GABINETE NACIONAL DE SEGURANÇA

AGENDA

- Introdução
- Terminologia
- Enquadramento
- Caracterização do ambiente
- Panorama das ameaças
- Tipificação dos ataques
- Estado da arte de cibersegurnaça
- Modelos de cibersegurança
- Medidas
- Conclusão

GNS
Gabinete Nacional de Segurança

TERMINOLOGIA

- Evento - Qualquer ocorrência observável num SIC, por exemplo, a detecção de códigos maliciosos, falha do sistema, inundação de pacotes dentro de uma rede.

- Incidente - Um evento adverso (ou a ameaça da ocorrência) num SIC, por exemplo, códigos maliciosos, acesso não autorizado, intrusões ou de negação ou ruptura de serviços

TERMINOLOGIA (cont.)

- Ciber-espaço - Um mundo digital, gerado por computadores e redes de computadores, no qual coexistem pessoas e computadores, e que inclui todos os aspectos de actividade online.

- Ciber-segurança –. Cyber Defense - A aplicação das medidas de segurança para proteger os componentes da infra-estrutura de um SIC contra Ciber-ataques.

- Ciber-ataque - Uma forma de ciber-guerra, que pode ser combinada com um ataque físico ou não, que se destina a (no minimo) perturbar SIC do adversário.

TERMINOLOGIA (cont.)

- Cyber war – Action taken to achieve a goal by influencing and controlling the information systems, of an adversary, while protecting one's own information, computer processes and information systems.

- Cyber terrorism – A cyber attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.

TERMINOLOGIA (cont.)

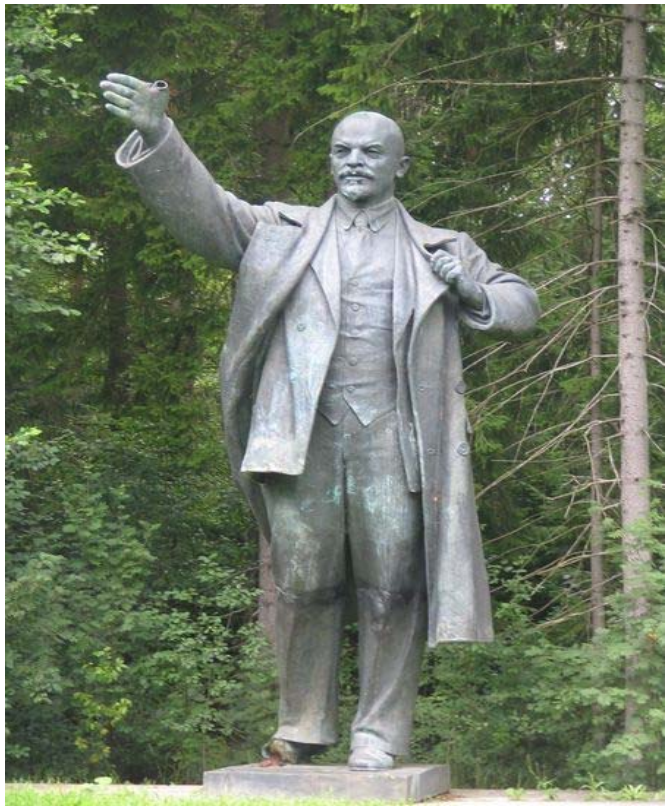
- CERT - Computer Emergency Response Team
- CSIRT – Computer Security Incident Response Team
- CIRC – Cyber Incident Response Capability

ENQUADRAMENTO - Estónia

- Data: 26 e 27Abr-18Mai07
- Origem: computadores em 178 países
- Motivação política
- Tipo de ataque
  - → Distributed Denial of service (DDoS)
  - → Botnets
  - → Ataque coordenado
  - → Ataques aos servidores de Nomes (DNS) Domain Name System)
- Sistemas afectados
  - → Servidores de instituições governamenta
  - → Online banking
  - → ISP off-line
  - → Alvos privados ao acaso

ENQUADRAMENTO - Lituânia

- Data: 28Jun08 a 2 de Jul08.
- Origem: Indeterminada (Rússia?)
- Motivação política
- Tipo de ataque
  - → Website defacement pro-soviético
  - → DDoS e e-mail spam
- Sistemas afectados
  - 300 sites afectados
  - (95% privados e 5% gov)

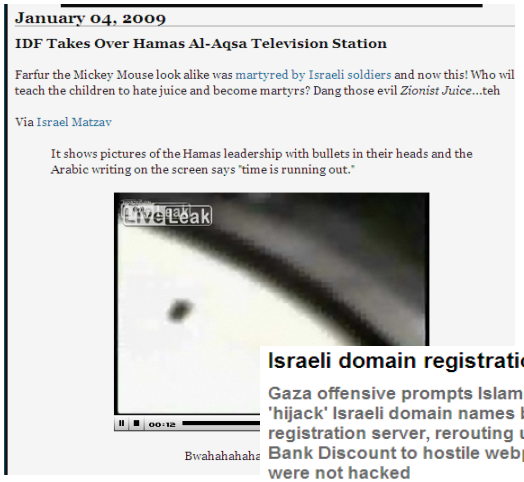


ENQUADRAMENTO - Geórgia

- Data: 08 a 28 Ago08
- Origem: Grupos organizados de hackers russos
- Motivação política
- Tipo de ataque
  - → SW malícioso
  - → DDoS
- Sistemas afectados
  - → Governo (Site Presidencial, parlamento, etc)
  - → "Media" e Finanças

ENQUADRAMENTO -Israel - Hamas

- Data: Jan09.
- Origem: Israel
- Motivação política
- Tipo de ataque
  - → Intrusão
  - → Defacement
- Sistemas afectados
  - → Estação televisão Al-Aqsa
  - → Ataque DNS



Israeli domain registration server hacked

Gaza offensive prompts Islamic group Team Evil to 'hijack' Israeli domain names by hacking into registration server, rerouting users of Ynetnews, Bank Discount to hostile webpage. Original sites were not hacked

Niv Lillian
Published: 01.02.09, 14:47 / Israel News

An Islamic group based on Morocco hacked into DomainTheNet's registration system server on Friday, effectively "highjacking" various prominent domain names, the likes of ynetnews.com and Bank Discount, and rerouting users to a page featuring anti-Israel messages

DomainTheNet is a multinational registration service provider (RSP), which offers registration and site-hosting services. The attack is believed to be in retaliation to Operation Cast Lead in the Gaza Strip.

The attack resulted in some users being referred to the hostile webpage, while others were able to access the original websites, undisturbed. **The group did not hack the actual websites.**

The hostile webpage

CARACTERIZAÇÃO DO AMBIENTE

Princípios

Era Industrial	Cyber Era
Os Estados como adversários;	Grupos em rede como adversários;
Forças concentradas;	Forças difusas;
Vantagem de “poder de fogo”;	Vantagem de Informação;
Força intimidadora.	Força omnipresente.

CARACTERIZAÇÃO DO AMBIENTE

Estratégia

Era Industrial	Cyber Era
❑ Alvos: Militar/Industrial;	❑ Alvo: Infra-estruturas críticas;
❑ Sucesso medido pela destruição de equipamentos	❑ Sucesso medido pela protecção/destruição de valor;
❑ Baseado na dissuasão.	❑ Baseado na resiliência.

CARACTERIZAÇÃO DO AMBIENTE

Táctica

Era Industrial	Cyber Era
❑ Os sistemas de informação como suporte;	❑ Os sistemas de informação como armas;

CARACTERIZAÇÃO DO AMBIENTE

O processo de decisão

Era Industrial	Cyber Era
▫ Centralização das decisões; ▫ Clareza sobre a identidade do adversário; ▫ Problemas em encontrar/ deduzir padrões (informação insuficiente).	▫ Distribuídos de forma flexível, a tomada de decisão; ▫ Incerteza sobre a identidade do adversário; ▫ Problemas com reconhecimento de padrões (excesso de informação).

CARACTERIZAÇÃO DO AMBIENTE

Ataque	Defesa
❑ Muito atractivo ❑ Baixo custo ▪ Subornar ▪ Criar informações falsas ▪ Manipular informação ▪ Utilização de armas lógicas ❑ Lançada de qualquer parte do mundo ❑ Não deixa rasto ❑ Tecnologia gratuita na Internet	❑ Amplos recursos para desenvolver: ▪ Ferramentas ▪ Processos ▪ Procedimentos ❑ Custo elevado ❑ Limites tecnológicos ❑ Limites humanos ❑ Não se consegue antecipar tudo ❑ A Ameaça interna

PANORAMA DAS AMEAÇAS

- Três vectores:
  - → Estão amplamente disponíveis, sendo baratos e fáceis de utilizar;
  - → A sociedade tende a confiar em produtos informáticos disponibilizados pelo mercado;
  - → Virtualmente qualquer indivíduo com um computador e a necessária habilidade, pode tornar-se num pirata informático ou até mesmo num "ciber-terrorista".

PANORAMA DAS AMEAÇAS

- Crackers ou Hackers com intenções maliciosas
- Grupos de pressão
- Organizações terroristas
- Estados

PANORAMA DAS AMEAÇAS - Gary Mckinnon

«Foi ridiculamente fácil», afirmou. «Eu não sou uma mente criminosa muito esperta que trabalhou uma estratégia. Eu fiz uma expedição pelas palavras passe administrativas - que nunca tinham sido mudadas - e foi incrivelmente surpreendente quantas eu descobri mesmo ao mais alto nível».

PANORAMA DAS AMEAÇAS - Kevin Mitnick

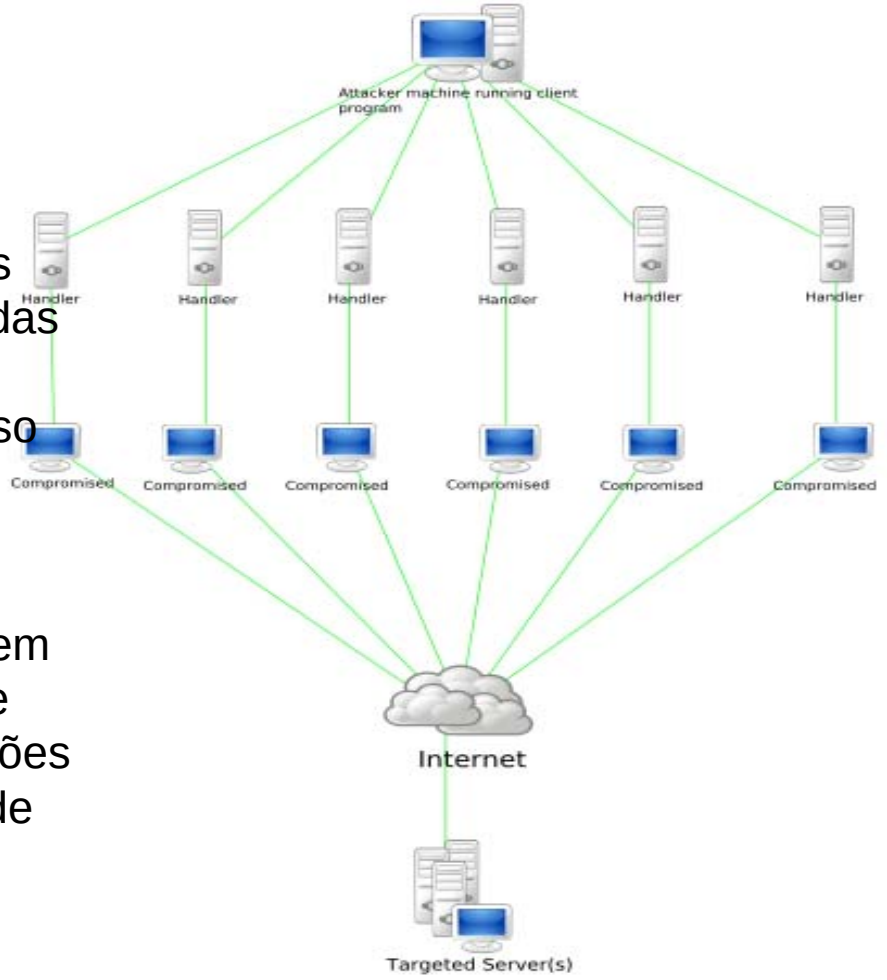
Embora Mitnick fosse capaz de feitos tecnológicos consideráveis (como manipular redes de telemóveis para aceder à Internet sem ser detectado), a sua principal estratégia para invadir computadores foi o que ele chama de «**engenharia social**», ou seja, enganar funcionários de empresas de informática para conseguir senhas e contas de acesso.

TIPIFICAÇÃO DOS ATAQUES

- **Botnets:**
  - → De forma resumida, Uma “botnet” é uma rede de máquinas infectadas (Maquina=robot=bot em rede (net)) . Os “Bots” são softwares maliciosos que se espalham de maneira autonoma (tal como um worm), aproveitando vulnerabilidades que podem ser exploradas remotamente, Passwords fáceis de adivinhar, ou mesmo usuários mal informados que executam inadvertidamente arquivos recebidos pela Internet. Os “bots” conectam-se normalmente atraves de IRC (Internet Relay Chat) a um determinado canal de um ou mais servidores IRC. Normalmente, o software usado para gerir estes canais é modificado de forma que sirvam mais “bots” e que não revelem a quantidade de “bots” associados, formando uma “botnet”, que o atacante controla por meio de comandos no canal IRC.
  - → Botnet é controlada por um computador mestre ("Master"), que tem sob seu comando um conjunto alargado (milhares) de computadores ("Zombies").

TIPIFICAÇÃO DOS ATAQUES

- **DDoS (DDoS-Distributed Denial of Service):**
  - → De forma resumida, o ataque consiste em fazer com que os "Zombies" (máquinas infectadas e sob comando do "Master", acedam a determinado recurso num determinado servidor à mesma data/hora. Como servidores web possuem um número limitado de ligações em simultaneo "slots", o grande e repentino número de requisições de acesso esgota o número de "slot", tornando esse recurso indisponível para os seus utilizadores.



ESTADO DA ARTE CIBERSEGURANÇA

- Cibersegurança ≠ CERT

- Cibersegurança =
  - → Hardening +
  - → Defense +
  - → Hunting
  - → (H+D+H)

ESTADO DA ARTE CIBERSEGURANÇA - Hardening

- Configuração de sistemas/produtos/redes
- Definição de requisitos de segurança (Global, Local e sistemas)
- Definição de procedimentos operacionais de segurança
- …

ESTADO DA ARTE CIBERSEGURANÇA - Defense

- Mecanismo de dissuasão
- Resposta a incidentes (CERTs)
- Capacidade de recuperação
- …

ESTADO DA ARTE CIBERSEGURANÇA - Hunting

- Forensics;
- Serviços de informações
- Avaliação de ameaças (Hackers, Crime organizado, Terroristas, Estados)
- “Common Picture” das ameaças
- …

MODELOS DE CIBERSEGURANÇA

- EUA:
  - → As responsabilidades de coordenação de cibersegurança e Information Assurance estão a cargo da NSA (National Security Agency).
  - → São o ponto central de controlo das ciber ameaças.
  - → A NSA tem capacidade e responsabilidades: Criptografia, sistemas seguros, certificação de sistemas e produtos (Nacionais e common criteria), criptologia, information assurance.

MODELOS DE CIBERSEGURANÇA (cont)

- Alemanha:
  - → As responsabilidades de coordenação de cibersegurança e Information Assurance estão a cargo da BSI
  - → O BSI é Autoridade Nacional de Comunicações;
  - → A BSI tem capacidade e responsabilidades: Criptografia, sistemas seguros, certificação de sistemas e produtos (Nacionais e common criteria), produção de doutrina e normas.
  - → Desde 2009 que o BSI, apesar de não ter redes para monitorizar, ficou ponto central de repporting de todos os incidentes, de modo a gerir uma BD de histórico de incidentes para memoria futura e constituição actualizada da common picture de ameaças,

MODELOS DE CIBERSEGURANÇA (cont)

- Noruega:
  - → As responsabilidades de coordenação de cibersegurança e Information Assurance estão a cargo da Autoridade Nacional de Segurança da Noruega. NA orgânica da ANS da Noruega foi contituido o NoCERT.
  - → A ANS NO tem capacidade e responsabilidades: Criptografia, sistemas seguros, certificação de sistemas e produtos (Nacionais e common criteria), produção de doutrina e normas, Information Assurance e Cibersegurança.
  - → O NoCERT tem como responsabilidades primárias a coordenação de incidentes e o cyber threat assessment.

MODELOS DE CIBERSEGURAnça (cont)

- Noruega:
  - → Laboratório de forensics
  - → Centro de monitorização de ameaças.
  - → Foi construído (desenvolvido) um sistema de sensores (VDI) com monitorização central.
  - → Cada rede (Publicas e privadas) que está integrada no VDI, é monitorizada (no sistemas de protecção de fronteira) através da introdução de 1 ou mais sensores

MEDIDAS

- Resposta institucional perante incidentes
- Constituição de Departamentos/Fóruns de Segurança da Informação
- Implementar políticas de segurança
- Direccionar os esforços para obtenção de certificação em segurança da informação
- Criação de Computer Security Incident Response Team (CSIRT), nos diversos níveis
- Formação e treino dos colaboradores
- Aplicação de medidas de protecção adequadas

CONCLUSÃO

"A SEGURANÇA NÃO É UM SENTIMENTO, É UM ESTADO QUE SE ATINGE PELA ADOPÇÃO DE MEDIDAS QUE PERMITAM A CONSCIENTE ACEITAÇÃO DO RISCO"

Assim:

- → Não existem sistemas de informação 100% seguros!
- → Não existem soluções milagrosas que combatam todas as ameaças e colmatem todas as vulnerabilidades!
- → A segurança é um processo DINÂMICO
- → **As arquitecturas de segurança são cada vez mais complexas**

CONCLUSÃO

- Os ataques DDoS attacks serão a maior ameaça no futuro próximo. Grande probabilidade de desenvolvimento de diversas formas, nomeadamente:
  - → Botnets hierarquicas, atraves de vários niveis de controlo. Os niveis secundários terão tarefas de controlo operacional., enquanto que o niveis de topo, terão maior inteligencia, controlo dos ataques em tempo real e capacidade para acultar a identidade dos atacantes.
  - → Extensões semanticas de DDoS serão possiveis, nas quais os sistemas de informação serão atacados por um conjunto alargados de pedidos de serviços, especialmente aquekles que requerem muito processamento.
- No curto prazo os ataques incidirão e terão como objectivo primordial o roubo de informação (configurações de redes, dados operacionais/tecnicos)
- As pequenas nações serão mais vulneraveis, especiamente aquelas que dispoem de menor largura de banda

GABINETE NACIONAL DE SEGURANÇA

QUESTÕES