NITE Team 4:

Unknown APT Group [IRIS] Intercept Analysis

CYBER INTEL

REIMAGINED

IRIS

The group responsible for the murder of Aconite Capital CFO Oran Plaskett as well as the suspected online harassment prior to his death will be known internally as **IRIS**. The messages Oran Plaskett received seemed to have been from a third party that Plaskett knew personally. The key was known by both parties and it appears that they were comfortable communicating in this covert manner. Our team was tasked with performing cryptanalysis on the messages received by Oran Plaskett.

Cryptanalysis

We used frequency analysis and n-grams to estimate the key length to be at 17 characters. For the entirety of the conversation, they did not change keys. Message intercepts between Plaskett and his friends/family during the exchanges with IRIS indicated that he was stressed. It's likely that the key is related to the material the group was using to harass the CFO. The message intercepts are currently being analyzed by several of our cryptanalysis algorithms and we have scheduled time on the supercomputer to attempt a brute force. If analysts can provide additional support, we would greatly appreciate it.

Possible Additional IRIS Networks

We recommend that the agency be on the lookout for any suspicious messages being relayed across social networks. The message exchanges were taking place over Facebook through a Game of Thrones fan page, users of the page were all bots (except for Plaskett and IRIS). We believe that the group's MO is to co-opt social networks and leverage their communication features for "hidden in plain view" messages. If automated bots are being used, possible ways to identify networks may be to search for common error messages (such as those dealing with reading/interpreting commands) and encrypted commands themselves (such as those to get current operations/targets and obtain info on those operations/targets).

Messages Between IRIS and Oran Plaskett (newest to oldest)

Last Text Message Received on Oran Plaskett's Phone

Contents:
3F0F1E03463B0C16060A07453E15000A42535F550E09031B4A452C0C080B54130D0
31D0B5B462F10491D0A1A430101541C0E18531D1D09115A4913004F11000211131
20953171A1314560D0D171B1A451D11111309071D5B

Facebook Message Exchange Between IRIS and Oran Plaskett

From: ThronesFan1337
3A1A550F15561D0B0A4F0F041A11520703014E1416091A06030C0A104523065C413
C1F0F060D03021D4845160C104E15011219010B1146130549100D0E17451A1C1B0F
0B004E0203141349110B0B06174E171D0F1801011948462F0611450702130B54160
40F1607030302561C1745090C174E001A044C1F0F0612460200090041433C0101521
6051F02550509191901170E17004E031B1504530F190A46190F440A1A11450801061
41E164E11030B17070016414326011A06000F074E1A131456070111180C17055410
0E18530F1B0246061B0B130607004E151E0D4C070610460F180F0B17020211071B1
C41151C1B550E07000C440A014311061152230012 0D1E4631171D070D02060B40

From: Oran Plaskett
2302100715134544010 00D7C1A54160E4C07061C1546020644080A4D45276D1E0D
4C070B190A460F0611450A15001C0D0609051D0959460C031A10451F0F000F07174
1081C006C12461A0C050E4F170D0707520802150155090856040 14B4F370D0B5430
0D0D1005553107020A0C080A0D451A1C00040D070B1B0302560401494F2A450615
1641021C4E160E091F0A01450D16114E001D41081C4E020E070249100D0A1A450F0
71904085D4E2C0913560105130A43110154070F08161C061207180D44110702114E
3D520F09050B074611170710000B431101541A0400034E010E031B4544071A17452
75414040D010B114600191B4408164309071217 4F4C3A7718461519 1B161C4F170D
0F00520E19014E16090B06080A1C4F0504071817054C0A010048

From: ThronesFan1337
240B550D08191E441C0016174E0717021E161A594613180501161C431C010152160
D1D1A550F12561D0B450806114E1B07154C0A010046111F0508451B06090254071
24C161810141F02010D0B0843040C1B07154C0A01001446040C08041B0A0A00071
A081C53191C120E561D0C004F21090F1719413B121A160E0B13074A