|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security + Icons | **Attacker path** | Potent Potables | **Victim** | Type of attack |
|  | The attacker obtains confidential information he wants to exploit | C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0233018.wmf | CEO and the board of directors and members | Choose an item. |
| C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0285750.wmf | Attacker posts a link to a fake Anti Spyware Site and puts it on various Social Media Locations to deceive users | C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0300520.gif | A broad group of people is affected | Choose an item. |
|  | Attacker is obtaining your credit card information |  | The Victim is being targeted through the telephone | Choose an item. |
|  | Attacker sends a mass email with information for products to groups that have already opted out of receiving these advertisements | C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0149481.wmf | A broad group of people is affected | Choose an item. |
| C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0286034.wmf | Attacker redirects name resolution entries from legitimate site to fraudulent site | C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0195384.wmf | Fraudulent SiteC:\Program Files (x86)\Microsoft Office\MEDIA\OFFICE14\Bullets\BD21301_.gif  Legitimate Site  X | Choose an item. |
|  |  |  |  |  |