Clase 3:
Complejidad, extensibilidad y conectividad + Implicaciones éticas

Herson Esquivel Vargas

IC8071 Seguridad de software

TEC | Tecnológico de Costa Rica

Introduction

- Atributos que exacerban los problemas de seguridad en el software
  - Complejidad
  - Extensibilidad
  - Conectividad

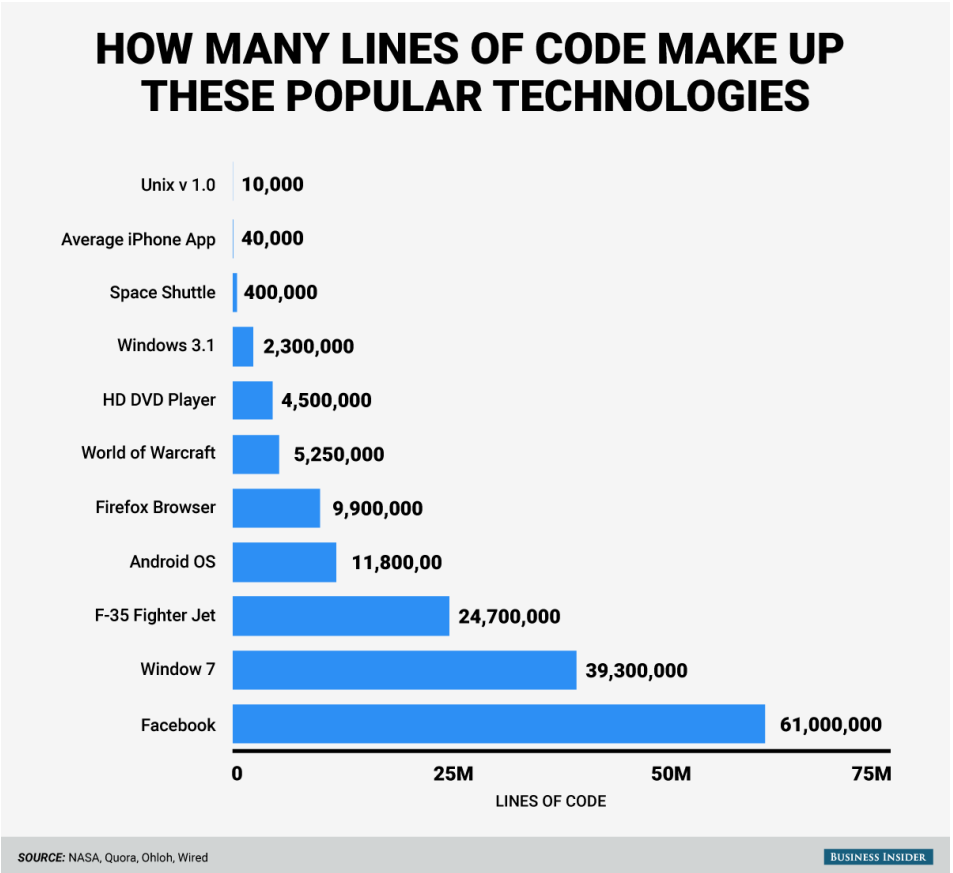
Fuente:
Exploiting software – How to break code? Greg Hoglund and Gary McGraw. Addison Wesley, 2004.

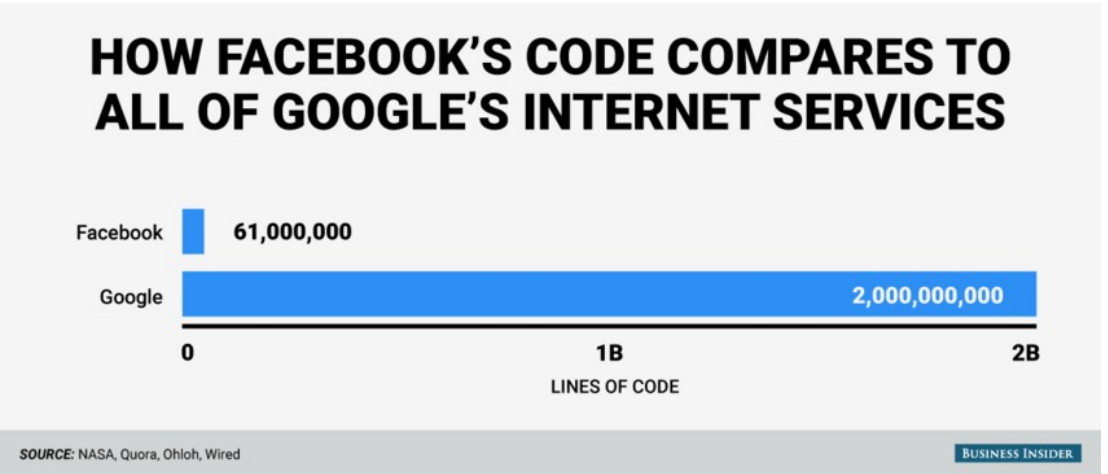
Complejidad, extensibilidad y conectividad

- Software
  - Se ejecuta en **compleja** infraestructura
    - SOs, navegadores, bibliotecas, APIs, µservicios, ...
  - Se escribe usando lenguajes **complejos**
    - SQL, C, C++, C#, Java, Python, JavaScript, HTML, …
    - Que requieren herramientas **complejas**
      - Compiladores, IDEs, preprocesadores, carga dinámica de código, …

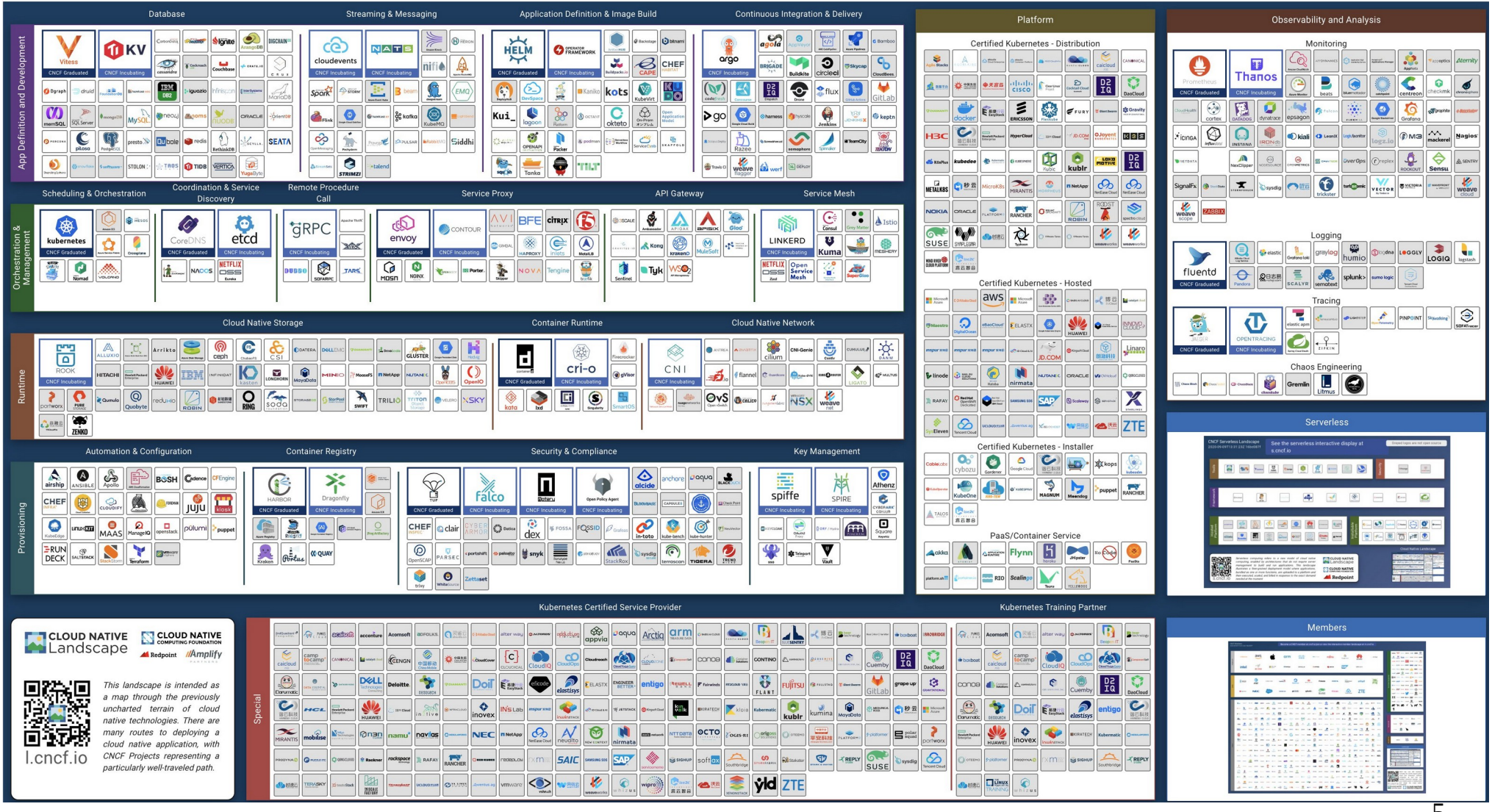
Estos pueden tener vulnerabilidades de seguridad o propiciar su inserción involuntaria

Complejidad, extensibilidad y conectividad





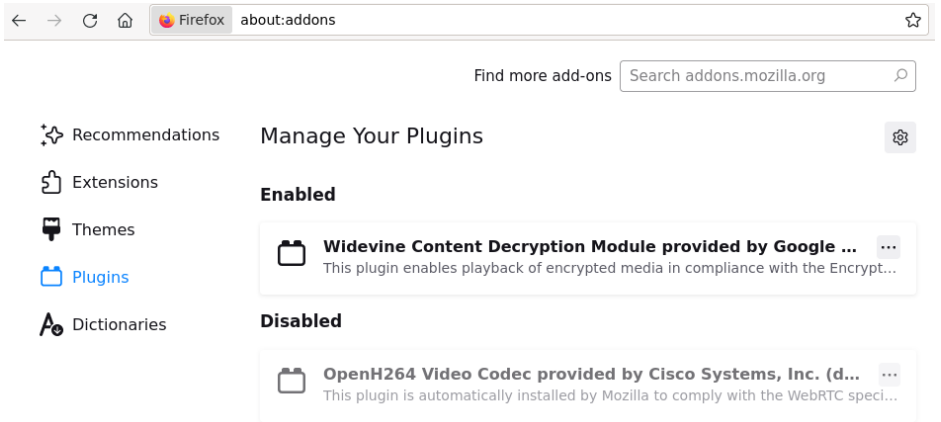
Fuente:
Google runs on 5000 times more code than the original space shuttle - https://www.weforum.org/agenda/2016/07/google-runs-on-5000-times-more-code-than-the-original-space-shuttle

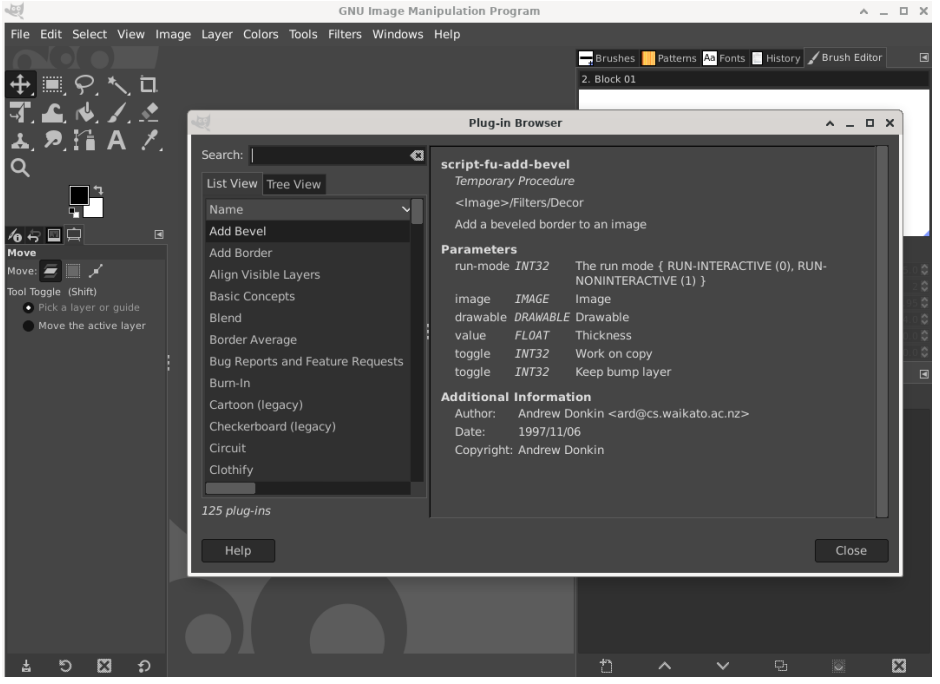

App Definition and Development
Database
Vitess
CNCF Graduated
KV
CNCF Incubating
Streaming & Messaging
cloudevents
CNCF Incubating
NATS
CNCF Incubating
Application Definition & Image Build
HELM
CNCF Graduated
OPERATOR FRAMEWORK
CNCF Incubating
Continuous Integration & Delivery
argo
CNCF Incubating
Orchestration & Management
Scheduling & Orchestration
kubernetes
CNCF Graduated
Coordination & Service Discovery
CoreDNS
CNCF Incubating
etcd
CNCF Incubating
Remote Procedure Call
gRPC
CNCF Incubating
Service Proxy
envoy
CNCF Graduated
CONTOUR
CNCF Incubating
API Gateway
Service Mesh
LINKERD
CNCF Incubating
Runtime
Cloud Native Storage
ROOK
CNCF Incubating
Container Runtime
containerd
CNCF Graduated
cri-o
CNCF Incubating
Cloud Native Network
CNI
CNCF Incubating
Provisioning
Automation & Configuration
Container Registry
HARBOR
CNCF Graduated
Dragonfly
CNCF Incubating
Security & Compliance
TUF
CNCF Graduated
falco
CNCF Incubating
Notary
CNCF Incubating
Open Policy Agent
CNCF Incubating
Key Management
spiffe
CNCF Incubating
SPIRE
CNCF Incubating
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Observability and Analysis
Monitoring
Prometheus
CNCF Graduated
Thanos
CNCF Incubating
Logging
fluentd
CNCF Graduated
Tracing
OPENTRACING
CNCF Incubating
Chaos Engineering
Serverless
Members
Kubernetes Certified Service Provider
Special
Kubernetes Training Partner
CLOUD NATIVE Landscape
CLOUD NATIVE COMPUTING FOUNDATION
Redpoint
Amplify
l.cncf.io
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

Complejidad, extensibilidad y conectividad

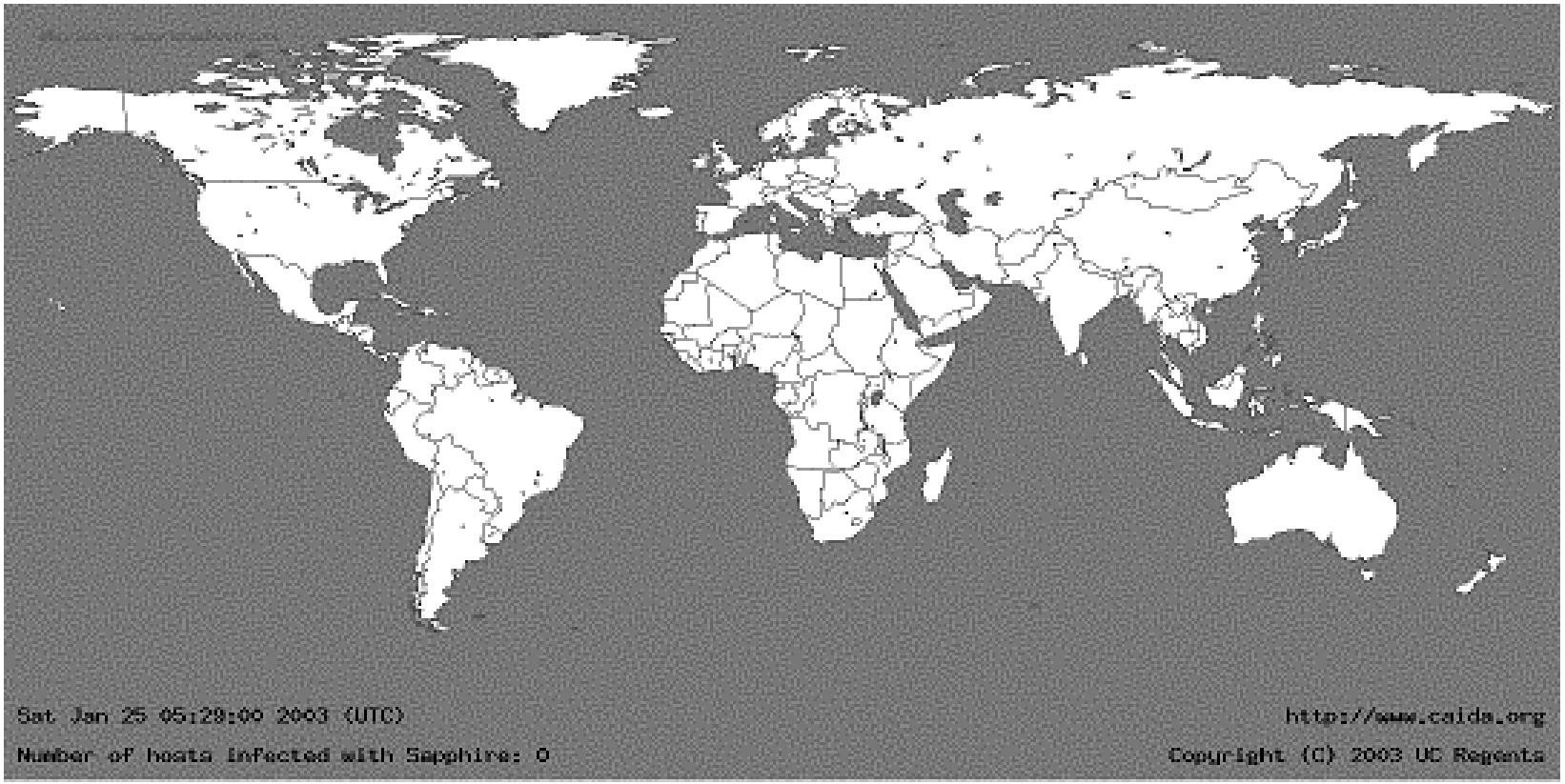
- Bibliotecas con código malicioso en repositorios “confiables”
  - PyPi
  - NPM
  - ...

Complejidad, extensibilidad y conectividad



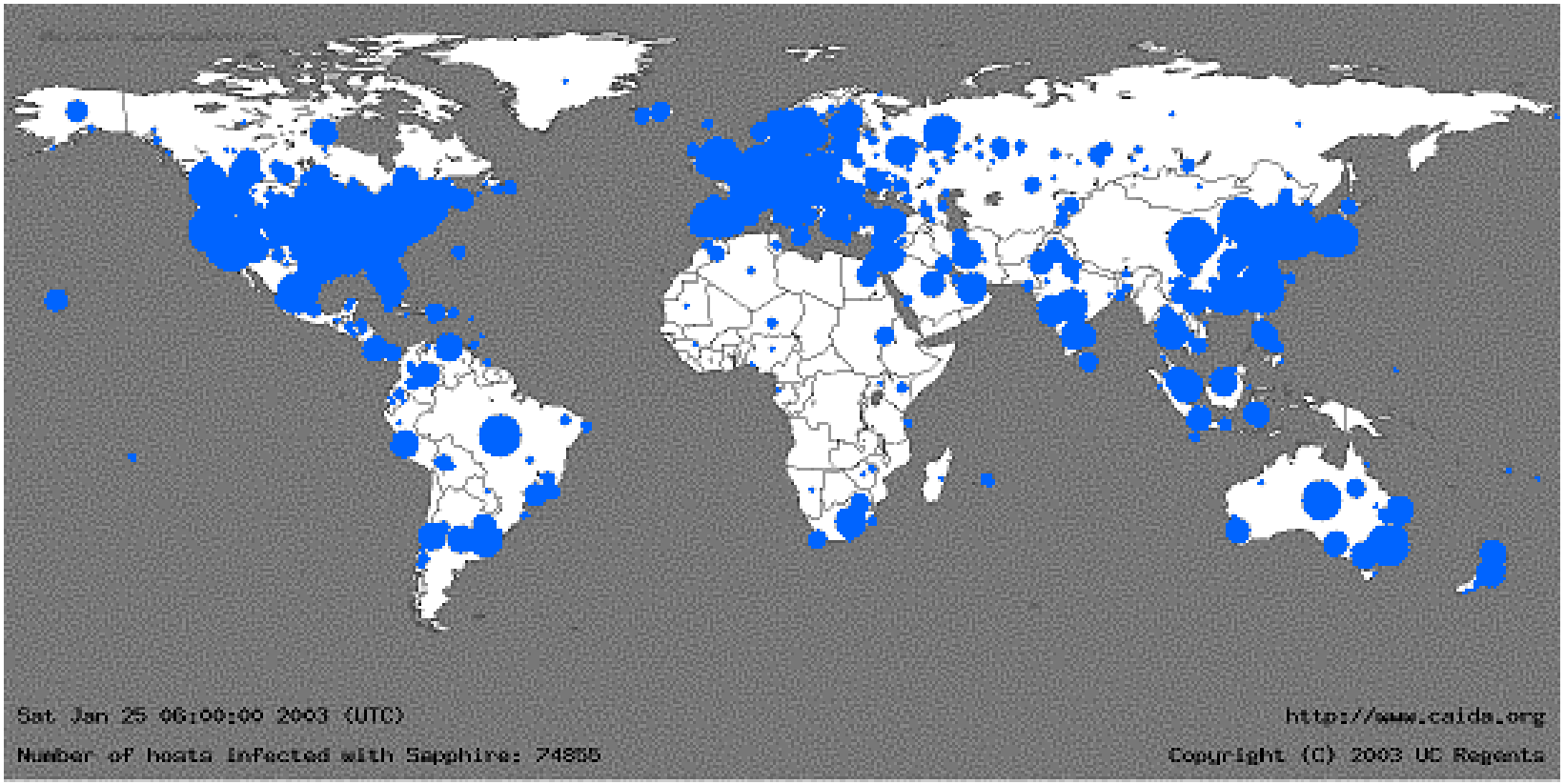


Complejidad, extensibilidad y conectividad



Fuente:
The Spread of the Sapphire/Slammer Worm - https://www.caida.org/catalog/papers/2003_sapphire/

Complejidad, extensibilidad y conectividad

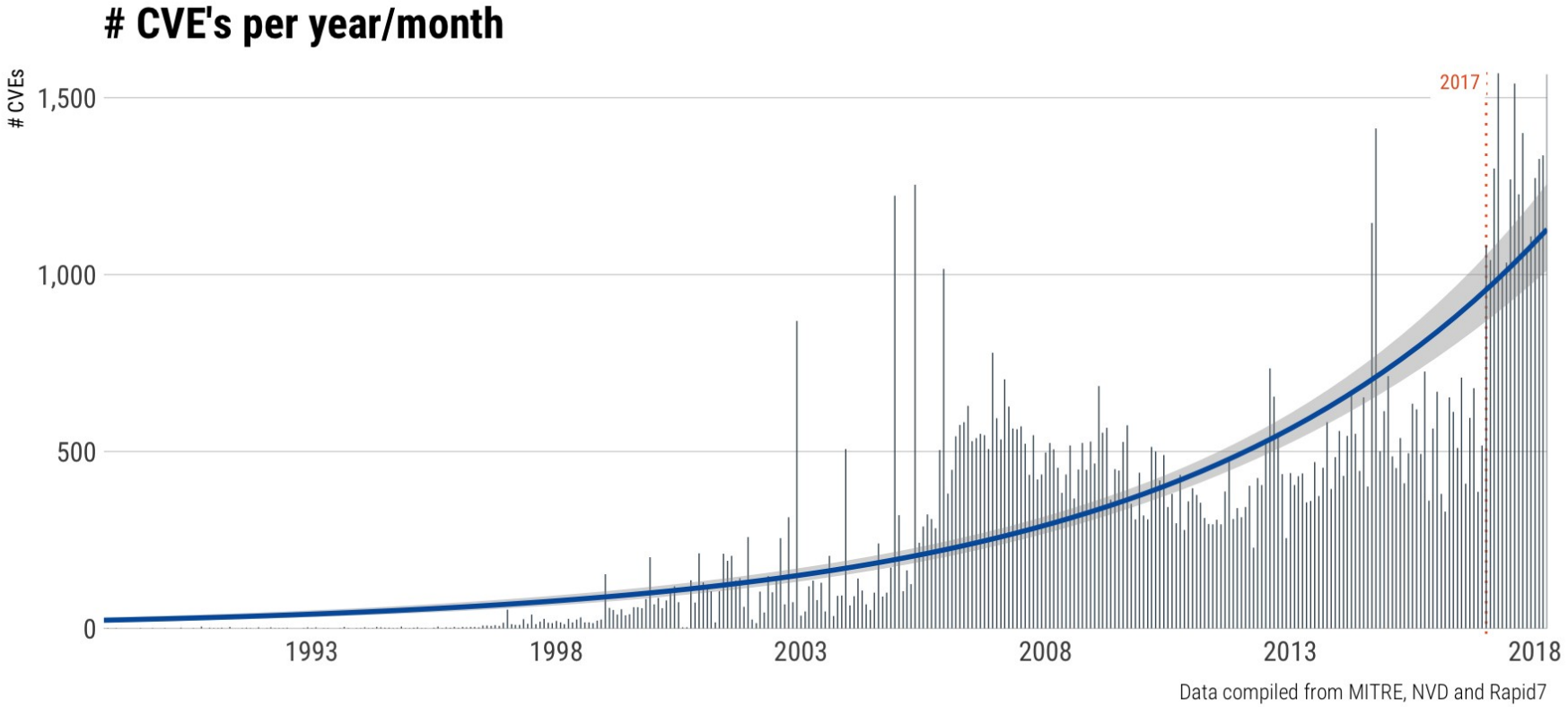


Fuente:
The Spread of the Sapphire/Slammer Worm - https://www.caida.org/catalog/papers/2003_sapphire/

Complejidad, extensibilidad y conectividad

- Control remoto de carros
  - https://www.youtube.com/watch?v=MK0SrxBC1xs
- IoT
- Sistemas de control industrial
- Edificios inteligentes
- ...

Complejidad, extensibilidad y conectividad



Fuente:
CVE 100K: By The Numbers - https://www.rapid7.com/blog/post/2018/04/30/cve-100k-by-the-numbers/

Implicaciones éticas de la seguridad del software


LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3: Analyst Note

April 18, 2022 TLP: White Report: 202204181300

Hive Ransomware

Executive Summary

Hive is an exceptionally aggressive, financially-motivated ransomware group known to maintain sophisticated capabilities who have historically targeted healthcare organizations frequently. HC3 recommends the Healthcare and Public Health (HPH) Sector be aware of their operations and apply appropriate cybersecurity principles and practices found in this document in defending their infrastructure and data against compromise.

Fuente:
Hive Ransomware - https://www.hhs.gov/sites/default/files/hive-ransomware-tlpwhite.pdf

Legislación Costarricense y otros referentes

- Artículo 217 bis.- Estafa informática
  - Se impondrá prisión de 3 a 9 años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información...
- Artículo 232.- Instalación o propagación de programas informáticos maliciosos

La pena será de 3 a 9 años de prisión cuando el programa informático malicioso:

  - i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.
  - ii) Afecte el funcionamiento de servicios públicos.
- ¡No hay excepción alguna para la divulgación responsable de vulnerabilidades!

Legislación Costarricense y otros referentes

- Coordinated vulnerability disclosure is a practice in which a hacker who finds a vulnerability in an IT-system reports that vulnerability to the system's owner
- The owner will then resolve the problem, after which the vulnerability can be disclosed publicly

Fuente:
Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure - https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-018-0090-8

Legislación Costarricense y otros referentes

- Bug bounty programs
- Hasta ransomeware gangs tienen bug bounty programs
  - LockBit

Legislación Costarricense y otros referentes

Fuente:
https://jacobriggs.io/blog/posts/i-hacked-the-dutch-government-and-all-i-got-was-this-t-shirt-24.html

Legislación Costarricense y otros referentes

- Nueva “Ley de ciberseguridad de Costa Rica”
  - Expediente N.º 23.292

ARTÍCULO 21- Divulgación responsable de vulnerabilidades

1- No se considerará que una persona, organización o institución pública, infringió disposiciones legales sobre la confidencialidad, integridad y disponibilidad de datos y sistemas de información o que incurrió en un incumplimiento de leyes, reglamentos, contratos y códigos de conducta profesionales, por el hecho de comunicar, publicar o divulgar vulnerabilidades, siempre, que demuestre su buena fe.

2- Con la finalidad de asegurar la buena fe de la persona u organización que divulgue una vulnerabilidad, se deberá tomar en cuenta que no se haya solicitado recompensas bajo coerción o amenaza de publicación de la información; que no se otorgue un tiempo límite para solucionar la vulnerabilidad antes de publicarla o divulgarla; que en el proceso de identificación, la persona u organización tomó las previsiones necesarias para prevenir vulneraciones a la privacidad, degradación o fallas en el servicio y destrucción o manipulación de la data; y que la persona u organización que divulga una vulnerabilidad consideró el impacto de dicha divulgación y tuvo el cuidado razonable para minimizar el daño que pueda causarse por tal divulgación.

3- Del proceso de identificación de vulnerabilidades basadas en la buena fe, quedan excluidos métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos.

Un resumen de problemas

- Falta de conciencia
- Falta de conocimiento
- Complejidad, extensibilidad y conectividad
- Funcionalidad > Seguridad

Lecturas opcionales

- Propuesta de Ley de ciberseguridad de Costa Rica

Lecturas obligatorias

- Exploiting software – How to break code? Greg Hoglund and Gary McGraw. Addison Wesley, 2004.
  - Páginas 33-40