actors.

Recommended Actions:

Investigation: If this rule is triggered, investigate the affected system for signs of PlugX infection and

related activity.

Removal: Remove the identified malware and any associated malicious files.

Network Monitoring: Monitor network traffic for suspicious connections and command and control activity.

Intelligence Sharing: Share information about the PlugX activity with relevant security communities.

Author & Attribution:

Rule Author: Area 1

Rule Reference: https://cdn.area1security.com/reports/Area-1-Security-PhishingDiplomacy.pdf

Rule Date: 2018-12-19

Rule Identifier: a5b4e781-f0d1-55df-926c-2d321aa48139