**Review – Existing Modelled Operations**

**Description and motivation for the table**

An intermediate step between construction of the documentation document (containing the timeline, context and techniques) and the creation of the ‘.afb’ file has been created. This step involves a ‘justification table’ designed to link events within the incident’s timeline to specific techniques from MITRE ATT&CK and DISARM. The table consists of four columns; Event, Technique, Comments, and Verified. The table was designed for reviewing and verifying existing modelled operations (their ‘.afb’ files). The event column contains a brief description of the event, and the technique column contains the name of the associated technique. The comments column can be used for descriptions of how the event relates to the technique, potential improvements or issues with the current model, or any other notes. The verified column may contain ‘Yes’, ‘Maybe’ and ‘No’, reflecting whether the technique is valid and confirmed against its relevant event.

The table was created to review models previously created for the project, to ensure that the model is verified, and to provide further documentation for each cyber-enabled influence operation. However, after using the table to review existing models, the table has now been adapted into the model creation process. The new process for creating models can be outlined as follows:

1. Conduct research and gather information (keeping track of all resources in the ‘Resources’ document, and saving copies of all resources in the respective ‘Resources’ folder to save resources in their current state)
2. Complete the documentation file (including the summary, timeline, list of techniques)
3. Complete the justification table (add to the documentation file?)
4. Construct the attack flow diagram using the MITRE ATT&CK flow builder (save the .afb file)

The table will help to explain how an operation’s timeline is translated into an attack flow diagram, and explicitly outline the thought process in the diagram’s creation. It will enable more detailed justification and structure to be provided between the creation of the timeline and the attack flow diagram. The template is displayed below:

Template:

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Event heading** | | | |
| Event element |  |  |  |
| Event element |  |  |  |
| Event element |  |  |  |
| **Event heading** | | | |
| Event element |  |  |  |
| Event element |  |  |  |
| Event element |  |  |  |

**To complete:**

* GRU 2016 Industroyer Malware on Ukrainian Entities \*\* Currently has no files on CEIO github

**2018 UNC1151 campaign**

**Verification against provided timeline of events**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Credentials harvested (Refer to Figure 1)** | | | |
| Credentials harvested (to then compromise accounts for website Tv3.lt, Lithuanian tv website) | ATT&CK: Gather Victim Identity Information: Email Addresses | Would need to gather email addresses to login | Yes |
| ATT&CK: Gather Victim Organisation Information: Identify Roles | Logical step to take to login with accounts with privileges to change permissions and configuration | Yes |
| Phishing for Information: Spearphishing Service | Description refers to [noreplay@tv3.lt](mailto:noreplay@tv3.lt)  This seems to fits better with “Email with malicious document attached” section of timeline (see below in table).  Use of email to get information confirmed against resource (Mandiant report). Email delivered using SMTP2GO delivery service according to report. It is possible that they could have use [noreplay@tv3.lt](mailto:noreplay@tv3.lt) to phish employees of Tv3.lt, however timeline states that this email was used to send out the email with the article lure to politicians & media organisations.  **Suggestion**  Change the description to remove reference to [noreplay@tv3.lt](mailto:noreplay@tv3.lt) in the description and move to the action “ATT&CK: Phishing: Spearphishing Attachment”. As at this stage of the operation is where it is noted that email [noreplay@tv3.lt](mailto:noreplay@tv3.lt) is used. | Maybe |
| Search Open Websites/Domains: Social Media | Description talks about a lure document attached to an email, providing a link to a fabricated article. Not necessarily relevant to the technique provided “Search Open Websites/Domains: Social Media”  However it would make sense that to gather emails of politicians and public figures, social media would be used as there contacts could be found there.  **Suggestion**  Technique could also be justified as Search Open Websites/Domains: Search Engines T1593.002 instead  Edit the description to remove the lure document discussion, move to a later part of the diagram. | Maybe |
| **Credentials used to login & article inseminated** | | | |
| Credentials used to login to Content Management System |  | **Not present in model** |  |
| Permissions and system access configuration changed |  | **Not present in model** |  |
| Article published via defacing the website | DISARM: Post Content | Article posted on the website | Yes |
| DISARM: Blogging and Publishing Networks | Posted on the publishing network’s site | Yes |
| English version of narrative inseminated including Ghostwriter controlled blogs | DISARM: Develop New Narratives | Need to create the narrative to spread | Yes |
| DISARM: Edit Open-Source Content | Posting on collaborative blog or encyclopaedia, aligns with Ghostwriter controlled blogs | Yes |
| DISARM: Develop Inauthentic News Articles | Create the news article | Yes |
| DISARM: Create Inauthentic Websites | Referring to the controlled blogs | Yes |
| DISARM: Create Inauthentic News Sites | Using already existing news site. Not sure if blog qualifies as a news site.  **Suggestion:**  Remove action if not sure, or change confidence of action | Maybe |
| **Email with malicious document attached** | | | |
| Email with malicious document attached containing defamatory information regarding the Lithuanian Defence Minister and links to the article sent to target mailing list | ATT&CK: Phishing: Spearphishing Attachment | Document sent to Lithuanian Media with spear phishing attachment | Yes |
| DISARM: Email | Email containing the fabricated article | Yes |
| Email contained image, can be monitored by sender to see who has opened the email |  | **Not present in model** |  |
| Document attached with links to fabricated content | ATT&CK: Phishing: Spearphishing Attachment | Document attached. Fabricated content represented by relationship to DISARM aspects of model that represent the fabricated article. | Yes |
| Execution of document attempts to run malicious code that uses PowerShell commands to leverage Dynamic Data Exchange (DDE) to download a file. | ATT&CK: User Execution: Malicious File | Referring to the document being a malicious file | Yes |
| ATT&CK: Inter-Process Communication: Dynamic Data Exchange | Referring to the use of DDE | Yes |
| ATT&CK: Command and Scripting Interpreter: PowerShell | Referring to the use of PowerShell | Yes |
| delivered using SMTP2GO delivery service where senders IP can be masked |  | **Not present in model**  Is related to masquerading as [noreply@tv3.lt](mailto:noreply@tv3.lt), so is still somewhat present. Does not necessarily need to be added |  |
| Masqueraded as noreply@tv3.lt using noreplay@tv3.lt | Search Open Websites/Domains: Social Media | Mentioned in this technique, early in model  **Suggestion:**  Could add new action object to reflect masquerading as noreply@tv3.lt | No |
| After execution of DDE, string representing secondary powershell command downloaded | ATT&CK: Command and Scripting Interpreter: PowerShell | Download acknowledged in the description | Yes |
| Powershell command runs secondary file which sets persistence with a run key registry (creating and running VBS script) | ATT&CK: Command and Scripting Interpreter: PowerShell | Referring to the use of PowerShell. Secondary powershell command acknowledged in the description | Yes |
| ATT&CK: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | Representing the run key registry | Yes |
| VBS script a basic launcher for RADIOSTAR downloader | ATT&CK: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | Mentioned in description for this technique. | Yes |
| **Creation of the defamatory article** | | | |
| Creating the article, designed to damage public opinion of Lithuanian Defence Minister | DISARM: Degrade Adversary | All techniques align with the aim of damaging public opinion through the article. | Yes |
| DISARM: Divide |
| DISARM: Demographic Segmentation |
| DISARM: Psychographic Segmentation |
| DISARM: Identify Existing Prejudices |
| DISARM: Identify Wedge Issues |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | Would need to determine target audiences before writing the inauthentic articles | Yes |
| Determine Strategic Ends | Would need to identify strategic ends and goals | Yes |
| After | DISARM: Content | All are “Assess Effectiveness” techniques, makes sense to occur after operation concludes | Yes |
| DISARM: Message Reach |
| DISARM: Social Media Engagement |

Figure 1: Section of Attack Flow Diagram relevant to credential harvesting for reference

A screenshot of a computer screen

Description automatically generated

**Potential techniques to add:**

Event: Credentials used to login to Content Management System

* TA0043: Reconnaissance
  + T1586: Compromise Accounts

Event: Permissions and system access configuration changed

* TA003: Persistence
  + T1098: Account Manipulation (in description of technique: “modifying credentials or permission groups”)

Event: Email contained image, can be monitored by sender to see who has opened the email

Event: delivered using SMTP2GO delivery service where senders IP can be masked

**2019 UNC1151 campaign**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Compromise of news sites** | | | |
| kaunas.kasvyksta[.]lt and baltictimes[.]com compromised through backdoor | Develop Capabilities: Malware | Description contains “Publicly available software code was modified to create a backdoor for the operation.” | Yes |
| Develop Capabilities: Malware | Another attack flow object is labelled as “Develop Capabilities: Malware”, but has a different technique ID T1588.001. This refers to “Obtain Capabilities: Malware”.    **Suggestion:**  Fix the label, change to “Obtain Capabilities: Malware”. | No |
| ATT&CK: Exploit Public-Facing Application | Description refers to backdoor and compromise. | Yes |
| Backdoor left in kaunas.kasvyksta[.]lt and file upload to the system | Stage Capabilities: Upload Malware | Software code placed in news portal, file uploaded | Yes |
| Defamatory news articles posted on both sites & Backdoor in news portal used, content of article is replaced with defamatory information | ATT&CK: Defacement: External Defacement | Event fits the technique of external defacement. | Yes |
| DISARM: Develop Inauthentic News Articles | Before posting the defamatory article needed to be written. | Yes |
| DISARM: Blogging and Publishing Networks | The existing news sites were used to post the content. Howe | Yes |
| DISARM: Co-opt Trusted Sources | Co-opt trusted sources likely refers to the use of existing news websites to publish the defamatory information. | Yes |
| DISARM: Post Content | Content was posted on the site. | Yes |
| Fake SIS website hosted | DISARM: Create Inauthentic Websites | To use the fake SIS website it had to be created. | Yes |
| Article had a ‘Notify SIS’ hyperlink which redirects to same web portal | ATT&CK: Defacement: External Defacement | Hyperlink mentioned in description for “ATT&CK: Defacement: External Defacement”  **Suggestion:** Add new separate attack flow object to specify use of the ‘Notify SIS’ link | Yes |
| Hyperlink links to fake Special Investigation Service (SIS) of the Republic of Lithuania website | DISARM: Co-opt Trusted Sources | Co-opt trusted sources could refer to the fake SIS website  **Suggestion:** Specify in the description if the action refers to the news sites, SIS site, or both. | Maybe |
| ATT&CK: Defacement: External Defacement | Mentioned in description for “ATT&CK: Defacement: External Defacement” | Yes |
| Defamatory content repeated on fake SIS site | ATT&CK: Defacement: External Defacement | Mentioned in description for “ATT&CK: Defacement: External Defacement”  Would not be classified as defacement as the defamatory content was posted on an inauthentic site that the adversary themselves had created. Did not deface their own website.  **Suggestion:** Mention the content posted on the fake SIS site in the DISARM: Post content description | No |
| TOR network services used to conceal location and usage of the network | **Not present** | Not mentioned in the attack flow diagram.  **Suggestion:** Add a new attack flow action object to reflect the use of TOR network services | No |
| **Spoof emails** | | | |
| Spoof emails of Ministry of National Defence Officer distributed to state representatives | ATT&CK: Gather Victim Identity Information: Email Addresses | Email addresses would have been gathered to send emails, so this is accurate. | Yes |
| ATT&CK: Gather Victim Organisation Information: Identify Roles | Email sent to specific politicians and state representatives. | Yes |
| DISARM: Email | Email used to distribute content | Yes |
| Contains slanderous content about the Minister of National Defence | DISARM: Leverage Conspiracy Theory Narratives | Narratives were leveraged in the slanderous content or the fake article. | Yes |
| IP spoofed | **Not present** | Not in the attack flow  **Suggestion:** Include object from DISARM: Conceal Network Identity | No |
| Containing 1x1 pixel image to tell the sender who has viewed the email and how many times they read it | Phishing for Information: Spearphishing Link | Description refers to the 1x1 image: “A link, in the form of a 1x1 pixel invisible image, was inserted into the email. The purpose of the image is to inform the sender who has read the message and how many times they read it.” | Yes |
| ATT&CK: Phishing: Spearphishing Link | Refers to the pixel image | Yes |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | It would make logical sense for all of these initial phases to have occurred before the operation. | Yes |
| Determine Strategic Ends |
| DISARM: Identify Existing Prejudices |
| DISARM: Identify Existing Conspiracy Narratives/Suspicions |
| DISARM: Identify Wedge Issues |
| DISARM: Identify Target Audience Adversaries |
| DISARM: Degrade Adversary |
| DISARM: Political Segmentation |
| After | DISARM: Content Focused | All are “Assess Effectiveness” techniques, makes sense to occur after operation concludes | Yes |
| DISARM: Content |
| DISARM: Message Reach |
| DISARM: Social Media Engagement |

**Suggestions:**

Event: Email sent from Spoof Emails of Ministry of National Defence Officer

* TA005: Defense Evasion
  + T1656: Impersonation

Event: IP spoofed

* TA11: Persist in the information environment
  + T0129.001: Conceal Network Identity

**2017 APT French election campaign**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Registering web addresses (APT 28)** | | | |
| Registers decoy internet addresses | Create Inauthentic Websites | Technique matches creating internet addresses | Yes |
| Acquire Infrastructure: Domains | Technique matches creating domains | Yes |
| Addresses designed to mimic the name of the ‘En Marche!’ movement | Spoof/parody account/site | The sites that were created were designed to mimic legitimate sites and the ‘En Marche!’ movement. This can be represented by Spoof/parody account/site | Yes |
| Registers web addresses to mimic legitimate websites (including ‘myaccount.google.com-changepasswordmyaccount-idx8jxcn3ufdmncudd.gq’) |
| Creating fake login pages |
| **Social media account communicates with individuals** | | | |
| Social media account communicates with French individuals, offering access to campaign documents (GRU) | Establish Accounts: Email Accounts | Timeline states that a social media account communicated with individuals, but then a spearphising email was sent.  There may be missing information in the timeline regarding how these communications migrated from social media to email within the timeline and the attack flow diagram.  However, an email account would need to be created to send an email, so this would make sense.  **Suggestion:** Add a new attack flow object that represents creation of a social media account in addition to the email accounts. | Maybe |
| Spearphising emails linking to websites established by APT | Phishing for Information: Spearphishing Link | Matches with the description, spearphising link or attachment not necessarily specified in timeline.  Confirmed against resource ‘MIT Technology Review’ source that a link was sent. | Yes |
| Phishing: Spearphishing Attatchment | Could not identify spearphising using attachments within the timeline or resources.  **Suggestion:**  Use Phishing: Spearphishing Link instead | No |
| Compromise Accounts: Email Accounts | Compromised login credentials would include emails. | Yes |
| Email Collection: Remote Email Collection | Technique refers to collecting sensitive information remotely. This relates to the collection of emails using the ‘myaccount.google.com-changepasswordmyaccount-idx8jxcn3ufdmncudd.gq’ site. | Yes |
| Valid Accounts: Domain Accounts | The same technique is repeated three times with different tactic IDs to reflect the different stages; Initial Access, Persistence, and Defense Evasion. | Yes |
| **Leaks** | | | |
| Unidentified individuals began leaking documents purporting to be from the campaign’s email accounts | Create Inauthentic Social Media Pages and Groups | Consistent with individuals leaking documents, need to create accounts first. | Yes |
| Create Anonymous Accounts | Same as above, need to create accounts. | Yes |
| Obtain Authentic Documents | From timeline can be confirmed that authentic documents were obtained, which then could be leaked. | Yes |
| Used hashtag #MacronLeaks | Create Hashtags and Search Artifacts | Hashtags were used for leaking documents from the campaign on social media. The hashtags are associated significantly with the operation. | Yes |
| Create Dedicated Hashtag |
| Use Hashtags |
| Posted on document sharing website | DISARM: Post Content | All techniques are suitable for representing posting on the document sharing website. | Yes |
| Media Sharing Networks |
| DISARM: Blogging and Publishing Networks |
| Post Across Platform |
| False documents added to genuine documents and leaked | Develop False or Altered Documents | Techniques relate to creating false documents, adding to genuine documents and leaking these documents. | Yes |
| Alter Authentic Documents |
| Manipulate Platform Algorithm |
| Flooding the Information Space |
| Mainstream Social Networks |
| Exploit Data Voids |
| Play the Long Game |
| Narratives surrounded terrorist attacks, email account lockouts, software updates for voting machines, etc | DISARM: Leverage Conspiracy Theory Narratives | Techniques are relevant to generating false narratives and spreading them. | Yes |
| Integrate Target Audience Vulnerabilities into Narrative |
| Generate Information Pollution |
| Create Echo Chambers/Filter Bubbles |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Identify Susceptible Targets in Networks | These techniques are all part of the planning stages, and make sense regarding the timeline of events that follow | Yes |
| Determine Target Audiences |
| DISARM: Determine Strategic Ends |
| Degrade Adversary |
| Distort |
| Divide |
| Political Segmentation |
| Identify Media System Vulnerabilities |
| Discredit Credible Sources | The title of the attack flow object is incorrectly labelled as “Descredit Credible Sources”  **Suggestion:** Fix spelling error | No |
| ATT&CK: Gather Victim Identity Information: Employee Names | Would need to gather relevant victim information in advance. | Yes |
| ATT&CK: Gather Victim Identity Information: Email Addresses |
| ATT&CK: Gather Victim Organisation Information: Identify Roles |
| ATT&CK: Gather Victim Network Information: Domain Properties |
| After | Measure Performance: Content Focused | These techniques all relate to steps taken after an operation to measure effectiveness. It would make sense for these to have occurred. However, it cannot be certain that all of these techniques were employed by the threat actor.  Need to check the resources | Maybe |
| Measure Effectiveness: Behaviour Changes |
| Measure Effectiveness: Content |
| Measure Effectiveness: Awareness |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/Attitude |
| DISARM: Message Reach |
| DISARM: Social Media Engagement |

**2022 GRU DDoS on Ukrainian services campaign**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **DDoS attack** | | | |
| DDoS attack on Privatbank and Oschadbank | Obtain Capabilities: Tool | Obtaining the tools and services (such as CLDAP) needed for the attack would make sense. | Yes |
| Compromise Infrastructure: Botnet | Would be relevant as the botnet (network of compromised systems) would be used to perform the DDoS attack. | Yes |
| Gather Victim Network Information | In order to perform the attack, the victim network information would be needed. | Yes |
| Endpoint Denial of Service: Service Exhaustion Flood | Technique represents the DDoS attack itself, so is appropriate. | Yes |
| Conceal Infrastructure | Could not necessarily identify any evidence within the sources that stated that GRU concealed infrastructure, network identity, or denied involvement. It would make sense for them to have done so but could not find evidence.  Suggestion: Double check resources | Maybe |
| Conceal Network Identity |
| Deny Involvement |
| CLDAP searchRequest operation (carrying out reflection attacks) | Endpoint Denial of Service: Service Exhaustion Flood | CLDAP searchRequest operation is how the DDoS attack was carried out.  **Suggestion:**  Mention this in the description of “Endpoint Denial of Service: Service Exhaustion Flood” | Yes |
| Successfully rendered some services offline | Endpoint Denial of Service: Service Exhaustion Flood | Represented also by the “Endpoint Denial of Service” technique. | Yes |
| **Fake messages** | | | |
| PrivatBank customers received texts |  | **Not present** | No |
| Oschadbank customers were targeted via social media |  | **Not present**  Somewhat addressed by the presence of the technique “Measure Effectiveness Indicators (or KPIs): Social Media Engagement”, however missing other techniques to reflect this aspect of the operation.  **Suggestion:**  Use techniques such as “Post Content” or “Create Inauthentic Accounts” to reflect the targeting of customers through social media. | No |
| Messages claiming the bank doesn’t work to drive more traffic to the website, adding to DDoS incident |  | **Not present**  **Suggestion:**  Integrate techniques related to spreading manipulative information. | No |
| Increasing fear and uncertainty surrounding Ukrainian government’s ability to protect itself. | Demographic Segmentation | Techniques contribute to the aim of increasing fear and uncertainty. | Yes |
| Economic Segmentation |
| Respond to Breaking News Event or Active Crisis |
| Integrate Target Audience Vulnerabilities into Narrative |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | DISARM: Determine Target Audience | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| DISARM: Determine Strategic Ends |
| Identify Social and Technical Vulnerabilities |
| Degrade Adversary |
| Dismay |
| Divide |
| After | Measure Effectiveness: View Focused | These techniques are all part of the post-operation. However, there is not necessarily any evidence to suggest that GRU performed all of these aspects of measuring effectiveness.  **Suggestion:**  Ensure the techniques are backed by evidence. | Maybe |
| Measure Effectiveness: Behavior Changes |
| Measure Effectiveness: Awareness |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/Attitude |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

**2016 Attacks Against Ukraine Financial and Treasury Services**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Spearphising campaign** | | | |
| Spearphishing campaign using malicious malware-laced attachments targeted State Treasury Service’s system administrators. | Search Open Websites/Domains | In order to conduct spearphising, victim identity information needs to be gathered, and an email account needs to be created for use. “Spearphising Attachment” accurately reflects the event. | Yes |
| Gather Victim Identity Information: Email Addresses |
| Gather Victim Identity Information: Employee Names |
| Establish Accounts: Email Accounts |
| Spearphishing Attachment |
| Malicious Microsoft Excel file developed that required user to enable macros. Allowing macros to run resulted in the execution of the malware-laced file ‘explorer.exe’. | Obtain Capabilities: Malware | Would need to obtain malware and stage it to be able to deploy the malicious excel file.  However, it is unclear whether these two techniques are meant to represent the macros Excel file or the KillDisk malware  **Suggestion:**  Add to the description what malware is being referred to. | Yes |
| Stage Capabilities: Upload Malware |
| A system administrator for the State Treasury Service opens the Excel file and enables macros. This establishes an unauthorized, cover encrypted communication between the computer and a third-party service used by the adversaries | Encrypted Channel | An encrypted channel established so is an accurate representation. | Yes |
| A dedicated network connection between the State Treasury Service and Ukraine’s Ministry of Finance is exploited to obtain unauthorised access to the Ministry of Finance’s computer network. | Control Information Environment through Offensive Cyberspace Operations | This technique more generally refers to the entire operation, and how through shutting off the financing system would affect the information environment. However, this could also relate to gaining unauthorised access to the computer network  **Suggestion:**  Add techniques such as “Acquire Access” to reflect gaining access to the Ministry of Finance’s computer network. | Maybe |
| **Malware deployed** | | | |
| Destructive malware deployed against the Ministry of Finance and State Treasury Service. | Obtain Capabilities: Malware | Would need to obtain malware to deploy it. | Yes |
| Deployed an updated version of the KillDisk malware | Stage Capabilities: Upload Malware | Aligns with deploying the KillDisk malware | Yes |
| KillDisk options: (1) delete the infected computers' Windows event logs.  (2) Delete all the files that matched a list of file extensions hardcoded into the malware.  (3) Overwrite portions of the infected computers' hard drives, thus rendering the computers inoperable. | System Time Discovery | Techniques relate to the listed KillDisk options. | Yes |
| Data Destruction |
| System Shutdown/Reboot |
| Stored Data Manipulation |
| Native API |
| Clear Windows Event Logs |
| Indicator Removal: File Deletion |
|  | Internal Defacement | Not present within the timeline or context. May not be appropriate for the diagram.  Suggestion:  Review resources | No |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| Determine Strategic Ends |
| Identify Social and Technical Vulnerabilities |
| Degrade Adversary |
| Dismay |
| Divide |
| Respond to Breaking News Event or Active Crisis |
| After | Measure Effectiveness: Awareness | These attack flow objects are not connected to any other objects using arrows.  **Suggestion:**  Remove or connect them to the attack flow diagram. | Maybe |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |
| Deny involvement | Both techniques verified by ‘2020\_10\_19\_unsealed\_indictment\_0.pdf’ document | Yes |
| Break Association with Content |
| Misc | Conceal Infrastructure: Obfuscate Payment | Both techniques are present in the attack flow diagram but are not mentioned in the timeline or context. Also appears to not be present in the resources  Suggestion:  Check resources. | No |
| Conceal Infrastructure: Use Cryptocurrency |

**Al-Toufan 2022 Defacement of Bahraini and Israeli websites**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Attacks on websites** | | | |
| Bahraini and Israeli pro-government news websites were defaced  (The group replaced legitimate content on news and government websites with articles that criticized the regime) | Vulnerability Scanning | Would need to identify existing vulnerabilities to help gain access to websites. | Yes |
| External Defacement | Accurate as the news websites were defaced. | Yes |
| Note | Note labelled “Unauthorised access to Bahraini and Israeli websites is achieved” is present.  **Suggestion:**  This could be replaced with technique or added beside “Acquire Access” | Maybe |
| The Bahraini airport website returned 504 and 404 errors, rendering the services unavailable for at least half an hour | Network Denial of Service | Network DoS attack could have been used to render the Bahraini airport services unusable. | Maybe |
| DDoS attacks on the Bahrain News Agency website and the Bahrain Chamber of Commerce website | Endpoint Denial of Service | Reflects the use of DDoS attacks accurately. | Yes |
| Attacks used to fan protests among the politically underrepresented Shi'ite majority in Bahrain by calling attention to poverty and inflation in the region | Degrade Adversary | These techniques are relevant to planning, creating a narrative and calling to action. | Yes |
| Divide |
| Distort |
| Discredit Credible Sources |
| Segment Audiences: Political Segmentation |
| Call to action to attend |
| Respond to Breaking News Event or Active Crisis |
| Integrate Target Audience Vulnerabilities into Narrative |
| **Use of social media** | | | |
| Create content (for defacement / content to post) | Create Localised Content | Before posting content or defacing the website, content needs to be created. | Yes |
| Develop Inauthentic News Articles |
| Publicising and exaggerating the attacks on social media | Distort Facts: Reframe Context | These techniques relate to publicising the attacks through social media and exaggerating them. | Yes |
| Mainstream Social Networks |
| Photo Sharing |
| Posted propaganda videos | Video Sharing | Posting the propaganda videos involves video sharing, posting content, and in doing so amplifying the existing narrative (through propaganda). | Yes |
| Post Content |
| Amplify Existing Narrative |
| Sockpuppet accounts are used to amplify the exaggerated news | Create Anonymous Accounts | Accounts were created to amplify the exaggerated news. | Yes |
| Create Sockpuppet Accounts |
| Create personas |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| Determine Strategic Ends |
| Assess Degree/Type of Media Access |
| Identify Wedge Issues |
| After | Measure Performance: Content Focused | Same note with “2016 Attacks Against Ukraine Financial and Treasury Services”; all of these techniques are not connected to the main attack flow. | Maybe |
| Measure Effectiveness: Behaviour Changes |
| Measure Effectiveness: Content |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Message Reach |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

**GRU & IRA 2016 US Election Campaign**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Computer compromise** | | | |
| FBI contacts the DNC to caution the IT department of a compromised computer by Russian hackers |  | Not present  **Suggestion**: May not necessarily be needed within the attack flow diagram, probably don’t need to resolve this. | N/A |
| **Email hacking** | | | |
| Used a variety of means to hack the email accounts of volunteers and employees of the Clinton campaign | Compromise Accounts: Email Accounts | Technique aligns with hacking email accounts. | Yes |
| Used URL-shortening services in conjunction with leased VPN |  | Not present  The technique “Acquire Infrastructure: Virtual Private Server” is present, however a Virtual Private Server is different from a VPN.  **Suggestion:** Include technique “External Remote Services” from MITRE ATT&CK to represent the use of a VPN | No |
| Spearphishing campaigns conducted with an email account created in the name (with a one-letter deviation from the actual spelling) of a known member of the Clinton campaign | Establish Accounts: Email Accounts | Techniques align with the spearphising timeline. | Yes |
| Spoofing email address | Phishing: Spearphishing Link |
| Emails looked like security notification from Google, stating that another user had tried to access the account and instructing users to change their password by clicking an embedded link. |
| Used embedded links purporting to direct the recipient to a document titled "hillary-clinton-favorable-rating.xlsx" - in fact this redirected to a GRU-created website. | Acquire Infrastructure: Server | To host the GRU-created website, GRU would have acquired a server and domain. | Yes |
| Acquire Infrastructure: Domains |
| Research into the names of victims and their association with the Clinton campaign on various social media sites led to targeted spearphishing operations | Search Open Websites/Domains: Social Media | These techniques all relate to research conducted regarding the victims and their association to the Clinton campaign. | Yes |
| Search Open Websites/Domains: Search Engines |
| Search Victim-Owned Websites |
| Gather Victim Identity Information: Credentials |
| Gather Victim Identity Information: Email Addresses |
| Gather Victim Identity Information: Employee Names |
| Credentials of a DCCC employee stolen through phishing email | Valid Accounts | The valid DCCC employee account is later used to access the network. | Yes |
| **Computer Networks** | | | |
| Research conducted into the DCCC and DNC computer networks to identify technical specifications and vulnerabilities | Gather Victim Host Information | These techniques generally relate to the research conducted into the DCCC and DNC computer networks, devices, and research of open-source information | Yes |
| Infiltrate Existing Networks: Identify Susceptible Targets in Networks |
| Ran technical query for the DNC's internet protocol configurations to identify connected devices. | Identify Social and Technical Vulnerabilities: Identify Existing Fissures |
| Searched for open-source information about the DNC network, the Democratic Party, and Hillary Clinton. | Search Open Websites/Domains: Social Media |
| Ran technical query for the DCCC's internet protocol configurations to identify connected devices. | Gather Victim Network Information: Network Topology |
| **Use of malware** | | | |
| Stolen credentials of a DCCC employee used to access the DCCC network. | Compromise Legitimate Accounts | The legitimate DCCC account was compromised and used to access the network. | Yes |
| Installed and managed different types of malware to explore the DCCC network and steal data. | Obtain Capabilities: Tool | Malware was obtained and developed in order to install it. The proxy may have been used to access the DCCC network.  **Note:** Check resources regarding the use of the proxy | Maybe |
| Develop Capabilities: Malware |
| Proxy: External Proxy |
| X-Agent malware installed on computers, which allowed them to monitor individual employees' computer activity (e.g., keylogging), steal passwords, and maintain access to the DCCC network, transmit information between victim devices and a GRU-leased server. | Stage Capabilities: Upload Malware | The malware was uploaded and installed onto the computers. | Yes |
| Stage Capabilities: Upload Tool |
| Unsecured Credentials: Credentials In Files | The X-Agent malware allows for all 3 techniques to be used. | Yes |
| Input Capture: Keylogging |
| Screen Capture |
| Installed and managed different types of malware (as with the DCCC network) to explore the DNC network and steal documents. | Archive Collected Data | Through using the installed malware, the DNC network was also explored, and documents were stolen. This is represented by ‘Archive Collected Data’, ‘File and Directory Discovery’, ‘Exfiltration over C2 Channel’ and ‘Obtain Private Documents: Obtain Authentic Documents’ | Yes |
| File and Directory Discovery |
| Exfiltration Over C2 Channel |
| Obtain Private Documents: Obtain Authentic Documents |
| Hacked the DNC Microsoft Exchange Server and stole thousands of emails from the work accounts of DNC employees | Gather Victim Identity Information: Email Addresses | Email addresses were taken, so aligns with the technique. However, the position of this technique in the attack flow likely doesn’t correspond with the DNC hack. It may also be represented by techniques relevant to DCCC such as “Unsecured Credentials: Credentials In Files”  **Suggestion:** Potentially include in the description of the techniques what specific action is occurring in terms of the timeline, and if it is referring to the DNC or DCCC networks. | Maybe |
| **DCLeaks** | | | |
| Domain dcleaks.com registered through a service that anonymized the registrant | Acquire Infrastructure: Domains | Aligns with the technique. | Yes |
| DCLeaks Facebook page is created using a pre-existing fictitious social media account | Create Inauthentic Social Media Pages and Groups | Technique reflects creating the Facebook page, as this is a social media site. | Yes |
| Twitter account @dcleaks\_ was also created and operated from Russian military computer infrastructure | Establish Accounts: Social Media Accounts | Technique aligns with creating the Twitter account | Yes |
| Adversaries created the online persona Guccifer 2.0 and falsely claimed to be a lone Romanian hacker to undermine the allegations of Russian responsibility for the intrusion | Create Anonymous Accounts | Guccifer is the pseudonym used by adversaries. The account can be considered as anonymous as their real identity is not displayed. | Yes |
| Conceal People: Use Pseudonyms |
| The IRA supported the data leak with troll farms and thousands of social media accounts purported to be Americans supporting radical political groups | Create Inauthentic Accounts: Create Sockpuppet Accounts | These techniques all relate to creating social media accounts, flooding the information space, and posting spam content.  Some of the techniques such as “divide” and “degrade adversary” may be more generally applicable to the entire operation itself. However, for the purposes of demonstrating their relevance within this table, they have been associated with the IRA troll farms. | Yes |
| Create Inauthentic Accounts: Create Bot Accounts |
| Flooding the Information Space: Trolls Amplify and Manipulate |
| Flooding the Information Space: Utilize Spamoflauge |
| Post Content: Share Memes |
| Use Existing Echo Chambers/Filter Bubbles |
| Divide |
| Degrade Adversary |
| Facilitate State Propaganda |
| These accounts encouraged attendance and/or created events in support of the Trump campaign. | Co-Opt Grassroots Groups | Techniques relate to organising events and using existing movements. | Yes |
| Organize Events |
| Encourage Attendance at Events |
| Published post on a blog site created through WordPress titled "DNC's servers hacked by a lone hacker". | Develop Owned Media Assets | To post content it first needs to be developed. | Yes |
| Post Content | The post was published on the blog site. | Yes |
| Select Channels and Affordances: Blogging and Publishing Networks | The post was published on a blogging WordPress site, so the technique is accurate. | Yes |
| Select Channels and Affordances: Traditional Media | A blog site may not be considered traditional media, so this technique may not be appropriate  Suggestion: Remove or replace with ‘Select Channels and Affordances: Social Media’ to reflect the use of social media (the Twitter account and Facebook account) | No |
| Guccifer 2.0 used to release and share stolen documents | Drive Online Harms: Dox | In releasing the stolen documents, private information would have been released, effectively ‘doxing’. Releasing documents would also attract the attention of traditional media. | Yes |
| Attract Traditional Media |
| GRU purchased VPN used to log into Guccifer profiles including @Guccifer\_2 Twitter account. VPN account opened from the same server used to register malicious domains for the hacking of the DCCC and DNC networks | Acquire Infrastructure: Virtual Private Server | Acquiring the server is relevant, as it is stated that the VPN account was opened from the same server used to register malicious domains for hacking DCCC and DNC networks. However, a VPN is not a Virtual Private Server. Including a technique to reflect the use of VPNs would be beneficial.  **Suggestion:**  Include technique “External Remote Services” from MITRE ATT&CK to represent the use of a VPN | Maybe |
| Posting content | Develop New Narratives | These techniques relate to developing narratives to integrate into content, and posting it. | Yes |
| Post Content |
| Integrate Target Audience Vulnerabilities into Narrative |
| Create Localized Content |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| Determine Strategic Ends |
| Assess Degree/Type of Media Access |
| Identify Social and Technical Vulnerabilities: Identify Existing Conspiracy Narratives/Suspicions |
| Identify Social and Technical Vulnerabilities: Identify Wedge Issues |
| Identify Social and Technical Vulnerabilities: Identify Media System Vulnerabilities |
| Segment Audiences: Political Segmentation |
| Respond to Breaking News Event or Active Crisis |
| General | Conceal Operational Activity: Deny Involvement | The adversaries did not want to have their involvement known as they used anonymous accounts. | Yes |
| After | Measure Performance: People Focused | These techniques are all part of the post-operation. However, there is not necessarily any evidence to suggest that GRU or the IRA performed all of these aspects of measuring effectiveness.  **Suggestion:**  Ensure the techniques are backed by evidence.  \*Same note as 2022 GRU DDoS on Ukrainian services campaign | Maybe |
| Measure Effectiveness: Behaviour Changes |
| Measure Effectiveness: Content |
| Measure Effectiveness: Awareness |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Message Reach |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

**Not sure where the following techniques fit into the timeline:**

Data Obfuscation: Junk Data

Obfuscated Files or Information: Binary Padding

Indicator Removal: Clear Windows Event Logs

Indicator Removal: Clear Linux or Mac System Logs

Indicator Removal: File Deletion

Acquire Infrastructure: Botnet

Conceal Infrastructure: Use Cryptocurrency

**GRU 2015 BlackEnergy Ukrainian Electricity Grid Disruption**

**\*Also note there is an issue with grammar & spelling in the timeline + list of techniques, need to reupload document with fix.**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Spearphising campaign & BlackEnergy** | | | |
| Spearphising emails sent. They contained malicious attachments including malicious Excel and MS Word files. | Establish Accounts: Email Accounts | Would have established email accounts to send spearphising emails. | Yes |
| Gather Victim Identity Information: Email Addresses | These information gathering techniques would have been used to find emails and other relevant information needed to conduct the spearphising campaign | Yes |
| Gather Victim Identity Information: Employee Names |
| Gather Victim Network Information |
| Search Open Websites/Domains |
| Spearphishing Attachment | Spearphishing attachments were used, the Excel and MS Word files were attached. | Yes |
| Command and Scripting Interpreter: Visual Basic | Description from document: Threat actors installed a VBA script that dropped the primary BlackEnergy implant for executing some malware and the default file used to determine folder displays on Windows machines. | Yes |
| Employees that opened the files and enables macros executed the BlackEnergy malware installation. | Obtain Capabilities: Malware | Description from document: BlackEnergy 3 malware used. Malicious plugins and malware such as KillDisk later uploaded. | Yes |
| User Execution: Malicious File | When the employee opens the file, they cause execution. | Ues |
| BlackEnergy facilitates the installation of additional malware plugins and tools. | Stage Capabilities: Upload Malware | The BlackEnergy malware would have been uploaded to then install it. | Yes |
| Ingress Tool Transfer | Description from document: Threat actors pushed additional malicious tools onto the infected system via BlackEnergy. Used to steal user credentials, move laterally, and destroy data. | Yes |
| Input Capture: Keylogging | Description from document: Account credentials were gathered via a BlackEnergy keylogger plugin. |  |
| Network Sniffing | Threat actors used BlackEnergy plugins/modules to perform network sniffing. This was used to sniff and capture more credentials being sent over the network between the local LAN and the power grid's industrial controls systems. |  |
| Process injection | Description from document:  Threat actors loaded BlackEnergy 3 into svchost.exe, which then launched iexplore.exe for their command and control server. |  |
| **Use of malware** | | | |
| Credential harvesting and network discovery functions are conducted. From here, valid credentials with administrator privileges are secured. | Acquire Infrastructure: Virtual Private Server | Description from document:  Valid credentials are used to interact directly with the client application for the document management system server via a VPN.  **Note:** A VPN is not the same as a Virtual Private Server. This technique may not apply | Maybe |
| Valid Accounts | Valid credentials with admin privileges are secured. Valid accounts from different stages are present in the attack flow (Initial Access, Persistence, Privilege Escalation, and Defence Evasion).  Description from document: Threat actors used valid accounts to escalate privileges, move laterally, and establish persistence. | Yes |
| Additional KillDisk malware is delivered to the network. Lateral movement within the network leads to the compromise of telephone communications and data centre servers. | Modify Registry | Description from document: Before starting the malware required to communicate with their command and control servers, threat actors lowered internet security levels. | Yes |
| Indicator Removal: Clear Windows Event Logs | Techniques relate to lowering defences and movement within the network to find information to allow compromise of the servers and communications.  \*Need to check the resources to ensure all are relevant | Yes |
| Impair Defenses: Disable or Modify Tools |
| Indicator Removal: File Deletion |
| Network Sniffing |
| Process Injection |
| Network Share Discovery | Description from document: KillDisk will attempt to enumerate mapped network shares to later attempt to wipe all files on those shares. | Yes |
| Remote System Discovery | Description from document: Threat actors remotely discover systems over LAN connections. Operational technology systems were visible from the IT network as well, giving the actors the ability to discover operational assets. | Yes |
| Lateral Tool Transfer | Description from document: The threat actors moved their tools laterally within the corporate network and between the ICS and corporate network. | Yes |
| An outage is scheduled for the backup power services at related telephone communications server and data centre servers. |  | None present  Suggestion: May not be necessary to add a technique to reflect this. | No |
| **Use of remote access services** | | | |
| Threat actors use native remote access services in conjunction with valid credentials to trip the breakers at the three power distribution companies. This disrupts the power supply to approximately 225,000 customers. | External Remote Services | Used native remote access services. Description from document: Threat actors installed a modified Dropbear SSH client as the backdoor.  The technique is used twice, once to reflect installing the backdoor (Initial Access) and using the backdoor (Persistence) | Yes |
| System Binary Proxy Execution: Rundll32 | Backdoor could execute supplied DLL using rundll32.exe  (Source: <https://attack.mitre.org/techniques/T1218/011/>) | Yes |
| Web Protocols | Description from document: BlackEnergy enabled communication between compromised hosts and their CC servers via HTTP post requests. | Yes |
| Create Account: Domain Account | Description from document: Threat actors exploited position on network to create privileged domain accounts. These were used for further exploitation and lateral movement. | Yes |
| KillDisk malware erases selected files on target systems and corrupts the boot record, rendering systems inoperable. | System Shutdown/Reboot | Techniques align with rendering the systems inoperable. | Yes |
| Data Destruction |
| Inhibit System Recovery |
| Threat actors conduct a denial-of-service attack on the telephone call centre at one of the power distributors. Simultaneously, the scheduled outage for the backup power occurs. This denies opportunities for the customers to gain clarity on the situation. | Obtain Capabilites: Tool | Description from document: Automated IP-based call generators used to conduct a denial-of-service attack. | Yes |
| Upload Tool |
| Network Denial of Service | Description from document: Threat actors initiate DoS attack on telephone call centre to prevent customers from gaining clarity on the power outage. | Yes |
| Control Information Environment through Offensive Cyberspace Operations | In conducting the denial-of-service attack, customers are unable to gain information about the situation. | Yes |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| Determine Strategic Ends |
| Identify Social and Technical Vulnerabilities |
| Motivations: GRU looks to take advantage of the tense climate surrounding the Russo-Ukrainian War. Driving perceptions of asymmetric warfare exploits vulnerabilities in the target audience by creating fear and undermining confidence in government services and security. | Respond to Breaking News Event or Active Crisis | Techniques all reflect the motivations of GRU in regard to the Russo-Ukraine War | Yes |
| Dismay |
| Divide |
| Control Information Environment through Offensive Cyberspace Operations |
| After | Measure Performance: View Focused | Same note with “2016 Attacks Against Ukraine Financial and Treasury Services”, all of these techniques are not connected to the main attack flow. | Maybe |
| Measure Effectiveness: Awareness |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

**Following techniques do not have an obvious location in the timeline / are not mentioned:**

Conceal Infrastructure: Use Cryptocurrency

Conceal Infrastructure: Obfuscate Payment

Break Association with Content

Deny involvement

**GRU 2017 NotPetya Disruption to Ukrainian Entities**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Preparation of NotPetya Malware** | | | |
| The GRU disseminated the NotPetya malware using a popular Ukrainian accounting software called M.E.Doc that was used to facilitate the communication of tax information to the Ukrainian government. | Develop Capabilities: Malware | The NotPetya malware was developed, aligning with this technique. | Yes |
| The software was periodically updated through an update server. |  | Not present  **Suggestion:** May not be needed to add a technique to reflect this. | No |
| Attacks were facilitated by rerouting internet traffic from (1) computers attempting to update the M.E.Doc software via the Update Server to (2) a France-based server controlled by the GRU. This France-based server delivered the malware to the victim computers that connected to it. |  | Not present  **Suggestion:** Include techniques relevant to rerouting traffic and establishing a controlled server. For example, use ‘Acquire Infrastructure: Server’ | No |
| GRU hackers familiarise themselves with M.E.Doc software and the Ukrainian EDRPOU number (equivalent of a tax file number in the US). This includes querying the EDRPOU website and computer language sets specific to the Ukrainian alphabet. | Search Open Websites/Domains | Description from document: Querying the EDRPOU website and computer language sets specific to the Ukrainian alphabet. | Yes |
| GRU gains access to the software code for the M.E.Doc software prior to the NotPetya attacks. Allowing the hackers to test malicious functionality. | Obtain Capabilities: Vulnerabilities | Description from document: GRU gains access to the software code for the M.E.Doc software prior to the NotPetya attacks. | Yes |
| GRU gains access to EternalBlue | Obtain Capabilities: Tool | Description from document: GRU gains access to EternalBlue, a product of the National Security Agency (NSA), the United States’ signals and communications intelligence agency. This tool is crucial to exploit the Ukrainian M.E.Doc software. | Yes |
| The GRU publishes the first malicious update file to the update server. | Upload Malware | Uploading the NotPetya malware aligns with this technique. | Yes |
| **Deployment of NotPetya** | | | |
| NotPetya malware was delivered to computers that attempted to receive a malicious software update from the Update Server. | OS Credential Dumping: LSASS Memory | Description from document: NotPetya contains a modified version of Mimikatz to help gather credentials that are later used for lateral movement. | Yes |
| File and Directory Discovery | Description from document: NotPetya searches for files ending with dozens of different file extensions prior to encryption. | Yes |
| Security Software Discovery | Description from document: NotPetya determines if specific antivirus programs are running on an infected host machine. | Yes |
| Data Encrypted for Impact | Description from document: NotPetya encrypts user files and disk structures with 2048-bit RSA. | Yes |
| System Shutdown/Reboot | Description from document: NotPetya will reboot the system one hour after infection. | Yes |
| Once a victims computer downloaded the malicious update file and the GRU rerouted the network traffic, victim computers could remotely receive and execute GRU commands. | SMB/Windows Admin Shares | Description from document: NotPetya can use PsExec which interacts with administrator network (ADMIN$) share to execute commands on remote systems. | Yes |
| Local Accounts | NotPetya gained access to local accounts, allowing victim computers to receive GRU commands. | Yes |
| Scheduled Task | Description from document: NotPetya creates a task to reboot the system one hour after infection. | Yes |
| Clear Windows Event Logs | Description from document: NotPetya uses wevtutil to clear the Windows event logs. | Yes |
| Masquerading | Likely that masquerading was used to rename tasks or services to make them appear less malicious. However, this is not mentioned in the timeline.  **Suggestion:** Check resources | Maybe |
| The malware propagated itself and wiped data from victim computers. | Exploitation of Remote Services | Description from document: NotPetya can use two exploits in SMBv1 to spread itself to other remote systems on the network. | Yes |
| Windows Management Instrumentation | NotPetya can use wmic to help propagate itslef across a network.  **Suggestion:** Note that just because the malware has the capability to perform an action, it does not mean this 100% occurred within the operation. If not sure, a confidence label should be given to the attack flow object. | Maybe |
| Rundll32 | Description from document: NotPetya installs itself on remote systems. | Yes |
|  | Service Execution | Description from document: NotPetya can use PsExec to help propagate itself across a network. | Yes |
| The malware appeared to be ransomware. Perhaps in an attempt to appear as if some other group other than a nation state were the culprits of the attack. | Misattribute Activity | Through appearing as ransomware, GRU potentially attempted to make it seem as though another group was the culprit.   **Suggestion:** It is not 100% known that this was to hide GRU involvement. Confidence level should be added to the attack flow objects. | Maybe |
| Deny involvement |
| Seed Kernel of truth |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | Both techniques would have occurred before the operation began and make sense. | Yes |
| Determine Strategic Ends |
| Motivations: This style of highly visible cyberattack on Ukrainian services is part of the Kremlin's hybrid warfare approach to the ongoing Russo-Ukrainian conflict. This approach aims to foster fear-based narratives within Ukraine and display strength and aggression. It can also attract media to disseminate a narrative and/or draw attention away from other actions. | Integrate Target Audience Vulnerabilities into Narrative | These techniques all reflect the motivation of the GRU explained on the left. | Yes |
| Respond to Breaking News Event or Active Crisis |
| Degrade Adversary |
| Segment Audiences: Economic Segmentation |
| Segment Audiences: Political Segmentation |
| Segment Audiences: Geographic Segmentation |
| After | Measure Performance: Content Focused | Same note with “2016 Attacks Against Ukraine Financial and Treasury Services”, all of these techniques are not connected to the main attack flow. | Maybe |
| Measure Effectiveness: Awareness |
| Measure Performance: View Focused |
| Measure Effectiveness: Behaviour Changes |
| Measure Effectiveness: Content |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Message Reach |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

**GRU 2018 Winter Olympic Games Campaign**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Spearphishing component** | | | |
| Reconnaissance and spearphishing was conducted. Emails were sent to the IOC, the Olympics, and Olympic partners. Recipients included official timekeeping partners and their subsidiaries. | Establish Accounts: Email Accounts | To conduct spear phishing, email accounts imitating official domains were created. | Yes |
| Phishing for Information: Spearphishing Attachment | Attachments were used in the spearphishing emails. | Yes |
| Gather Victim Identity Information: Email Addresses | Aligns with reconnaissance being conducted on the Olympics, IOC and those associated. | Yes |
| Gather Victim Identity Information: Employee Names |
| Business Relationships |
| GRU scanned Korean-based network infrastructure for vulnerabilities. | Vulnerability Scanning | Both techniques reflect scanning for vulnerabilities. | Yes |
| Identify Social and Technical Vulnerabilities |
| Malicious email attachments were developed and attached to emails using the IOC’s domain ‘pyeongchang2018.com’ and imitating the IOC Commission Chairman and Vice-President. | Develop Capabilities: Malware | Malware was developed to be used in the spearphishing campaign. | Yes |
| Spoofed email addresses were used to imitate the official domain of South Korea’s National Counterterrorism Centre. | Phishing for Information: Spearphishing Attachment | Use of spoofing can be represented by the ‘Phishing for Information’ technique.  **Suggestion:** It may be useful to include in the attack flow object description that spoofing was used and include the email addresses. | Yes |
| Malware-laced Microsoft word files were sent using phishing emails ‘olympicgameinfo@gmail.com’ and ‘alert.safekorea@gmail.com’.  Files from the latter were used to download additional content from a GRU controlled domain, ‘templates-library.ml’. | Stage Capabilities: Upload Malware | Description from document:  - alert.safekorea@gmail[.]com used for malware-laced Microsoft Word files to download additional content from a GRU controlled domain templates-library[.]ml.  - Malware-laced documents that downloaded an image file, which used open-source steganography tool to establish an encrypted channel from the recipient's computer to the adversaries command-and-control server.  - Malicious mobile applications uploaded to application store. | Yes |
| Data Obfuscation: Steganography |
| Malicious email links were embedded in images to redirect users to GRU controlled websites that mimicked legitimate websites. | Spearphishing Attachment | Aligns with the technique, spearphising attachment as the images are attached to the email.  **Suggestion:** ‘Spearphishing Link’ may also be appropriate. | Yes |
| Malware-laced documents included in these emails (from spoof email addresses imitating Counterterrorism centre). Document downloads an image file that uses Invoke-PSImage, an open-source steganography tool, to establish an encrypted channel to the threat actor’s command-and-control server. | Data Obfuscation: Steganography | Not clear whether steganography was used, or just if the steganography tool was simply used to establish an encrypted channel.  **Suggestion:** Check the resources to see if steganography was used. | Maybe |
| Obtain Capabilites: Tool | Aligns with timeline description of using the steganography tool. | Yes |
| Malicious emails contained fake resume attachment that contained a user executed PowerShell script. | User Execution: Malicious File | The malicious emails contained a malicious file. | Yes |
| Spearphishing Attachment | This event is also relevant to ‘spearphishing attachment’ as the file is attached to a spearphishing email. | Yes |
| Blurred version of resume displayed, and the user is prompted to enable certain features to view the document. Once the user enables the features, the blurred image is removed, and a malicious PowerShell script runs and attempts to download the next stage of malware. | Powershell | Technique reflects the use of PowerShell scripts in downloading malware. | Yes |
| GRU registered domain/subdomain names and created URLs for their malicious activities. | Acquire Infrastructure: Domains | Techniques reflect acquiring domains. | Yes |
| The threat actors used an email service that allowed for mass simultaneous emailing. This allowed emails to appear to come from legitimate organisations’ domains i.e. IOC. |  | Through using the email service, the threat actors aim to appear more legitimate.  **Suggestion:** Include technique ‘Phishing - Spearphishing via Service’ to reflect the use of an email service. | No |
| **Use of malware (Olympic Destroyer)** | | | |
| Malware was deployed against computer systems used by the Olympic Games' information technology vendor and the PyeongChang Organizing Committee for the 2018 Olympic & Paralympic Winter Games. | Stage Capabilities: Upload Malware | To deploy the malware, it would have been uploaded. | Yes |
| Reported laptops unexpectedly rebooting with messages from BitLocker, a full-volume encryption feature, asking for a recovery key. | Inhibit System Recovery | Description from document: Olympic Destroyer uses the native windows utilities vssadmin, wbadnim, and bcdedit to delete and disable operating system recovery features such as the Windows backup catalog and Windows Automatic Repair. It forced shutdowns, and impeded rebooting and recovery by misconfiguring BitLocker. |  |
| Widespread deployment of the malware across multiple companies led to the compromise of thousands of devices used by the IT company and PyeongChang Organising Committee. | Remote System Discovery | Description from document: Olympic Destroyer uses WMI to enumerate all systems in the network. | Yes |
| System Network Configuration Discovery | Description from document: Olympic Destroyer uses API calls to enumerate the infected system's ARP table.  \*\*Need to research if this fits | Maybe |
| Network Share Discovery | Description from document: Olympic Destroyer will attempt to enumerate mapped network shares to later attempt to wipe all files on those shares. | Yes |
| Windows Management Instrumentation | Description from document: Olympic Destroyer uses WMI to help propagate itself across a network | Yes |
| Lateral Tool Transfer | Description from document: Olympic Destroyer attempts to copy itself to remote machines on the network. | Yes |
| SMB/Windows Admin Shares | Description from document: Olympic Destroyer uses PSExec to interact with the hidden, full control administrator account ADMIN$ network share to execute commands on remote systems. | Yes |
| The malware was designed to knock computers offline by deleting critical system files, which would render the machines useless. The result saw internal servers including the Olympic website, display monitors and public Wi-Fi to crash. | Data Destruction | Description from document: Olympic destroyer overwrites files locally and on remote shares. | Yes |
| Inhibit System Recovery | Description from document: Olympic Destroyer uses the native windows utilities vssadmin, wbadnim, and bcdedit to delete and disable operating system recovery features such as the Windows backup catalog and Windows Automatic Repair. It forced shutdowns, and impeded rebooting and recovery by misconfiguring BitLocker. | Yes |
| Service Execution | Description from document: Olympic Destroyer uses PsExec to help propagate itself across a network. | Yes |
| **Computer compromise** | | | |
| Credentials were stolen using an open-source credential harvesting tool. | Automated Collection | Description from document: PowerShell script credential harvesting tool used. | Yes |
| Credentials from Web Browsers | Credentials could have been taken from web browsers. | Maybe |
| A file containing credentials and plaintext passwords was sent to a compromised computer to assist in lateral movement via privilege escalation. | Local Data Staging | Description from document: Stolen credentials and other files were moved to the Domain Administration Account's computer storage prior to exfiltration. | Yes |
| A malicious PowerShell script was executed containing versions of a credential harvesting tool designed to gather user, IP address, and server data. | PowerShell | Technique reflects use of the PowerShell script | Yes |
| Stolen credentials were used to access a domain administration account. | Domain Accounts | Domain account accessed using stolen credentials. | Yes |
| PowerShell scripts were used to dump credentials from more than 16,000 computers and servers belonging to company 1. | Credential Dumping: LSASS Memory | Technique aligns with credential dumping. | Yes |
| Unauthorised file access was likely used to help understand the company’s computer network architecture and configuration and move laterally across the computer network. | Ingress Tool Transfer | \*\* Need to check | Maybe |
| **Further compromise** | | | |
| The adversaries used a compromised account to deploy the Olympic Destroyer malware on the computer network of company 1. | Stage Capabilities: Upload Malware | To deploy the malware, it would have been uploaded. | Yes |
| The account was also used to deploy and execute the wiper component of the Olympic Destroyer malware within the compromised domain of the company. | Inhibit System Recovery | Description from document: Olympic Destroyer uses the native windows utilities vssadmin, wbadnim, and bcdedit to delete and disable operating system recovery features such as the Windows backup catalog and Windows Automatic Repair. It forced shutdowns, and impeded rebooting and recovery by misconfiguring BitLocker. | Yes |
| A connection between company 2’s computer network and the PyeongChang Organising Committee’s computer network was used to compromise key computers within the Committee’s network and deploy the malware on those computers. | Lateral Tool Transfer | Description from document: Olympic Destroyer attempts to copy itself to remote machines on the network. | Yes |
| The adversaries attempted to hide their activities and avoid being identified by:  o Obfuscating the true source of the malware – emulating malware used by the Lazarus Group in North Korea.  o Obscuring certain features of the malware – hindering any post-attack investigation and avoiding antivirus software.  o Established command-and-control implant on only one computer to create a single point of access between company 1 and the GRU controlled server. This reduced the chances of detection, while still allowing the adversaries to issue commands, install additional tools, and transfer data. | Break Association with Content | Techniques all relate to concealing activity.  However, clearing windows event logs is not mentioned in the timeline.  **Suggestion:** Check resources to ensure this specific technique occurred. | Yes |
| Misattribute Activity |
| Indicator Removal: Clear Windows Event Logs |
| Conceal Infrastructure |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| Determine Strategic Ends |
| Degrade Adversary |
| Assess Degree/Type of Media Access |
| After: After the attacks, the adversaries logged into a Moscow-based server to locate news about the attacks and track the attacks' impacts. | Measure Performance: View Focused | Same note with “2016 Attacks Against Ukraine Financial and Treasury Services”, all of these techniques are not connected to the main attack flow. | Maybe |
| Measure Effectiveness: Behaviour Changes |
| Measure Effectiveness: Awareness |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

**GRU 2019 Various Georgian Entities Defaced**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Cyberattack conducted against entities in Georgia** | | | |
| This attack targeted websites belonging to Georgian government, non-government, and private sector entities and involved the defacement of approximately 15,000 websites and the disruption of service to some of these websites | Active Scanning | Reconnaissance scans would have been conducted to identify target websites. | Yes |
| Gather Victim Org Information: Business Relationships | Description from document: Information about an entities business relationship may include a variety of details, including second or third-party organizations/domains (ex: managed service providers, contractors, etc.). This includes the Georgian web hosting provider ProService. | Yes |
| Search Victim-Owned Websites | Description from document: Victim-owned websites may contain a variety of actionable information including business operations and relationships. | Yes |
| Endpoint Denial of Service | Reflects the disruption of service to the websites. | Yes |
| Co-opt Trusted Sources | Trusted websites were co-opted and defaced. | Yes |
| External Defacement | Websites were defaced. | Yes |
| Attract Traditional Media | The defacement of the websites would have attracted media.   Suggestion: Add a confidence level to the attack flow object. | Maybe |
| Occurred after computer systems of a Georgian web hosting provider were compromised. | Compromise Infrastructure: Server | The systems of the hosting provider being compromised relates to the technique. | Yes |
| In many cases, the Conspirators replaced website home pages with an image of a former Georgian president, who was known for his efforts to counter Russian influence in Georgia, along with the caption "I'll be back." | Integrate Target Audience Vulnerabilities into Narrative | Techniques are relevant to creating content for defacement, to push a certain narrative. | Yes |
| Leverage Existing Narratives |
| Develop Competing Narratives |
| Create Localised Content |
| Create Localised Content |
| External Defacement |
| Following those attacks, local hosting provider ProService reported that 15,000 websites were disabled after their servers were attacked by hackers. | Compromise Infrastructure: Server | Description from document: ProService servers were attacked. | Yes |
| **Russia’s long-running campaign of hostile and destabilising activity against Georgia.** | | | |
| The Kremlin unleashed a multi-channel counter-messaging campaign after it had been made clear Russia’s GRU was behind the attack. | Recruit Partisans | Techniques relate to denying involvement and conducting a campaign through social media to adjust narrative. | Yes |
| Amplify Existing Narrative |
| The Russian Ministry of Foreign Affairs was first to dismiss the attribution, which was later amplified by Russian diplomatic social media accounts and then large Kremlin-funded outlets. Amplification of anti-Western narratives continued with Russian fringe media outlets and pro-Kremlin Georgian media outlets. | Develop Owned Media Assets |
| Demand insurmountable proof |
| Continue to Amplify |
| Break Association with Content |
| Deny involvement |
| Irakli Chikhladze, head of news at TV station Imedi, posted on Facebook that there was no signal, and the station was unable to broadcast. | Block Content | TV stations were blocked, destroying their information generation capabilities temporarily. | Yes |
| Both Imedi and another network, Maestro, were affected, he said. Imedi TV was paralysed for under an hour while Maestro's computers and other equipment were reportedly damaged or destroyed. | Destroy Information Generation Capabilities |  |  |
| Another network, Maestro, reported that some computers and other equipment were damaged or destroyed. |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Target Audiences | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| Determine Strategic Ends |
| Respond to Breaking News Event or Active Crisis |
| Facilitate State Propaganda |
| Dismiss: Discredit Credible Sources |
| Segment Audiences: Geographic Segmentation |
| Segment Audiences: Political Segmentation |
| Assess Degree/Type of Media Access |
| Identify Social and Technical Vulnerabilities: Identify Media System Vulnerabilities |
| After | Measure Performance: Content Focused | Same note with “2016 Attacks Against Ukraine Financial and Treasury Services”, all these techniques are not connected to the main attack flow. | Maybe |
| Measure Effectiveness: Behaviour Changes |
| Measure Effectiveness: Content |
| Measure Effectiveness: Awareness |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Message Reach |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

**IRA 2016 FaceMusic Malware**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **FaceMusic website and advertisements** | | | |
| FaceMusic website registered in April 2016. | Acquire Infrastructure: Domains | Website was acquired for FaceMusic, so fits these techniques. | Yes |
| Acquire Infrastructure: Server |
| Create Inauthentic Websites |
| FaceMusic was promoted through Facebook ads on or about May 2016. Promotions ran through one of the IRA’s fraudulent profiles “Stop All Invaders” | Deliver Ads: Social Media | Ads were delivered using Social Media including Facebook and Reddit. | Yes |
| These ads garnered approximately 25,000 impressions from 107 ads. However, this only produced 85 clicks. | Map Target Audience Information Environment: Evaluate Media Surveys | The threat actors would have access to data about their ad’s performance, and would have conducted research prior.   **Suggestion:** However, it is not stated if the IRA used Media Surveys. This needs to be checked against the resources. | Yes |
| The most successful ad, with 28 clicks, utilised the targeted ad system within Facebook to promote to U.S. teenage female users between the ages of 14 and 17. | Map Target Audience Information Environment: Conduct Web Traffic Analysis |
| Infiltrate Existing Networks: Identify Susceptible Targets in Networks | Susceptible targets were identified and subsequently targeted using the ad system. | Yes |
| FaceMusic was also advertised through Reddit on the subreddit r/UsefulWebsites. | Establish Accounts: Social Media Accounts | Social media accounts were created for both Facebook and Reddit. | Yes |
| Use Search Engine Optimization | It is possible that the threat actors may have used search engine optimisation to make their advertisements for FaceMusic more likely to appear to users.  **Suggestion:** Add a confidence level unless this is explicitly stated in the resources. | Maybe |
| **Malware infection** | | | |
| More than 13,000 machines were likely infected by the malware. | Develop Capabilities: Malware | The FaceMusic malware was developed and uploaded to the FaceMusic app. | Yes |
| Stage Capabilities: Upload Malware |
| Drive-by Compromise | Description from document: User visits the chrome plug-in website for FaceMusic and installs the malware. | Yes |
| Browser Extensions |
| Compromise Infrastructure: Botnet | Description from document: Victim’s machines are pulled into botnet as a consequence of the malware. | Yes |
| Scheduled Task/Job | Description from document: FaceMusic is programmed to communicate with a control server every minute as long as the victim’s browser is open. The server tells the app to connect to a web address from the victim’s machine. | Yes |
| The malware was used to enhance the visibility of troll farm content used by IRA accounts. Thus, expanding the reach of the content. | Recruit Malign Actors: Enlist Troll Accounts | These techniques are all relevant to the use of troll farms and troll farm content. The botnet was used to expand the reach of the content. | Yes |
| Build Network: Create Community of Sub-group |
| Create Inauthentic Social Media Pages and Groups |
| Acquire/Recruit Network: Acquire Botnets |
| Flooding the Information Space: Bots Amplify via Automated Forwarding and Reposting |
| Manipulate Platform Algorithm |
| Continue to Amplify |
| On or about June 2016, one FaceMusic user posted to Imgur claiming that FaceMusic had spammed their friends with a message that contained a direct download link. | Compromise Accounts: Social Media Accounts | Description from document: Compromised social media accounts were claimed to have been used to spam direct download links to friends of the accounts in an attempt to spread FaceMusic to other machines. | Yes |
| Google removed the app from the Chrome Store and the FaceMusic website is no longer available. |  | Not present  **Suggestion:** No technique needed, this element of the timeline just reflects the action taken by Google. |  |
| **Key tactics, systems & technology** | | | |
| Microtargeting. The IRA harvests large amounts of user data from various social media platforms. This is analysed and provides the IRA with clear segmented populations and microtargeted audiences to target with tailored messaging. | Search Open Websites/Domains: Social Media | To harvest data, social media platforms were searched. | Yes |
| Leverage Existing Narratives | Tailored messaging is used to leverage certain narratives for specific audiences. | Yes |
| Determine Target Audiences | Target Audiences would be determined based on the data. **Suggestion:** Technique is repeated twice along the same path which is not necessary. | Maybe |
| Integrate Target Audience Vulnerabilities into Narrative | Tailored message integrates specific target audience vulnerabilities. | Yes |
| Map Target Audience Information Environment: Monitor Social Media Analytics | It is likely that analytics and trending hashtags would have been researched. | Yes |
| Map Target Audience Information Environment: Identify Trending Topics/Hashtags |
| Identify Social and Technical Vulnerabilities: Find Echo Chambers | It is likely that as part of their microtargeting, the IRA would have used these techniques. | Yes |
| Identify Social and Technical Vulnerabilities: Identify Existing Prejudices |
| Identify Social and Technical Vulnerabilities: Identify Existing Fissures |
| Identify Social and Technical Vulnerabilities: Identify Existing Conspiracy Narratives/Suspicions |
| Identify Social and Technical Vulnerabilities: Identify Wedge Issues |
| Identify Social and Technical Vulnerabilities: Identify Target Audience Adversaries |
| Identify Social and Technical Vulnerabilities: Identify Media System Vulnerabilities |
| Sock Puppet accounts. The IRA frequently uses sock puppet and other false/counterfeit sites to grow and target large audiences. These create or infiltrate existing social media groups, actively engaging and targeting members the IRA wishes to cultivate as assets. These assets sometimes go on to post and organise rallies and demonstrations. | Encourage Attendance at Events | The accounts were used to encourage attending rallies. | Yes |
| Create Inauthentic Accounts: Create Bot Accounts | To use the sock puppet and bot accounts they needed to be created. | Yes |
| Create Inauthentic Accounts: Create Sockpuppet Accounts |
| Acquire/Recruit Network: Fund Proxies | Using sock puppet accounts fits within the broader description of using proxies. | Yes |
| Post Content: Share Memes | The groups would share posts such as memes. | Yes |
| Attract Traditional Media | It is possible that the IRA aimed to attract traditional media to further expand their reach. | Maybe |
| Flooding the Information Space: Trolls Amplify and Manipulate | Having a large amount of sock puppet and bot accounts would enable flooding the information space. | Yes |
| Flooding the Information Space: Utilize Spamoflauge |
| Respond to Breaking News Event or Active Crisis | The content posted was relevant to current events. | Yes |
| Organize Events | Some accounts would be used to organise rallies. | Yes |
| Cultivate Ignorant Agents | In using these accounts they aimed to attract large audiences. | Yes |
| Generate Information Pollution | These techniques all relate to developing content and sharing it. It is likely that the IRA would have used many of these techniques through their sock puppet accounts. | Yes |
| Distort Facts: Reframe Context |
| Reuse Existing Content: Use Copypasta |
| Reuse Existing Content: Plagiarize Content |
| Develop Text-based Content: Develop False or Altered Documents |
| Develop Text-based Content: Develop Inauthentic News Articles |
| Develop Image-based Content: Develop Memes |
| Develop Video-based Content |
| Obtain Private Documents: Obtain Authentic Documents |
| Leverage Content Farms: Create Content Farms |
| Virtual Private Networks are often used to hide identity and location | Conceal People: Conceal Network Identity | This technique reflects the use of a VPN | Yes |
| Acquire Infrastructure: Virtual Private Server | Description from document: IRAs use of VPN’s to hide identity and location is well known  **Suggestion:** A virtual private server is different to a virtual private network. It is inaccurate to represent a VPN by this technique. | No |
| Cryptocurrency allows the IRA to establish and operate location relevant email accounts, PayPal accounts, purpose political advertising, and operate false social media accounts for long periods without detection. | Conceal Operational Activity | Both techniques align with concealing activity through use of cryptocurrency. | Yes |
| Conceal Infrastructure: Use Cryptocurrency |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | Determine Strategic Ends | These techniques are all part of the planning / initial stages and make sense regarding the timeline of events that follow. | Yes |
| Segment Audiences: Geographic Segmentation |
| Segment Audiences: Demographic Segmentation |
| Segment Audiences: Economic Segmentation |
| Segment Audiences: Psychographic Segmentation |
| Segment Audiences: Political Segmentation |
| Dismiss: Discredit Credible Sources |
| Divide |
| Distract |
| After | Measure Performance: People Focused | Same note with “2016 Attacks Against Ukraine Financial and Treasury Services”, all these techniques are not connected to the main attack flow. | Maybe |
| Measure Performance: Content Focused |
| Measure Performance: View Focused |
| Measure Effectiveness: Behaviour Changes |
| Measure Effectiveness: Awareness |
| Measure Effectiveness: Knowledge |
| Measure Effectiveness: Action/attitude |
| Measure Effectiveness Indicators (or KPIs): Message Reach |
| Measure Effectiveness Indicators (or KPIs): Social Media Engagement |

These techniques are not connected to the attack flow:

A screenshot of a computer

Description automatically generated