DTC Security – Threat Intel "Baseball Cards"

Typical Credential Stuffers

- Historically our credential stuffing attacks have shared some common characteristics

Regular 4AM Attacks

- Attacks begin almost daily at 4am

Endures Counter Measures

- Attacks from 9 different ASN's

The Cloud Attacker

- Targets Comet /tokens endpoint
- Uses well known cloud provider
- Uses single IP address at a time, with efforts lasting 8-12 hours per attack

Device serial number troll

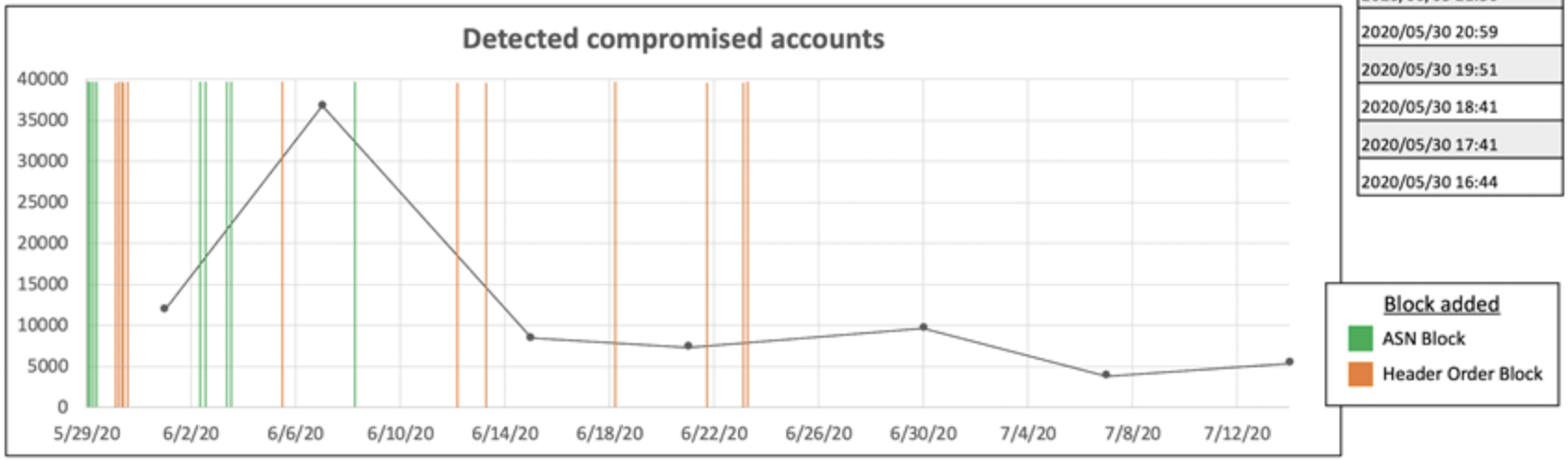
- Uses multiple Hurley Account IDs
- DSN "00000000-0000-4000-8000-000000000000"
- DSN "pepelaugh-oh-no-no-no"

DTC Security - WAF Blocks vs. Password Resets

AS Number block	ISP name	Date/time that block took effect
9009	M247	2020/06/03 11:14 ET
12989	Highwinds Network Group, Inc.	2020/06/03 14:27 ET
20473	Choopa, LLC	2020/06/02 11:56 ET
23470	ReliableSite.net	*(Before 2020/06/01 13:30 ET)*
46261	QuickPacket, LLC	*(Before 2020/06/01 13:30 ET)*
46844	ST-BGP	2020/06/08 17:50 ET
53755	Input Output Flood LLC	*(Before 2020/06/01 13:30 ET)*
55286	B2 Net Solutions	2020/06/02 16:00 ET
60781	LeaseWeb Netherlands / AMS-01	*(Before 2020/06/01 13:30 ET)*

Manual password reset date	Detected compromised accounts	Jira issue
2020/06/01	12,009	XS-14215
2020/06/07	36,827	XS-14258
2020/06/15	8,479	XS-14354
2020/06/21	7,386	XS-14486
2020/06/30	9,638	XS-14577
2020/07/07	3,827	XS-14725
2020/07/14	5,401	XS-14761

Header order block date/time
2020/06/23 10:07
2020/06/23 05:30
2020/06/21 17:36
2020/06/18 10:34
2020/06/13 15:38
2020/06/12 11:41
2020/06/05 21:36
2020/05/30 20:59
2020/05/30 19:51
2020/05/30 18:41
2020/05/30 17:41
2020/05/30 16:44



DTC Security Overview