# **Anthony Munoz – Report 1**

**Reason**

This alarm fired because splunk\_server “mhn-server” caught a “high” severity connection the honeypot.

**Supporting Evidence**

Event start time: 2024-11-07T19:38:11.826+00:00 AKA 7:38:11 PM

Event end time: N/A

Timezone:UTC

Source Identity:

splunk\_server “mhn-server”

Destination Identity:

Dionaea honeypot

Source Device: mhn-server

Source IP Address: 58.56.198.186 | TCP port 56241

Source Device Type: MHN\_Log located at *var*log/mhn-mhn-splunk.log

Source Email Address: N/A

Destination Device: dionaea honeypot sensor ec7c2d8e-8429-11ef-916b-000d3a556b22

Destination IP address: 20.217.82.118 | TCP port 445

Destination Device Type: dionaea honeypot sensor

Destination Email Address: N/A

File name: N/A

File MD5: ecc0433f80932193d2a399046328f726

File SHA512: f1048317a01c2f57562c7fecb8bfdc3a8024bc86299414b02a0e9878e958632caf94215badc7dd099efcb8532e007297add751b6c0919d65952e9c4cf1d76824

File Size: N/A

Signed By: N/A

Original URL:

Raw Logs:

2024-11-07T19:38:11.826279 direction="inbound", protocol="ip", ids\_type="network", sha512="f1048317a01c2f57562c7fecb8bfdc3a8024bc86299414b02a0e9878e958632caf94215badc7dd099efcb8532e007297add751b6c0919d65952e9c4cf1d76824", dest="20.217.82.118", app="dionaea", transport="tcp", md5="ecc0433f80932193d2a399046328f726", src="58.56.198.186", src\_port="56241", severity="high", type="dionaea.capture", vendor\_product="Dionaea", signature="Connection to Honeypot", dest\_port="445", sensor="ec7c2d8e-8429-11ef-916b-000d3a556b22"

Account Actions:

N/A

**Analysis**

Whois:

inetnum: 58.56.0.0 - 58.59.127.255

netname: CHINANET-SD

descr: CHINANET SHANDONG PROVINCE NETWORK

descr: Shandong Telecom Corporation

descr: No.999,Shunhua road,Jinan,Shandong

country: CN

admin-c: XR55-AP

tech-c: CH93-AP

abuse-c: AC1573-AP

status: ALLOCATED PORTABLE

mnt-by: APNIC-HM

mnt-lower: MAINT-CHINANET-SD

mnt-routes: MAINT-CHINANET-SD

mnt-irt: IRT-CHINANET-CN

last-modified: 2021-06-15T08:05:56Z

source: APNIC

Landing URL: https://wheregoes.com/trace/20246495009/

Domain age: According to IPSpamlist.com, the source IP was first seen on November 22, 2021

Reverse IP: <None. Goes back to itself.

VT: virustotal results show 58/67 security vendors flagged as malicious

IPVoid: 2/93 found on IP blocklists

- IPSpamList: First seen November 22, 2021 and last seen November 10, 2024. The category is **“MS-DS Attack”**

- PlonkatronixBL: general ip blacklist website

URLVoid: No results

URLScan.io Verdict: no verdict

Joe Sandbox Verdict: no results

TOR Exit Node: No

Historical Alerts:

N/A

Google Results:

no Google results for SHA512 hash or MD5 hash

Actions:

I decided to block the IP address on our blocklist. I’ve also blacklisted the md5 hash.

**Conclusion**

The alarm went off when our Dionaea honeypot considered this inbound traffic was malicious. According to VirusTotal, the MD5 hash is a general Trojan, with a few vendors classifying it as a wannacry attack. This evidence coincides with IPSpamList’s conclusion that this is a MS-DS attack, which is port 445 as our Splunk log indicated as well. I conclude that this is malicious behavior.

**Next Steps**

Block IP address/MD5 hash/SHA512 hash where we are able. Perhaps some research is needed because there was no results on Google when it came to the MD5 hash or SHA512 hash.