#### **WannaCry**

O WannaCry foi um dos maiores ataques de ransomware de sempre,e passou-se em Maio de 2017.

##### Porque ficou famoso?

O ataque afetou centenas de milhares de computadores em mais de 150 países num curto período de tempo. Entre os computadores afetados encontravam-se diversas infraestruturas críticas, incluindo hospitais, telecomunicações, empresas de transporte e organizações governamentais. O caso pior aconteceu no Serviço Nacional de Saúde (NHS) do Reino Unido, onde muitos hospitais tiveram que cancelar consultas e cirurgias - ponde em risco a vida de várias pessoas (embora não consegui encontrar dados oficias de mortes como resultado do ataque)

##### O que era o WannaCry?

O WannaCry era um ransomware, um tipo de malware que criptografa os arquivos dos users e exige um pagamento de resgate em Bitcoin para liberá-los.

##### Como ele entrou nas máquinas dos utilizadores?

O WannaCry espalhou-se através de emails de phishing e explorou uma vulnerabilidade chamada EternalBlue no sistema operativo Windows, que permitia a execução remota de código em sistemas desatualizados.

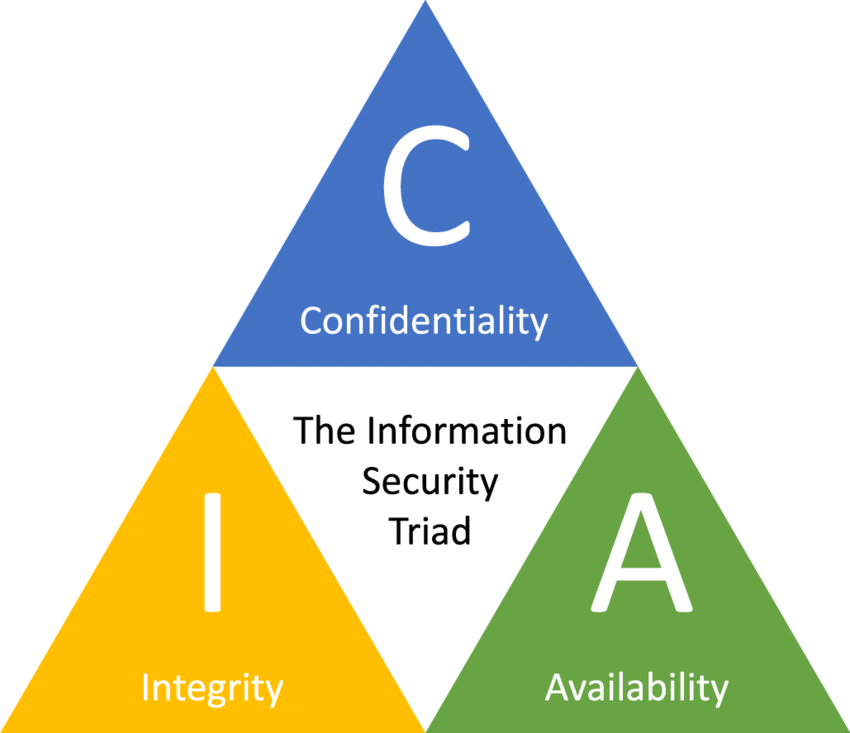
##### O que ele fez quando entrou nas máquinas?

Após infectar uma máquina, o WannaCry criptografava os arquivos, tornando-os inacessíveis, e exibia uma mensagem de resgate exigindo pagamento para a descriptografia.

##### De que falhas de cibersegurança ele se aproveitou?

O WannaCry explorou a vulnerabilidade EternalBlue no Windows, que a NSA tinha descoberto anteriormente (mas mantido em segredo) e que foi vazada pelo grupo de hackers Shadow Brokers. Muitos sistemas ainda não tinham aplicado o patch de segurança que resolvia essa vulnerabilidade (o patch MS17-010, lançado pela Microsoft). Esses computadores estavam portanto vulneráveis ao ataque.

##### Impacto no Triângulo CIA



* **Confidentiality (Confidencialidade)**: O WannaCry não focou diretamente em violar a confidencialidade dos dados, mas ao criptografar os arquivos, tornou-os inacessíveis, o que indiretamente afeta a confidencialidade ao impedir que os dados sejam utilizados.
* **Integrity (Integridade)**: O ransomware comprometeu a integridade dos sistemas ao modificar o estado dos arquivos (criptografando-os) sem o consentimento dos users.
* **Availability (Disponibilidade)**: A disponibilidade foi severamente afetada, pois os dados criptografados pelo WannaCry ficaram inacessíveis até que o resgate fosse pago ou os dados fossem restaurados de backups.

**A historia em mais detalhe:**

**O Caso:** WannaCry

**O que aconteceu?** Os attacantes criptografavam os dados dos computadores e exigiam um resgate em Bitcoin (i.e. uma ransomware) para desencriptar os arquivos.

**Como aconteceu?**

Passo 1: A Descobertade uma vulnerabilidade - EternalBlue (CVE-2017-0147)

A Agência de Segurança Nacional dos EUA (NSA) descobre uma vulnerabilidade crítica no Windows chamada EternalBlue, que permite a execução de código remoto em sistemas Windows desatualizados.

Nota importante: **Esta informação não era de conhecimento público** e foi mantida em segredo pela NSA para uso em operações de inteligência.

(não se sabe oficialmente desde quando a NSA sabia de existencia desta vulnerabilidade)

Passo 2: A fuga de informação (em Março de 2017)

Um grupo de hackers conhecido como Shadow Brokers descobre e vaza a vulnerabilidade EternalBlue, tornando-a disponível publicamente. Isso abriu caminho para que cibercriminosos passassem a explorar essa mesam vulnerabilidade.

Passo 3: A criação do WannaCry (durante Abril de 2017)

Cibercriminosos desenvolvem o ransomware WannaCry explorando a vulnerabilidade EternalBlue.

O ataque consegue criptografar arquivos em computadores infectados e depois os criminosos passam a exigir um resgate em Bitcoin (ransomware).

Passo 4: A primeira infeção e posterior propagação (12 de Maio de 2017)

O WannaCry espalhou-se inicialmente através de e-mails de phishing e daí foi explorando diretamente a vulnerabilidade EternalBlue em redes desprotegidas. A Propagação foi exponencial pois uma vez que um computador era infectado, o WannaCry propagava-se rapidamente para outros computadores na mesma rede (usando a vulnerabilidade EternalBlue).

Passo 5: A criptografia e o pedido de resgate

O WannaCry criptografava arquivos no computador infectado, tornando-os inacessíveis para os seus utilizadores. Nas suas máquinas os utilizadores viam uma mensagem de resgate exigindo pagamento em Bitcoin para descriptografar os arquivos.



Passo 6: A resolução do problema

Um especialista de segurança (Marcus Hutchins, também conhecido online como "MalwareTech") descobre um domínio descobriu um domínio oculto dentro do código do WannaCry. Ele registrou esse domínio que o WannaCry estava a usar e que passou a funcionar como um "kill switch" parando a propagação do WannaCry em muitos sistemas infectados.

Mas isto só resolveu o problema da propagação. (ainda assim estima-se que mais de 300.000 computadores em 150 países já tinham sido afetados.)

Além disso, existia tambem o Patch MS17-010. Ainda em março de 2017, e antes do ataque, a Microsoft lançou o patch MS17-010 para corrigir a vulnerabilidade EternalBlue. No entanto, muitos sistemas não foram atualizados a tempo.

Faltava ainda descriptografar os dados nos computadores já afetados. Para isso havia varias opções:

* Pagando o Resgate: Alguns users optaram por pagar o resgate exigido pelos atacantes na esperança de que seus arquivos fossem descriptografados. Mas estima-se, de acordo com análises de blockchain, que aproximadamente $130.000 em Bitcoin foram pagos às carteiras associadas ao WannaCry. Um valor relativamente baixo tendo em conta a dimensão do ataque.
* Recorrendo a Backups: Organizações e users que possuíam backups dos seus dados puderam restaurar suas informações a partir dessas cópias.
* Reinstalando o Sistema: Em casos onde não havia backups disponíveis, alguns users precisaram reinstalar o sistema operacional - **mas perderam todos os dados criptografados.** A recuperação completa só era possível se existissem backups.
* Desenvolvimento de funções de desencriptação: Mais tarde, a 19 de maio de 2017 é desenvolvido o WannaKey (Ela funcionava explorando uma falha no processo de criptografia do WannaCry, mas apenas se o computador não tivesse sido reiniciado após a infecção.) Depois houve outas funções semelhantes como o WannaCry File Restorer e o wanakiwi.