Fundamentos de Segurança Informática (FSI)

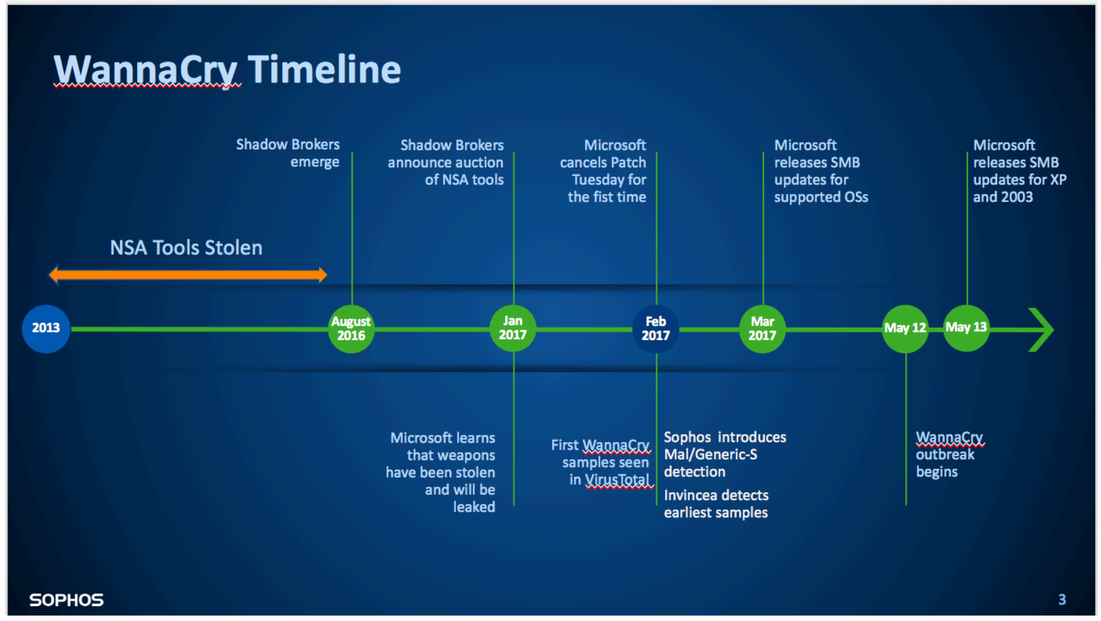
2021/2022 - LEIC

Manuel Barbosa
mbb@fc.up.pt

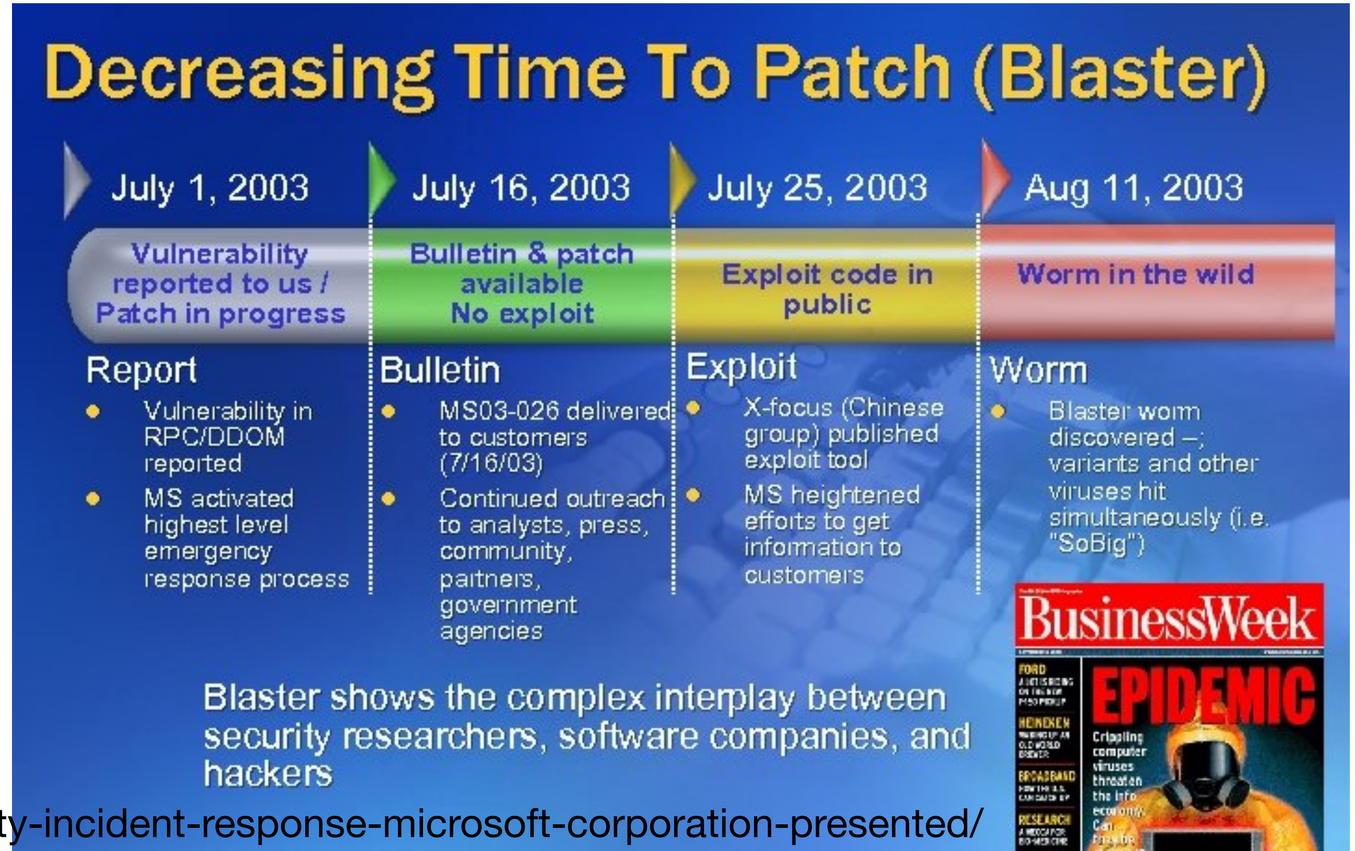
Aula 11
Malware

Exemplos de tomada de controlo

- Atacar um serviço vulnerável exposto na rede (internet toda em 10m!):
  - típico de worms: e.g., Morris (1998), Blaster (2003), Wannacry (2017)



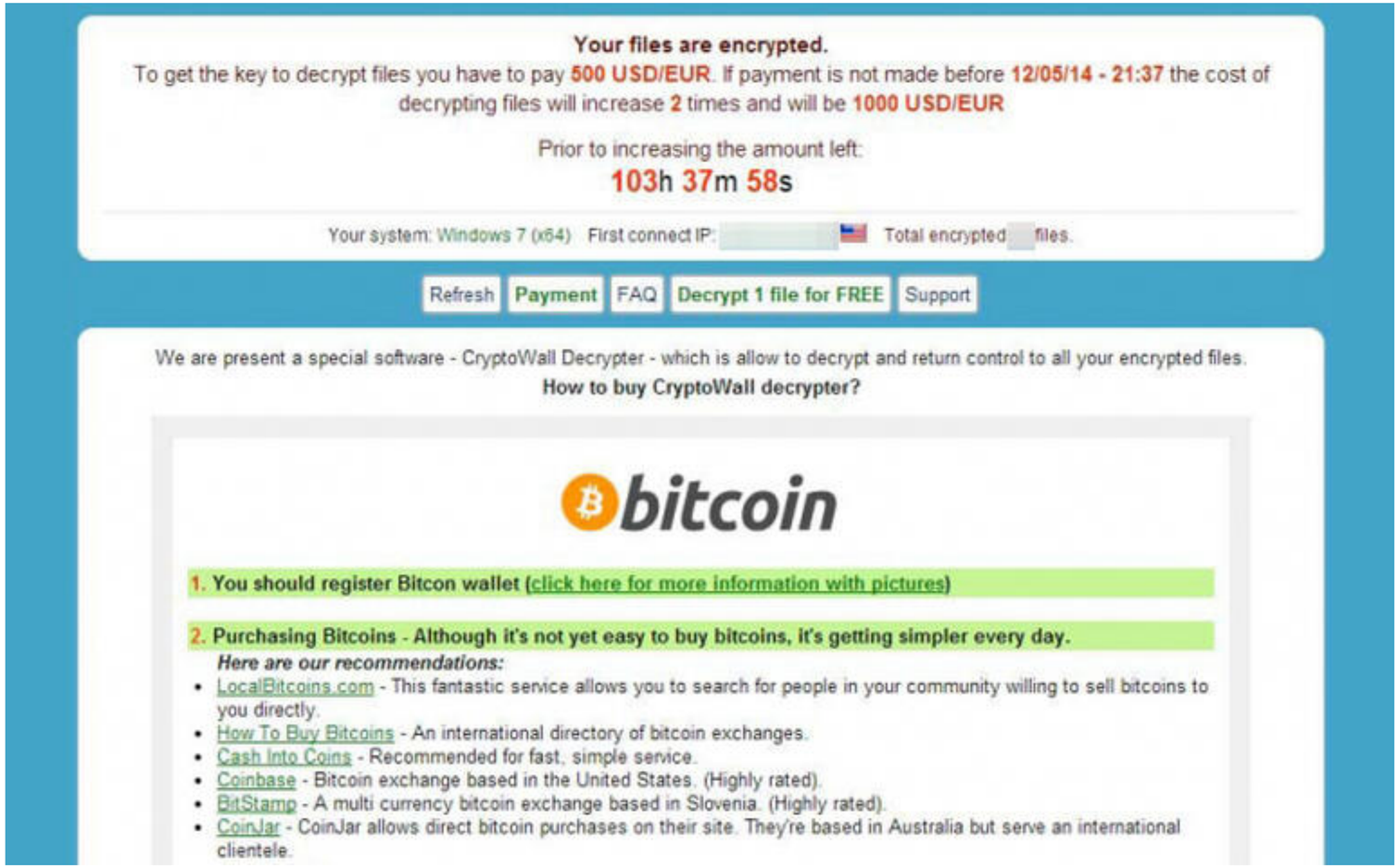
https://news.sophos.com/en-us/2017/05/19/wannacry-how-the-attack-happened/



fonte: Microsoft
https://slidetodoc.com/patch-warfare-security-incident-response-microsoft-corporation-presented/

Exemplos de tomada de controlo

- Servidor web malicioso injeta malware nos clientes
  - *Malvertising*: utilizar sistemas de placement de anúncios para chegar até browsers vulneráveis
  - Exemplo: Cryptowall (adaptação CryptoLocker)



Exemplos de tomada de controlo

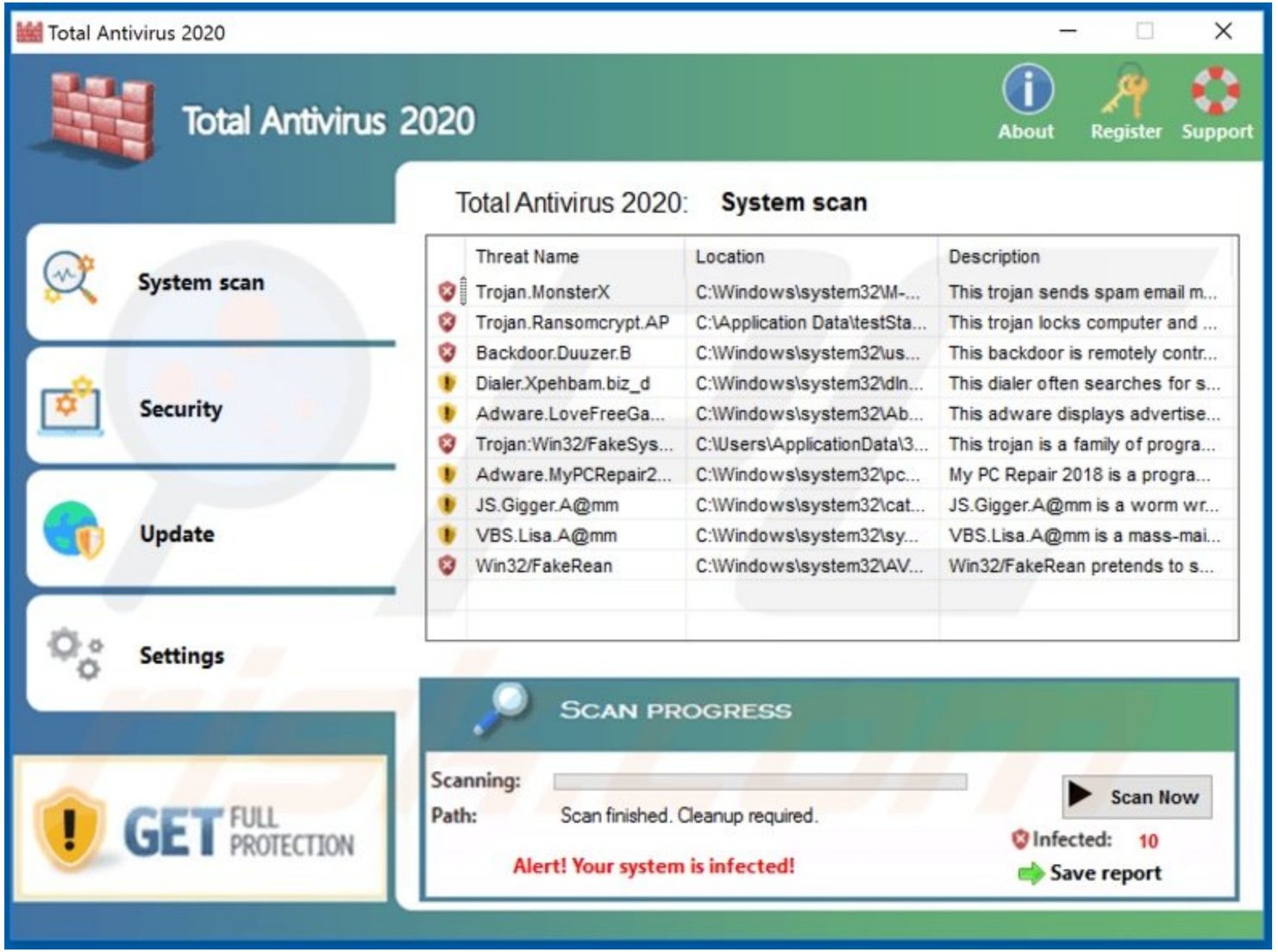
- Servidor web malicioso injeta malware nos clientes
  - O governo dos EUA descreve isto como uma técnica de investigação criminal

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the TARGET WEBSITE, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the TARGET WEBSITE, located in the Eastern District of Virginia,the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information. The NIT will not deny the user of the "activating" computer access to any data or functionality of the user's computer.

https://www.lawfareblog.com/examining-fbi-hacking-warrant

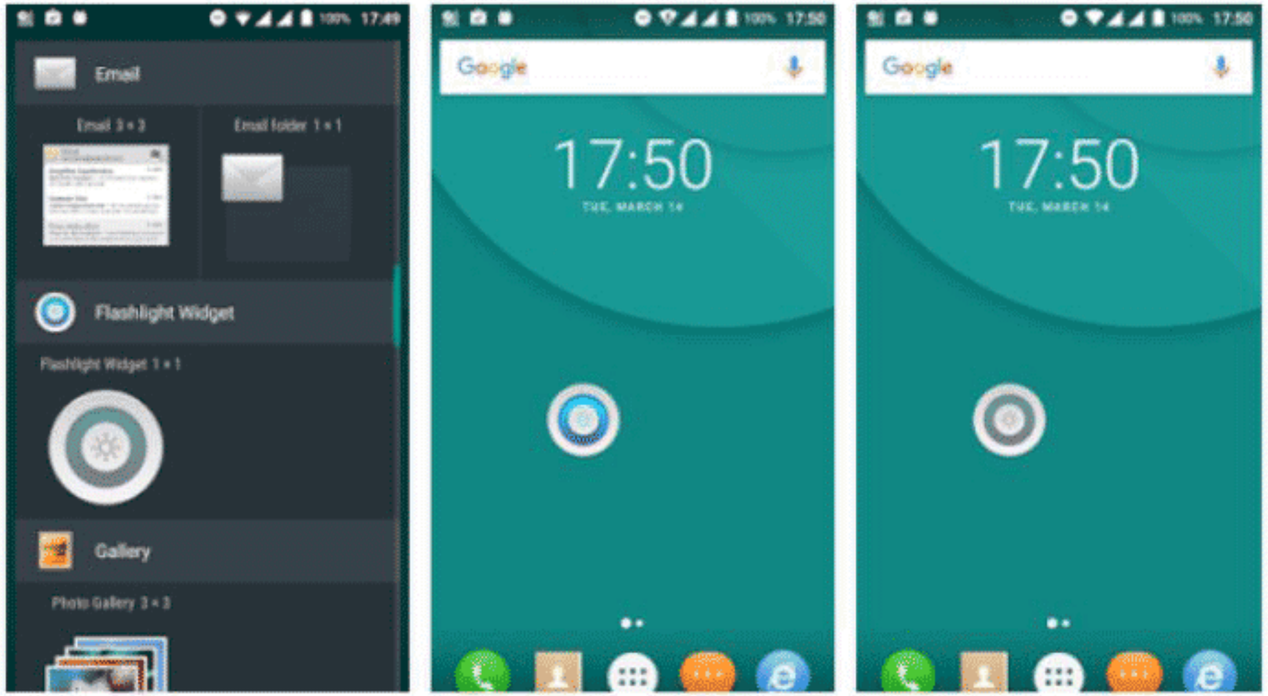
Exemplos de tomada de controlo

- Software enganador: convence o utilizador a instalar/executar
  - Fake Antivirus: oferece serviços, mas depois toma conta da máquina



Exemplos de tomada de controlo

- Software enganador: convence o utilizador a instalar/executar
  - Aplicações "giras"
  - Roubam credenciais



You scared at night? Just turn on Flashlight!

Flashlight LED Widget is the super simple widget that turns your phone's LED flash into a super bright flashlight that you control with a tap!

It's free of cost and doesn't contain any ads!
Just try it and enjoy!

Exemplos de tomada de controlo

- Software enganador: convence o utilizador a instalar/executar
  - "Isco" para apanhar dissidentes

On Friday the 13th of July 2012, the Moroccan citizen media and journalism project Mamfakinch[3] was targeted by an electronic attack that used surveillance malware. Mamfakinch.com, a website that is frequently critical of the Moroccan government, received a message via their website directing recipients to a remote webpage:

> Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d embrouilles...
> http://freeme.eu5.org/scandale%20(2).doc

The page, found at http://freeme.eu5.org/scandale%20(2).doc prompted the user for the installation of malicious java, file, “adobe.jar”:

> 53cd1d6a1cc64d4e8275a22216492b76db186cfb38cec6e7b3cfb7a87ccb3524 adobe.jar

https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

Exemplos de tomada de controlo

- Engenharia social: convence o utilizador a instalar/executar
  - USB autorun
  - salta airgaps (stuxnet)

2016 IEEE Symposium on Security and Privacy

Users Really Do Plug in USB Drives They Find

Matthew Tischer† Zakir Durumeric‡† Sam Foster† Sunny Duan†
Alec Mori† Elie Bursztein◇ Michael Bailey†

† University of Illinois, Urbana-Champaign ‡ University of Michigan ◇ Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu
zakir@umich.edu elieb@google.com

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

Exemplos de tomada de controlo

- Deturpar equipamento no fabrico

https://hackaday.com/2017/05/31/counterfeit-hardware-may-lead-to-malware-and-failure/
https://www.edn.com/guide-for-spotting-counterfeit-cisco-equipment/

Exemplos de tomada de controlo

- Deturpar equipamento em transito

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

Exemplos de tomada de controlo

- Atacar fornecedor de sofware, injetar updates que contêm backdoors!

Juniper admits to “multiple security issues” with ScreenOS

Juniper Networks Inc. has provided more details about the “unauthorized code” found in its ScreenOS operating system for firewalls.

The company made the revelation that apparent “spying code” was found in ScreenOS versions 6.2.0r15 to 6.2.0r18, and 6.3.0r12 to 6.3.0r20 last week. Over the weekend, the company posted an article on the knowledge base section of its website, detailing two particular vulnerabilities through which someone with knowledge of the code can access sensitive data.

“The first issue allows unauthorized remote administrative access to the device over SSH or telnet,” Juniper said in its post. “Exploitation of this vulnerability can lead to complete compromise of the affected system.”

The company adds that skilled attackers would also be able to remove any trace of their presence in a compromised network by removing entries from the local log file, thereby eliminating any signature that might tell admins the network has been compromised.

Exemplos de tomada de controlo

- Atacar fornecedor de sofware, injetar updates que contêm backdoors!

The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal

- **SolarWinds was the subject of a massive cybersecurity attack that spread to the company's clients.**
- **Major firms like Microsoft and top government agencies were attacked, and sensitive data was exposed.**

https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Exemplos de tomada de controlo

- Atacante tem acesso direto à máquina comprometida

Interpol Now Supporting The Coalition Against Stalkerware To Fight Tech-enabled Abuse

Controlo é um serviço

- Hacking team
  - https://en.wikipedia.org/wiki/Hacking_Team
- NSO group
  - https://www.bbc.com/news/technology-57922664
- Há governos que pagam muito $ por estes produtos/serviços
- Isto gera um enorme mercado para vulnerabilidades/exploits
  - zero day => porta aberta para novo malware

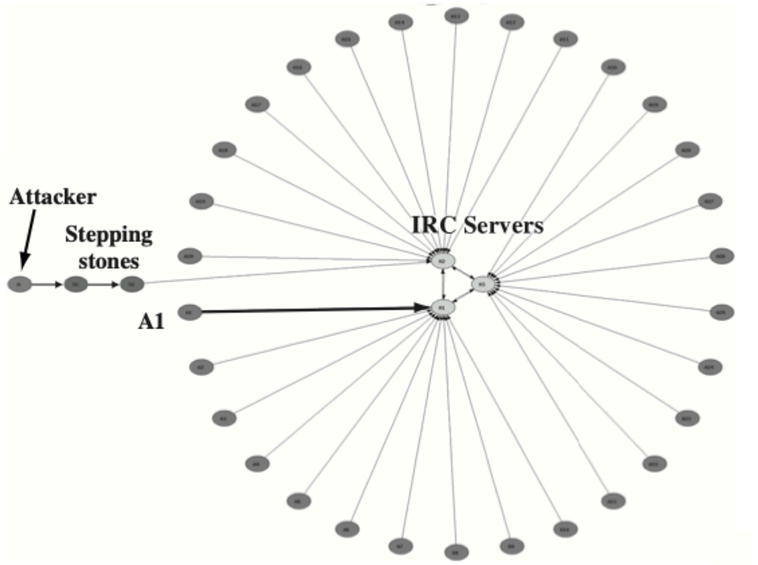
Botnets

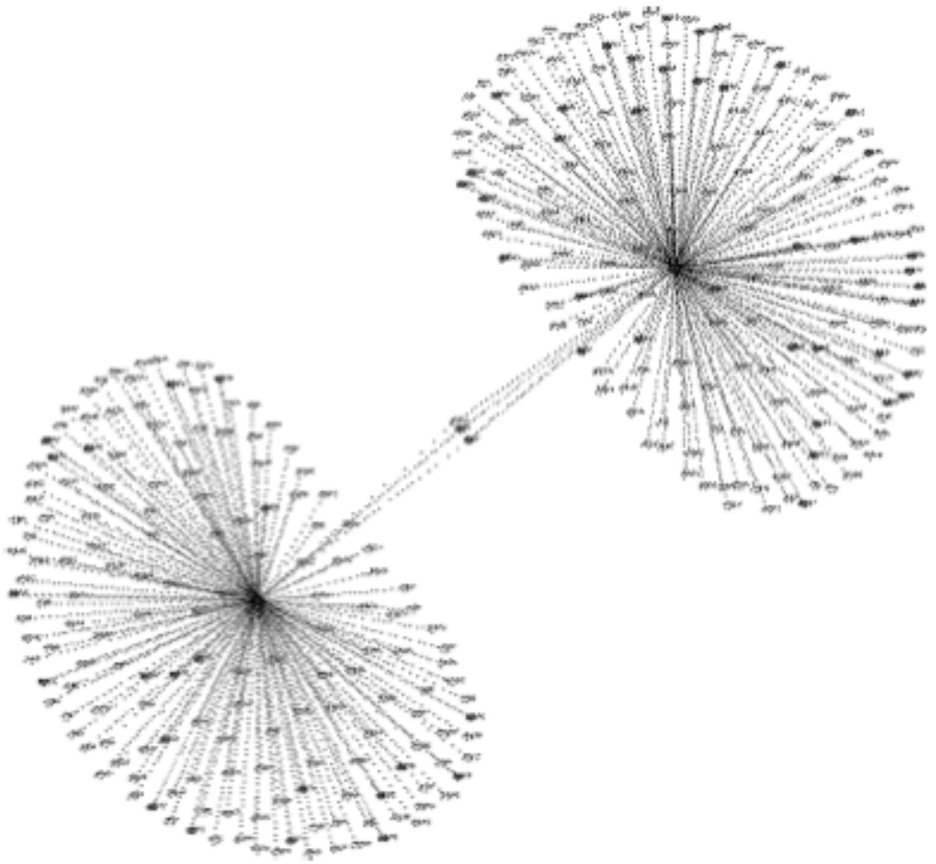
- Uma botnet é uma rede de computadores com um sistema de comando e controlo (C2) comum:
  - cada computador é chamado um *bot*
- O controlador envia comandos através da rede:
  - spam, phishing, DoS, roubo de informação local, etc.
- As *botnets* têm geralmente a capacidade de se actualizar automaticamente

Botnets

- Dois tipos de arquitectura:
  - centralizada, com múltiplos servidores centrais para robustez
  - peer-to-peer, auto organizada (worker vs proxy), hierárquica
- Dois tipos de fluxo:
  - push => servidor envia comandos
  - pull => bot pergunta se há comandos
- Recuperação/resiliência no caso de ataque ao controlador
  - procurar por novos servidores utilizando algoritmos de geração dinâmica de domínios

Botnets: Diferentes modelos





https://www.usenix.org/legacy/event/leet08/tech/full_papers/holz/holz.pdf
https://www.usenix.org/system/files/login/articles/525-dittrich.pdf

Botnets: Deteção e Combate

- Estratégias
  - Detectar o malware na máquina comprometida
  - Detectar tráfego de rede para comunicação com C2
  - Expor máquinas (honeypots) para serem comprometidas e monitorizadas
- Combate
  - Limpar máquinas comprometidas e/ou isola-las da rede
  - Isolar/desligar o C2
  - Tomar o controlo do C2 e usa-lo para desativar botnet

Deteção

Combater Malware

- Terminologia:
  - Intrusion Detection System
  - Intrusion Prevention System
  - HIDS/NIDS: Host/Network Based IDS
- IDS => deteção ocorre depois do ataque ter sido concretizado
- IPS => intervenção rápida para evitar ataque (e.g., packet filtering)
- Muitas ferramentas => uma mistura dos dois

Erros de Deteção

- Falso positivo: alerta para um problema que não existe
- Falso negativo: ausência de alerta para problema existente
- A precisão é geralmente especificada relativamente à frequência de ocorrência destes erros:
  - I => evento de intrusão, D => evento de alerta/deteção
  - Falso positivo => Pr [D | not I]
  - Falso negativo => Pr [not D | I]

Erros de Deteção

- Deteção perfeita:
  - será que podemos ter 0% de falsos negativos?
    - sim => alerta em todos os cenários!
  - será que podemos ter 0% de falsos positivos?
    - sim => nunca lançar alerta
- Na prática pretende-se um bom equilíbrio:
  - E.g., 0.1% FP + 2 % FN
  - Como parametrizar? Depende do custo de um erro!

Erros de Deteção

- Problemas na prática:
  - Cenário 1: servidor que atende 1K pedidos/dia, sendo 5 maliciosos
    - FP a 0.1% => 1 falso positivo/dia
    - FN a 2% => 0.1 falso negativo/dia (menos do que um por semana)
  - Cenário 2: servidor que atende 10M pedidos/dia, sendo 5 maliciosos
    - FP a 0.1% => 100 falsos positivos/dia! para os mesmos falsos negativos
    - Problema: quando a frequência relativa de ataques é muito baixa, é difícil ter um sistema eficaz e eficiente

Como se detecta malware?

- Signature-based: reconhecer assinaturas, padrões em ataques conhecidos (*black listing*)
  - fácil de implementar, eficaz contra ataques conhecidos
- Anomalias: utilização de recursos, e.g., acesso a rede anómalo, acessos a ficheiros sensíveis, etc.
  - ideal para deteção de uma larga gama de ataques, sem enumeração exaustiva
  - menos preciso com ataques conhecidos e particularmente sensível a eventos raros
- Integridade/especificação: especificar o que é correto, manter registo que permite detetar alterações a ficheiros críticos (e.g., checksum criptográfico, *whitelists* de processos)
  - pode apanhar ataques novos, mas exige muito esforço e constante actualização
- Todos estes métodos podem ser aplicados a diferentes níveis semânticos: rede, processos, URLs.

Antivirus: Deteção de Assinaturas

- Os virus não podem ser totalmente invisíveis
  - O código está armazenado algures
  - O vírus muda qualquer coisa quando executa
  - Para vírus conhecido: extrair assinatura, padrão único
- Dificuldades:
  - onde procurar? como procurar (e.g., apenas string search ou correr programa?)
  - frequência, duração?
  - como detetar vírus que mudam de forma?

Antivirus: Deteção de Assinaturas

- Onde procurar? Geralmente head/tail => string padrão no princípio e fim dos ficheiros
  - Evolução => procurar com base no control-flow do programa (entry points, saltos, etc.)
- Temos uma corrida às armas:
  - Evolução para vírus cifrados => o vírus re-cifra-se com uma nova chave, pelo que os padrões alteram-se de um ficheiro para outro!
  - desde que o código que decifra o virus se mantenha, ainda fácil de detectar
  - evolução para polimorfismo => a própria rotina de decifração é alterada!
  - o vírus inclui um "mutation engine" que sintetiza versões alternativas do código
  - problema de investigação atualmente => execução controlada

Antivirus modernos

- Bloqueio de URL/Web: utilizadores são avisados/impedidos de visitar sites perigosos
- Scanning de rede (especialmente HTTP)
  - Detectar e bloquear ataques conhecidos
  - Detectar e bloquear comunicação de malware
- Scanning de "payload"
  - detetar e bloquear malware conhecido
  - auto-actualizar assinaturas de malware
- Consulta online de sistemas de reputação para feedback rápido de problemas

Antivirus modernos (HIDS)

- Execução em sandbox
  - permitem executar alguns programas numa sandbox
  - analisar utilização de recursos e comportamentos suspeitos (e.g., código que se modifica a si mesmo)
- Scanning de ficheiros para deteção de malware no disco
- Scanning de memória para malware que nunca se armazena no disco
- Monitorização de métricas em runtime para detetar anomalias

Deteção na rede (NIDS)

- Monitorização de toda a rede e não só da fronteira com o exterior
- Análise completa do protocolo: extração de objetos complexos e vasto número de protocolos
- Análise de assinaturas e comportamentos:
  - ataques conhecidos e comunicação de malware
  - "payloads conhecidas”, sequências/padrões de atividade
- Execução "shadow" para deteção de problemas: e.g., análise de PDF, Flash, etc.
- Logging => análise forense
- Atualização automática de assinaturas, black lists, etc

NIDS vs HIDS

- Benefícios do NIDS:
  - um sistema único permite proteger N sistemas diversos
  - mais simples de gerir e instalar
  - não ocupa recursos nos sistemas em produção
  - mais difícil acesso para os atacantes

NIDS vs HIDS

- Benefícios do HIDS:
  - tem acesso direto à semântica da atividade maliciosa
    - observa os efeitos do ataque
    - mais difícil de contornar, porque é mais preciso
  - protege de ameaças que não vêm da rede (e.g., USB)
  - é possível observar dados que estão cifrados na rede
  - não afeta o sistema todo, é possível configurar de maneira mais fina