|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Compromise of email account** | | | |
| Email account of former senior advisor compromised. | Phishing | Specific details regarding access of Roger Stone's account unknown, probable that access was achieved using a form of spearphishing. Object given a confidence level. |  |
| DISARM: Compromise legitimate accounts | Roger Stone email account breached. |  |
| Compromise Accounts: Email Accounts |
| Valid Accounts |
| Spear phishing email sent to official in the Trump campaign from the compromised account of a former senior advisor. | Trusted Relationship | Link attached to email from Roger Stone account sent to Trump officials.  Microsoft reports Mint Sandstorm used a compromised account of a former senior advisor to send a spearphishing email to a high-ranking official in the Trump campaign. |  |
| DISARM: Co-Opt Trusted Individuals |
| Spearphishing Link |
| APT 42 controlled domain established. | Acquire Infrastructure: Domains | May not have occurred at this exact point, but domains would have been acquired at some stage for use in the spearphishing link sent from the Stone account. |  |
| Proxy: Domain Fronting | Spearphishing link would direct traffic through domain controlled by adversary before routing to website of the link.  No evidence that the spearphishing attempts through the Stone account were successful. |  |
| Involvement denied by Iranian representative. | DISARM: Deny Involvement | Reported that involvement was denied. |  |
| **Use of WhatsApp for phishing** | | | |
| Meta reports APT 42 using services such as WhatsApp to contact US officials and public figures associated with Trump and Biden | Establish Accounts: Social Media Accounts | Whatsapp accounts created posing as support agents for tech companies |  |
| Phishing: Spearphishing via Service | WhatsApp used for spearphishing.  No evidence of successful spearphishing, unlikely how Roger Stone account was compromised. |  |
| **Politico Leak** | | | |
| Politico receives emails from anonymous AOL account containing authentic documents from within the Trump campaign | Acquire Access | Access to documents would have been acquired. |  |
| DISARM: Obtain Authentic Documents | Authentic Documents on JD Vance, Trump's running mate, and Marco Rubio, a finalist for the VP role obtained. |  |
| DISARM: Create Anonymous Accounts | AOL email account. |  |
| DISARM: Email | Politico contacted by email. |  |
| DISARM: Traditional Media | Traditional media used to draw attention to the compromise of the campaign. |  |
| Sender refers to themselves as “Robert” | DISARM: Use Pseudonyms | Referring to themselves as 'Robert'. |  |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | DISARM: Determine Target Audiences | Business relationships, targets audiences and vulnerabilities were identified prior to beginning the operation, as this information was needed to know which members of the campaign to target. |  |
| DISARM: Identify Social and Technical Vulnerabilities |
| Gather Victim Org Information: Business Relationships |