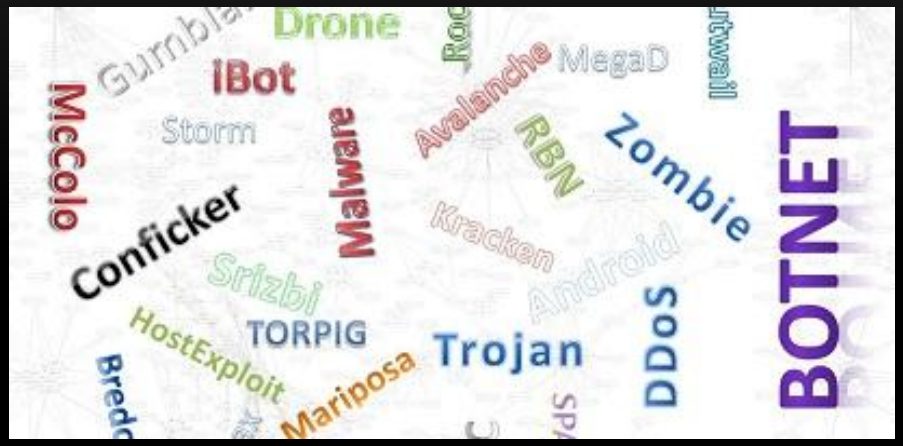
Ameaças Cibernéticas uma visão holística

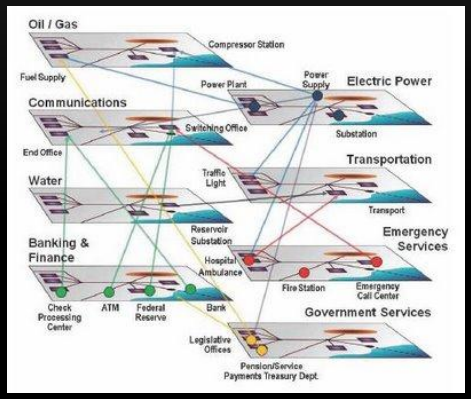
Otávio Cunha

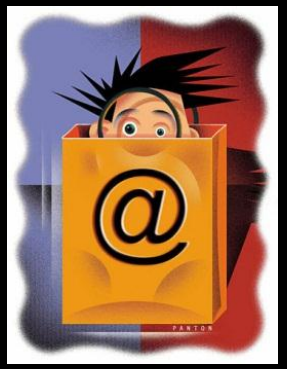
Agenda

- Introdução
- Desenvolvimento
- Debates

Introdução


Drone
iBot
Storm
McColo
Conficker
Malwara
Avalanche
RBN
Zombie
Kracken
Srizbi
TORPIG
HostExploit
Mariposa
Trojan
DDoS
BOTNET


Oil / Gas
Compressor Station
Fuel Supply
Power Plant
Power Supply
Electric Power
Communications
Switching Office
Substation
End Office
Transportation
Water
Traffic Light
Transport
Reservoir
Substation
Emergency Services
Banking & Finance
Hospital Ambulance
Fire Station
Emergency Call Center
Check Processing Center
ATM
Federal Reserve
Bank
Government Services
Legislative Offices
Pension/Service Payments Treasury Dept.


@

Conceito

- Espaço Cibernético
  - A palavra espaço cibernético foi cunhada por Willliam Gibson na ficção NEUROMANCER, no ano de 1984.
  - Ele é usado como um meio que denota o local aparente ou virtual, dentro do qual se realizam atividades eletrônicas. Espaço cibernético, portanto, é um local onde pessoas encontram-se não fisicamente mas virtualmente e se comunicam eletronicamente.

Conceito

- No contexto das ameaças cibernéticas pode-se elencar quatro domínios de atividade hostil e comportamento:
  - ataques cibernéticos patrocinados pelo Estado,
  - extremismo ideológico e político,
  - a criminalidade organizada e
  - crime de nível/individual.
- Estes domínios são interligados.

Efeitos de um ataque cibernético

- Diretos
  - Os sistemas computacionais controlando os elementos da infraestrutura crítica da nação, por exemplo, a grade de energia elétrica, o sistema de controle de tráfego aéreo, a infraestrutura de transporte, o sistema financeiro, purificação e distribuição de água ou telecomunicações.
- Indiretos
  - Os efeitos indiretos — são, muitas vezes, o objetivo principal de um ataque cibernético — geralmente não são reversíveis, por exemplo: um ataque cibernético pode interromper um computador que controla um gerador.

Ações patrocinadas por estados-nação

- Atribuição
  - é o esforço para identificar o responsável por um ataque cibernético.
  - Técnica de atribuição é a capacidade de associar um ataque a um responsável através de meios técnicos, com base nas informações disponibilizadas pelo fato do ataque cibernético em si — isto é, atribuição técnica baseia-se em pistas disponíveis em cena (ou cenas) do ataque.
  - As duas questões-chave na atribuição técnica são precisão e exatidão.

Ações patrocinadas por estados-nação

- A triste realidade é que a **técnica de atribuição** de um ataque cibernético é difícil de ser realizada: **"bits não vestem uniformes"** e pode ser quase impossível de ser efetivada quando um usuário inconscientemente comprometido ou inocente está envolvido.

Ações patrocinadas por estados-nação

- Intenção
  - Atribuição de um ataque cibernético ajuda, mas se a parte identificada como sendo responsável não é um governo nacional ou outra parte com intenções declaradas na direção do Governo, será praticamente impossível determinar a intenção com alta confiabilidade.
  - Determinações de intenções e atribuição da fonte são muitas vezes complicadas, e inadequadamente tendenciosas, por falta de informação.

Quando um ataque cibernético é considerado um ato de guerra?

- O conflito cibernético é um problema estratégico novo e complicado.
- Não há um quadro de política adequada para gerenciar conflitos no espaço cibernético nem um léxico satisfatório para descrevê-lo.
- Incerteza é o aspecto mais proeminente do conflito cibernético – na atribuição da identidade de atacantes, o âmbito dos danos colaterais e o efeito potencial sobre o destino pretendido de ataques cibernéticos.
- O conflito no espaço cibernético combina o crime, a espionagem e a ação militar de maneiras que muitas vezes tornam estes elementos indistinguíveis.
- A utilização de criminosos cibernéticos por Estados tornou-se um elemento de conflito cibernético, alguns países usam criminosos como agentes ou mercenários contra outros Estados.

Exploração cibernética

- A missão da **exploração cibernética** é **diferente** da missão do ataque cibernético nos seus objetivos e as idéias legais que os envolvem.
- No entanto, muito da tecnologia da oculta exploração cibernética é **semelhante** à do ataque cibernético, e o mesmo é verdadeiro para algumas das considerações operacionais.

Pontos para reflexão

- A segurança cibernética constitui-se em assunto complexo e profundo.
- Sua análise deve ser executada sob um ponto de vista holístico levando-se em consideração a multiplicidade de áreas do conhecimento que se fazem necessárias para o tratamento adequado da questão.

Pontos para reflexão

- A segurança cibernética deve ser um **esforço coletivo** e não pode ser vista apenas como responsabilidade de um único ator: **o Governo**.
- A questão das ameaças cibernéticas é muito mais do que apenas uma questão de segurança nacional ou defesa militar ela é uma **questão integrada** em função das inter-relações entre as áreas componentes da infraestrutura crítica de um país. Portanto, necessita de um **esforço integrado** dos setores civil e militar mantidas as suas competências individualizadas sob um ponto de vista holístico.

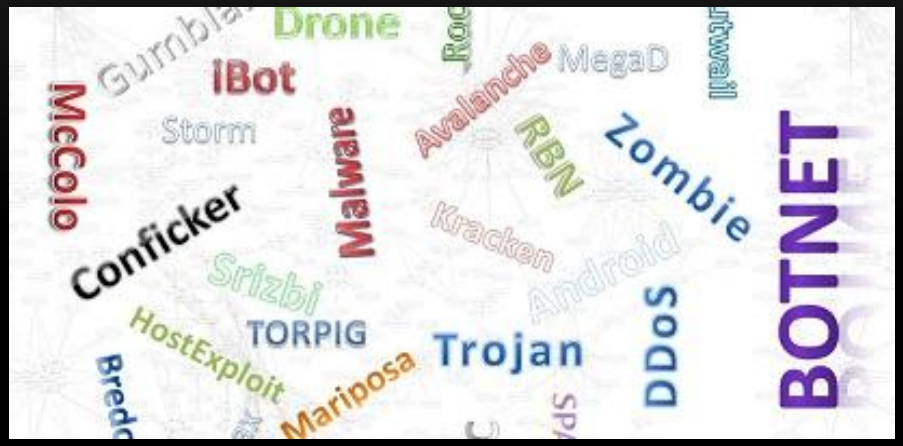
Pontos para reflexão

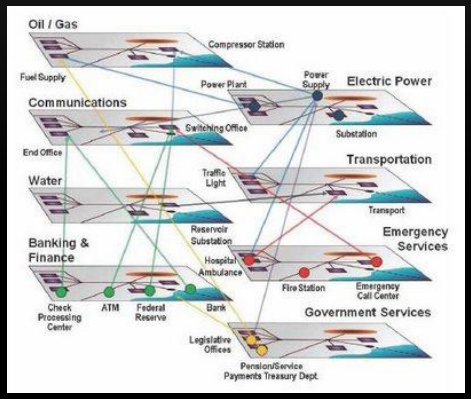
- Questões vitais para os tomadores de decisão quanto ao tratamento das ameaças cibernéticas:
  - atribuição, intenção, marco regulatório e, no campo militar, as regras de engajamento em caso de um conflito cibernético.
- Não se pode esquecer que no espaço cibernético a unidade de tempo é medida em ciclos de máquina e os tomadores de decisão devem levar isso em consideração, talvez a máxima:
  - Quem ataca primeiro tem sempre a vantagem no conflito seja uma verdade, ou não?

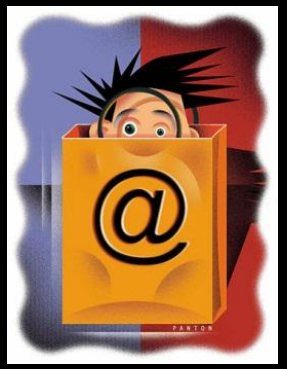
Pontos para reflexão

- Necessidade de trabalhar, com antecedência e profundidade, as questões da atribuição, intenção e dissuasão cibernética.
- Tomando por base o conceito de **visão holística** nenhum sistema, hoje em dia, deve ser analisado de maneira isolada.

Conclusão


Drone
iBot
Storm
McColo
Conficker
Malwara
Avalanche
MegaD
RBN
Zombie
Kracken
Srizbi
TORPIG
HostExploit
Mariposa
Trojan
DDoS
BOTNET


Oil / Gas
Compressor Station
Fuel Supply
Power Plant
Power Supply
Electric Power
Communications
Switching Office
Substation
End Office
Transportation
Water
Traffic Light
Transport
Reservoir
Substation
Emergency Services
Banking & Finance
Hospital Ambulance
Fire Station
Emergency Call Center
Check Processing Center
ATM
Federal Reserve
Bank
Government Services
Legislative Offices
Pension/Service Payments Treasury Dept.


@

Muito Obrigado!

Otávio Cunha

otavicunha@gmail.com