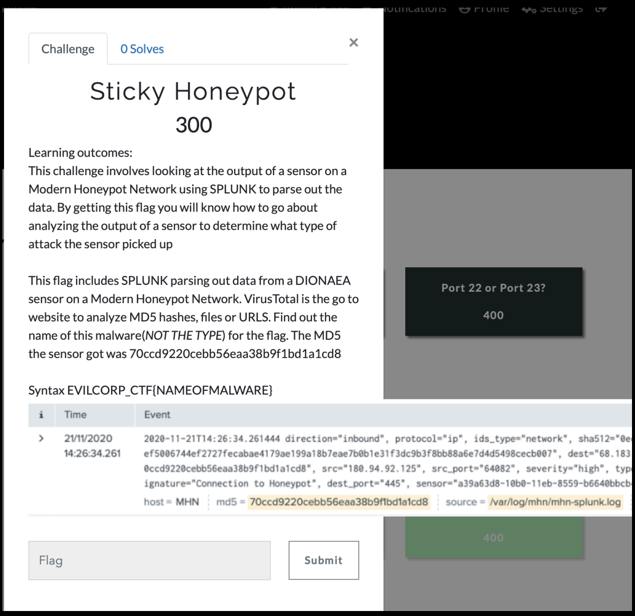
MR. ROBOT

1. In this challenge we are giving an output from SPLUNK. A Dionaea sensor has alerted an MD5 that could be potentially harmful. Using VirusTotal find the name of the potentially dangerous MD5.



Sticky Honeypot

300

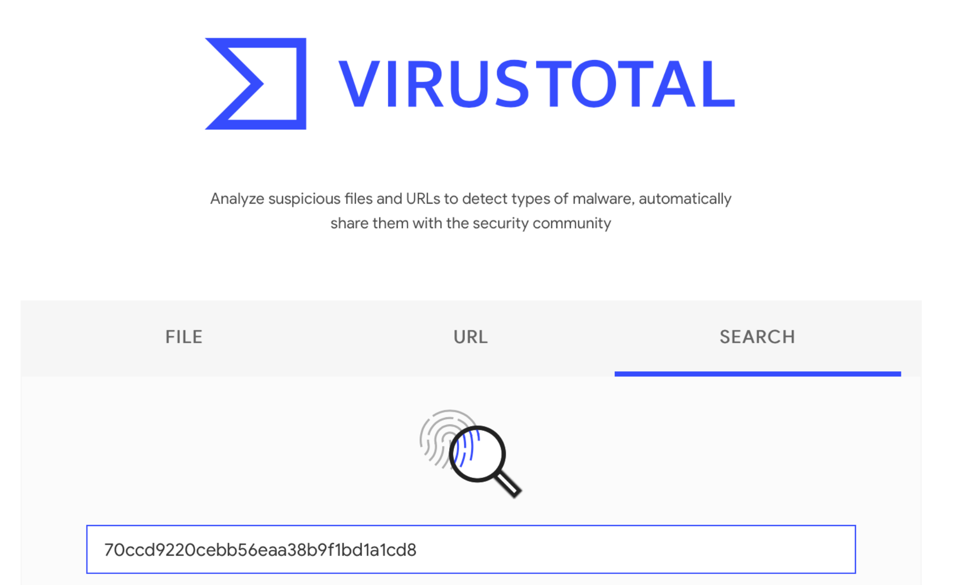
Learning outcomes:
This challenge involves looking at the output of a sensor on a Modern Honeypot Network using SPLUNK to parse out the data. By getting this flag you will know how to go about analyzing the output of a sensor to determine what type of attack the sensor picked up

This flag includes SPLUNK parsing out data from a DIONAEA sensor on a Modern Honeypot Network. VirusTotal is the go to website to analyze MD5 hashes, files or URLS. Find out the name of this malware(*NOT THE TYPE*) for the flag. The MD5 the sensor got was 70ccd9220cebb56eaa38b9f1bd1a1cd8

Syntax EVILCORP_CTF{NAMEOFMALWARE}

```
i  Time          Event
>  21/11/2020    2020-11-21T14:26:34.261444 direction="inbound", protocol="ip", ids_type="network", sha512="0e
   14:26:34.261  ef5006744ef2727fecabae4179ae199a18b7eae7b0b1e31f3dc9b3f8bb88a6e7d4d5498cecb007", dest="68.183
                 0ccd9220cebb56eaa38b9f1bd1a1cd8", src="180.94.92.125", src_port="64082", severity="high", typ
                 ignature="Connection to Honeypot", dest_port="445", sensor="a39a63d8-10b0-11eb-8559-b6640bbcb
                 host = MHN   md5 = 70ccd9220cebb56eaa38b9f1bd1a1cd8   source = /var/log/mhn/mhn-splunk.log
```

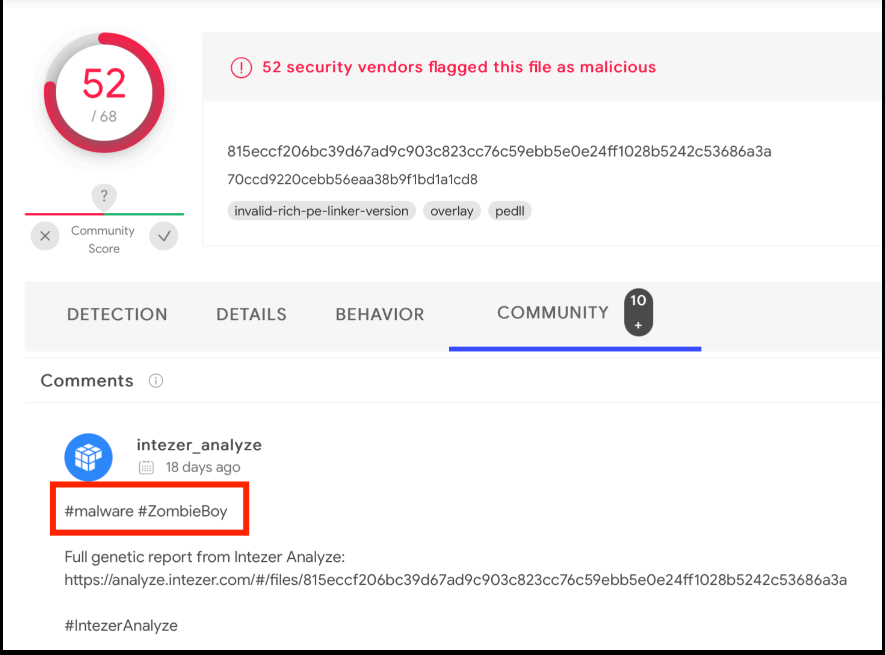
2. Copy the MD5 and paste the MD5 into the search bar in VirusTotal.com



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

70ccd9220cebb56eaa38b9f1bd1a1cd8

3. Searching the MD5,VirusTotal has shown that this file is malicious and checking what the community has said about this malware says its called a ZombieBoy malware.



52 security vendors flagged this file as malicious

815eccf206bc39d67ad9c903c823cc76c59ebb5e0e24ff1028b5242c53686a3a

70ccd9220cebb56eaa38b9f1bd1a1cd8

Comments

intezer_analyze

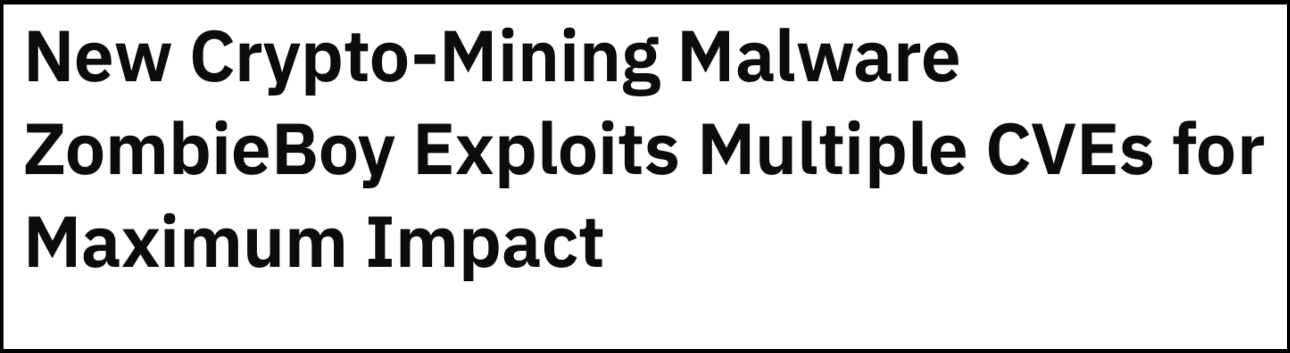
18 days ago

#malware #ZombieBoy

Full genetic report from Intezer Analyze:
https://analyze.intezer.com/#/files/815eccf206bc39d67ad9c903c823cc76c59ebb5e0e24ff1028b5242c53686a3a

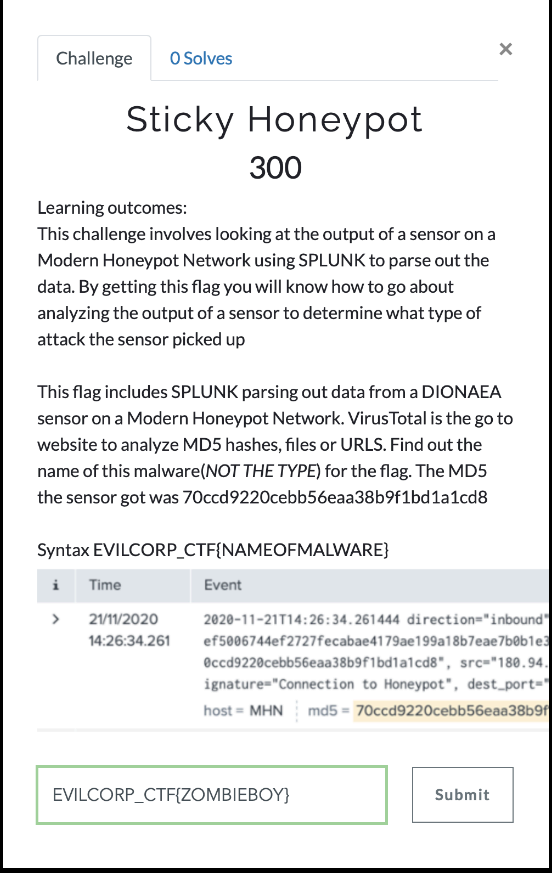
#IntezerAnalyze

3. Googling ZombieBoy malware shows that this malware is a Crypto-Mining malware.



New Crypto-Mining Malware ZombieBoy Exploits Multiple CVEs for Maximum Impact

3. The answer for the challenge is EVILCORP_CTF{ZOMBIEBOY}



Sticky Honeypot

300

Learning outcomes:
This challenge involves looking at the output of a sensor on a Modern Honeypot Network using SPLUNK to parse out the data. By getting this flag you will know how to go about analyzing the output of a sensor to determine what type of attack the sensor picked up

This flag includes SPLUNK parsing out data from a DIONAEA sensor on a Modern Honeypot Network. VirusTotal is the go to website to analyze MD5 hashes, files or URLS. Find out the name of this malware(*NOT THE TYPE*) for the flag. The MD5 the sensor got was 70ccd9220cebb56eaa38b9f1bd1a1cd8

Syntax EVILCORP_CTF{NAMEOFMALWARE}

i	Time	Event
>	21/11/2020 14:26:34.261	2020-11-21T14:26:34.261444 direction="inbound" ef5006744ef2727fecabae4179ae199a18b7eae7b0b1e3 0ccd9220cebb56eaa38b9f1bd1a1cd8", src="180.94. ignature="Connection to Honeypot", dest_port=" host = MHN md5 = 70ccd9220cebb56eaa38b9f

EVILCORP_CTF{ZOMBIEBOY}