Analyzing the Democratic National Committee Hack Through the Lens of Routine Activities Theory

John McFarland

FEBRUARY 13, 2017

John McFarland

Professor Marie-Helen Maras

Cybercriminology

February 13, 2017

During the summer of 2015, and again during the spring of 2016 the Democratic National Committee's(DNC) internal systems were compromised by two Russian Intelligence Service(RIS) actors, referred to in the Joint Analysis Report(JAR) released by the Department of Homeland Security (DHS) as Advanced Persistent Threat(APT)29, and APT28.(Steppe, 2016, 2) These groups used targeted spearphishing attacks to gain access to primary cybervictims, where they then stole sensitive information that was later wielded against the Democratic Party in the 2016 presidential election.(ICA,2017,ii) Many political advisors speculate that the information leaked in this attack is a core reason Hillary Clinton lost the presidential election. Looking at this breach through the lens of Routine Activity Theory (RAT) we can determine the DNC's culpability, and how they can improve security going forward. RAT states that three things need to be true for a crime to occur. First, there needs to be exposure to a malicious offender. Second, there needs to be a suitable target, and finally, there needs to be a lack of suitable guardianship.

Malicious offenders exist everywhere on the internet but exposure to them can be limited through proper security protocols. With a target-rich environment like the United States Government(USG) a malicious offender has a wide variety of suitable victims to choose from, and by using Value, Inertia, Visibility, and Accessibility (VIVA) metrics (Maras, 2017, pg49) a

more specific target can be determined. Given the set of all USG targets publicly listed email addresses are the most visible. For a suitable victim to be exposed to a malicious offender we need to see a failure of established physical, and social guardianship. During the attack by APT29 this failure occurred when security officers, and anti-virus failed to prevent DNC members from activating links to malware that installed Remote Access Tools on targeted databases. From the JAR, we see that APT29 set up Operational Infrastructure (OI) to reduce offender exposure during the attacks (Steppe, 2016, 3). The OI served as the launcher, and receiver of information stolen during the breach. Once the OI was established "a spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple USG victims."(Steppe, 2016, 2-3) When DNC members activated these links, they gave the attackers access to important systems where they created encrypted channels to exfiltrate sensitive data.

Considering RAT, we see that all three requirements for a crime to occur were present. Because of the lack of vigilance shown by the security officers in charge of protecting the DNC infrastructure, and because of flaws in the anti-virus software used on the systems targets, the DNC exposed themselves to malicious RIS actors that stole sensitive information from them. This data breach may have been the source for many Wikileaks data dumps that occurred during the election, and combined with a Russian misinformation campaign detailed in the Intelligence Community Assessment(ICA) may have led to Hillary Clinton's loss in the 2016 presidential election. (ICA,2017, ii)

Works Cited

Grizzly Steppe. Russian Malicious Cyber Activity. NCCIC, Dec 29th 2016, pp. 1-13. www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

Intelligence Community Assessment(ICA). Assessing Russian Activities and Intentions in Recent US Elections. ICA 2017-01D, Jan 6th 2017, pp 1-25. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Maras, Marie-Helen. Cybercriminology. Oxford University Press. 2017