3. It happened on Christmas day (2019-12-25)

3-1. 구성 환경

구성 환경

Internal webserver IP address: 10.12.25.101

External webserver IP address: 128.199.64.235

3-2. 문제 및 해답

문제 및 해답

Q. What the heck is going on here?

: IP 139.199.184.166의 probe/scan을 시도하는 웹 서버 트래픽들이 포함되어 있다.

tcp.port == 80 and http

	Time	Source	Destination	Protocol	Length	Info
2420	1122.453192	139.199.184.166	10.12.25.101	HTTP	237	GET /manager/html HTTP/1.1
2417	1122.185962	139.199.184.166	10.12.25.101	HTTP	245	GET /MySQLAdmin/index.php HTTP/1.1
2414	1121.917833	139.199.184.166	10.12.25.101	HTTP	241	GET /websql/index.php HTTP/1.1
2411	1121.648288	139.199.184.166	10.12.25.101	HTTP	238	GET /SQL/index.php HTTP/1.1
2408	1121.379921	139.199.184.166	10.12.25.101	HTTP	238	GET /sql/index.php HTTP/1.1
2405	1121.108763	139.199.184.166	10.12.25.101	HTTP	243	GET /sqladmin/index.php HTTP/1.1
2387	1113.535139	139.199.184.166	10.12.25.101	HTTP	251	GET /mysql/sqlmanager/index.php HTTP/1.1
2380	1109.788214	139.199.184.166	10.12.25.101	HTTP	248	GET /mysql/dbadmin/index.php HTTP/1.1
2377	1109.517815	139.199.184.166	10.12.25.101	HTTP	246	GET /mysql/admin/index.php HTTP/1.1
2374	1108.714118	139.199.184.166	10.12.25.101	HTTP	240	GET /phpmy/index.php HTTP/1.1
2371	1108.448265	139.199.184.166	10.12.25.101	HTTP	241	GET /phppma/index.php HTTP/1.1
2368	1103.530249	139.199.184.166	10.12.25.101	HTTP	241	GET /shopdb/index.php HTTP/1.1
2364	1102.318988	139.199.184.166	10.12.25.101	HTTP	242	GET /program/index.php HTTP/1.1
2361	1101.447841	139.199.184.166	10.12.25.101	HTTP	247	GET /__phpMyAdmin/index.php HTTP/1.1
2358	1100.658513	139.199.184.166	10.12.25.101	HTTP	248	GET /phpMyAdmin_ai/index.php HTTP/1.1
2355	1098.123600	139.199.184.166	10.12.25.101	HTTP	245	GET /phpMyAdmln/index.php HTTP/1.1
2352	1097.834846	139.199.184.166	10.12.25.101	HTTP	249	GET /WWW/phpMyAdmin/index.php HTTP/1.1

요약

1. 이것은 약점/취약성을 scan/probe 시도하고 있는 웹 사이트의 트래픽 예이다.
2. 관리자는 Digital Ocean 에 호스팅 된 것처럼 새로운 웹서버를 설정하였고, 트래픽을 감시 해보았다.
3. 트래픽 중에서 IP 139.119.184.166 의 많은 행동들이 보였고, 실제로 probe/scan 을 시도한 것을 확인