

Ethical Hacking

Vulnerability Research

Federico Pacheco



@FedeQuark



www.federicopacheco.com.ar



info@federicopacheco.com.ar

Vulnerabilidad

Ausencia o debilidad de un control

Exploit

Software que explota una vulnerabilidad

Problemática actual

- Mercados
 - Negocios muy dependientes de los sistemas
 - Complejidad para gerenciar infraestructuras tecnológicas
 - Impacto directo en activos de la organización
 - Ambientes interconectados
- Tecnología
 - Penetración masiva de la tecnología
 - Infraestructura crítica informatizada
 - Aplicativos basados en la red
 - Privilegio de la funcionalidad y facilidad de uso
- Seguridad
 - Existencia de cibercrimen organizado
 - Dificultad de articular leyes globales
 - Disponibilidad de herramientas de explotación avanzadas



Vulnerability Research

- Proceso de descubrimiento de vulnerabilidades
 - Software
 - Dispositivos
 - Procesos
 - Entornos físicos
- Clasificación de vulnerabilidades
 - Explotabilidad
 - Impacto
- Permite determinar hacia dónde se moverá una industria

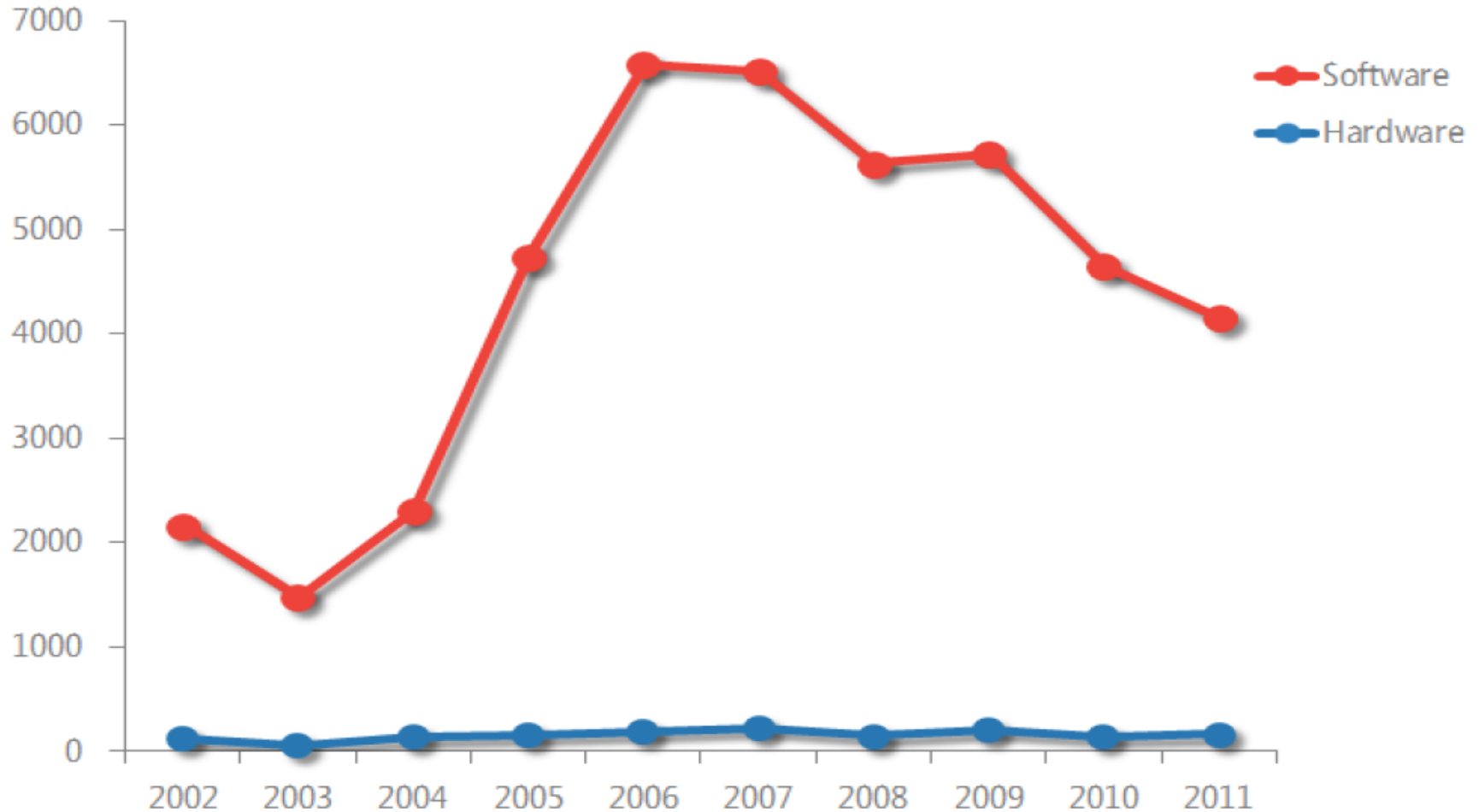


Vulnerability Researchers

- La actividad es realizada por profesionales o entusiastas de la seguridad
 - De forma particular o para empresas de software o de seguridad
- Motivación
 - Diversión
 - Curiosidad
 - Desafío
 - Aprendizaje
 - Dinero
 - Trabajo



Vulnerabilidades en software y hardware (2002-2011)



Fuente: Microsoft Security Intelligence Report

Tendencias

- Introducción de seguridad en procesos de desarrollo de software
- Fin de la gratuidad en el conocimiento de las vulnerabilidades
- Full Disclosure → Responsible Disclosure
- Ataques directos → Ataques Client Side
- Menos vulnerabilidades, pero más graves



Reporte de vulnerabilidades

- Es muy importante y beneficioso reportar vulnerabilidades
- Es posible que la misma vulnerabilidad se haya descubierto por distintas personas
- El reporte formal reduce la posibilidad de su uso en mercado negro



Información en un reporte

- Producto y versión afectada
- Tipo de problema (BoF, SQL Injection, XSS, etc.)
- Descripción detallada del software instalado en el sistema (parches, SPs, etc.)
- Pasos necesarios para reproducir el problema
- Configuración requerida para reproducir el problema
- Prueba de Concepto (PoC)
- Impacto alcanzado

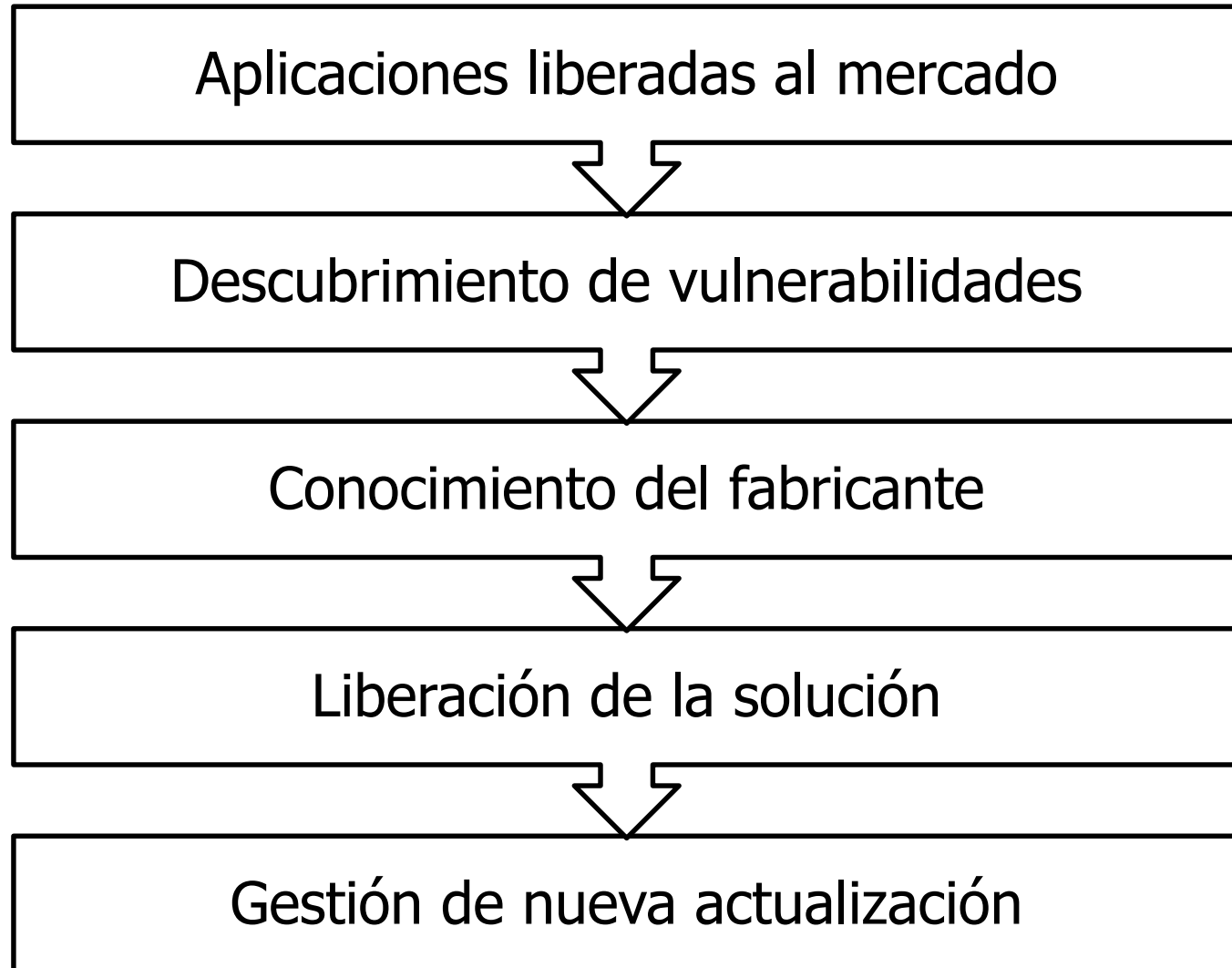


Vulnerabilidades en software propio

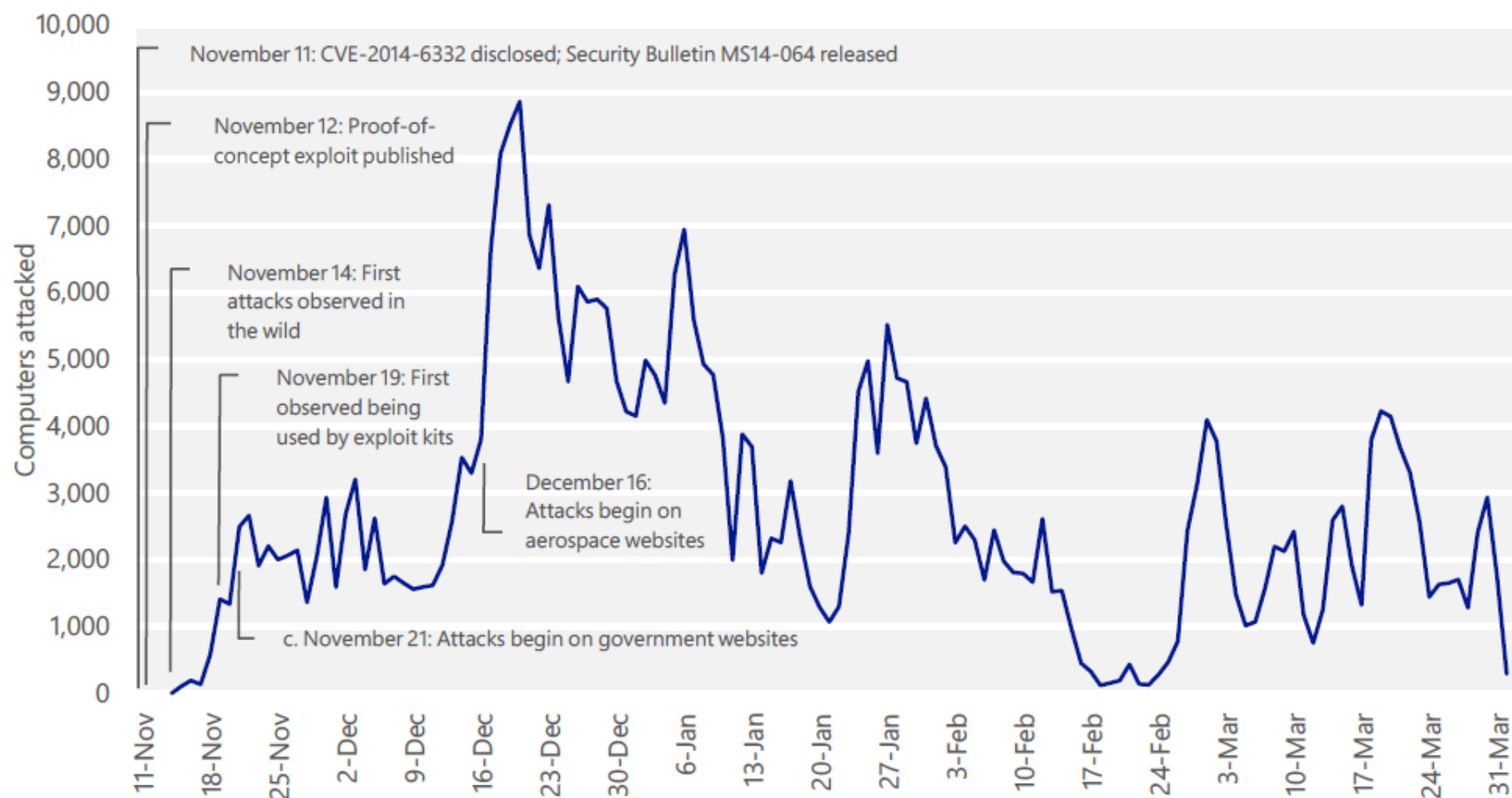
- Definir canales de contacto
- Definir procedimiento de respuesta ante reportes
- Determinar formas de mitigar el problema (workaround)
- Desarrollar y testear la corrección definitiva
- Publicar parches para los productos y versiones afectadas
- Buscar errores relacionados



Ciclo de vida de las vulnerabilidades

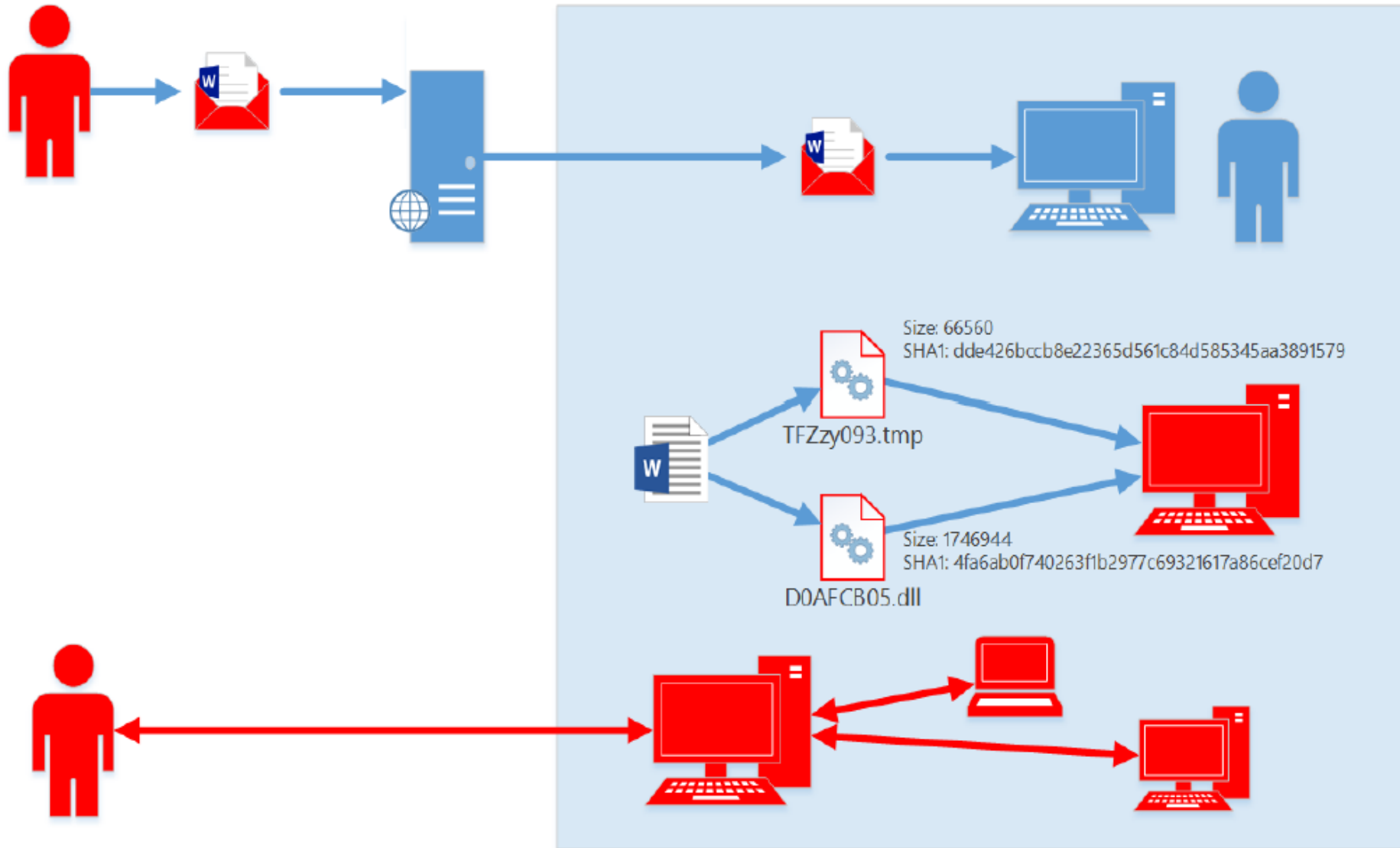


Ciclo de vida Vulnerabilidad CVE-2014-6332

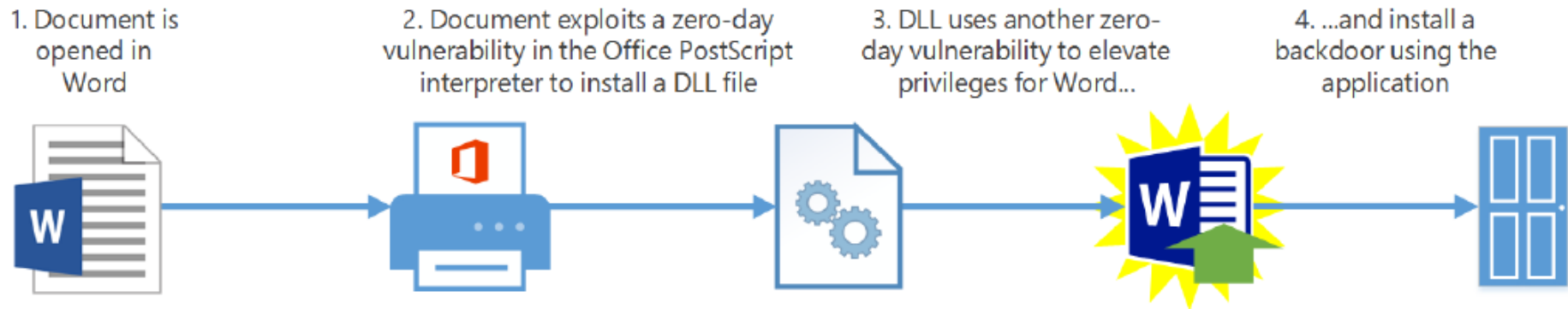


Fuente: Microsoft Security Intelligence Report

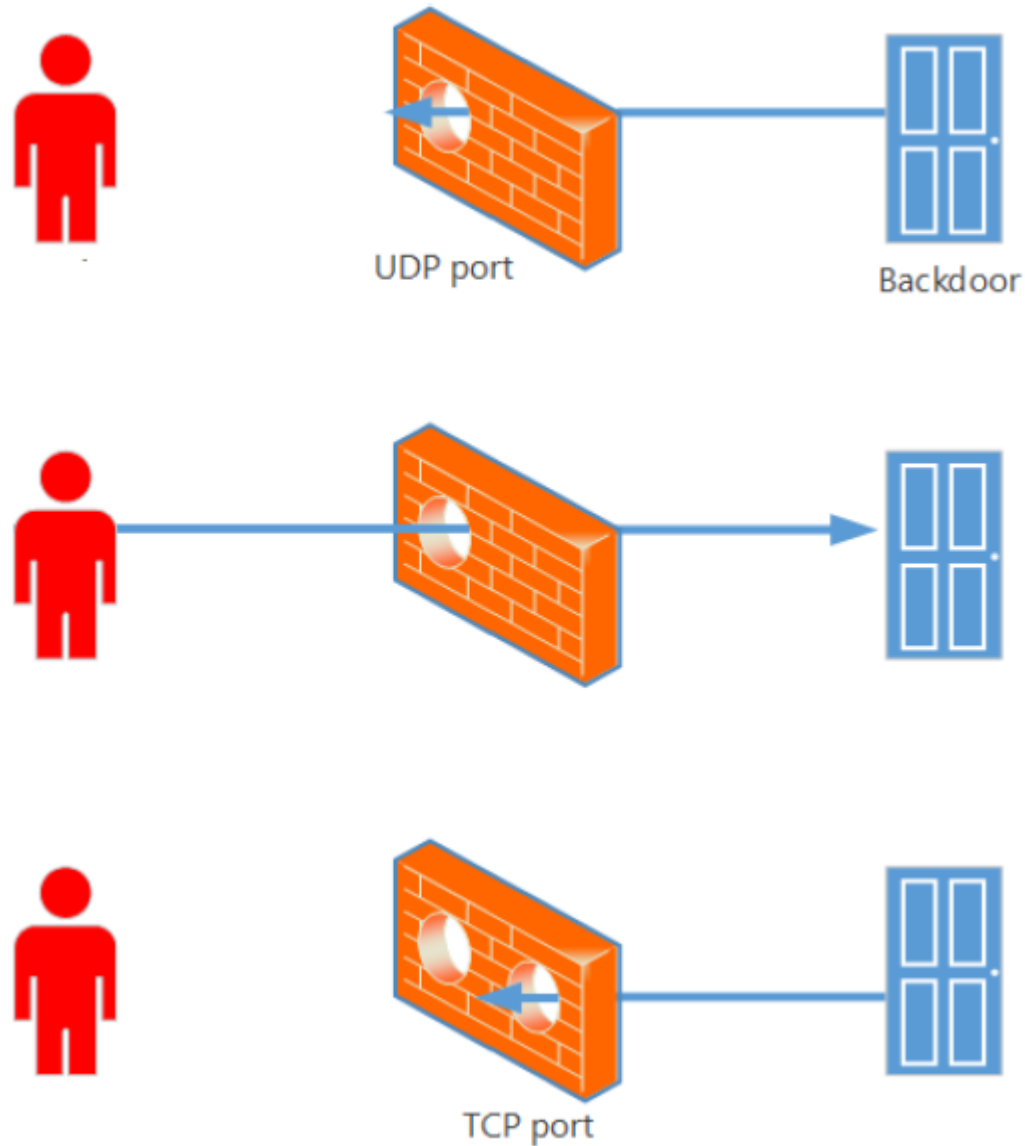
Esquema de ataque a red mediante vulnerabilidad



Ejemplo: Esquema de explotación con archivos



Conexión de equipo infectado hacia el exterior



Common Vulnerability Scoring System v3 (CVSS)

- Framework para scoring de vulnerabilidades del NIST
 - Ampliamente utilizado, aunque no del todo aceptado en entornos profesionales
- Estructura: 14 elementos divididos en 3 grupos de métricas
 - Métricas Base (obligatorias)
 - Métricas Temporales (no obligatorias)
 - Métricas Ambientales (no obligatorias)
- Características
 - Orientado a NO especialistas en seguridad (falta de profundidad)
 - Asume que la vulnerabilidad ya ha sido descubierta y verificada
 - No contabiliza información incompleta
 - Tiene una tendencia hacia el impacto en el sistema físico

Vulnerabilidades – Métricas base

- Explotabilidad
 - Vectores de acceso: Físico, local o remoto (externo o red adyacente)
 - Complejidad de acceso: Alta, baja
 - Privilegios requeridos: Ninguno, bajos, altos
 - Interacción con usuario: ninguna, requerida
- Alcance
 - Sin cambio
 - Con cambio
- Impacto (alto, bajo)
 - Confidencialidad
 - Integridad
 - Disponibilidad



Vulnerabilidades – Métricas temporales

Explotabilidad



☐ No comprobado

☐ Prueba de concepto (PoC)

☐ Exploit funcional

☐ Alta explotabilidad

Remediación



☐ Fix oficial

☐ Fix temporal

☐ Workaround

☐ No disponible

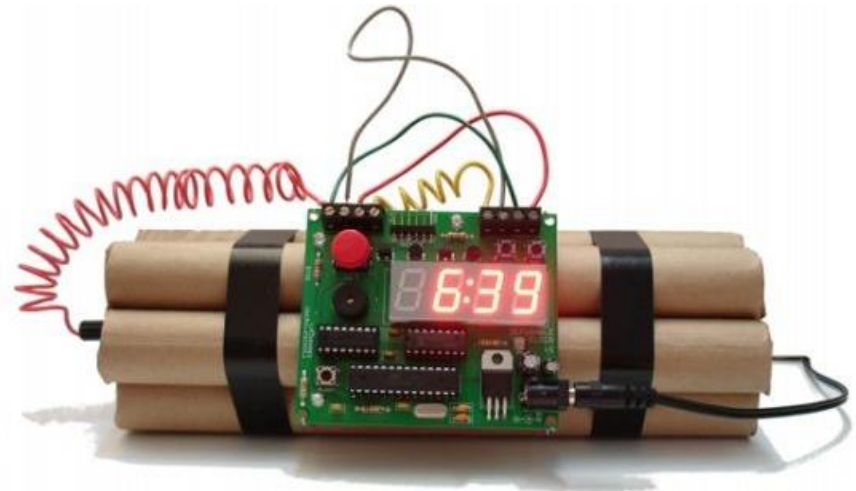
Confianza



☐ Desconocido

☐ Razonable

☐ Confirmado



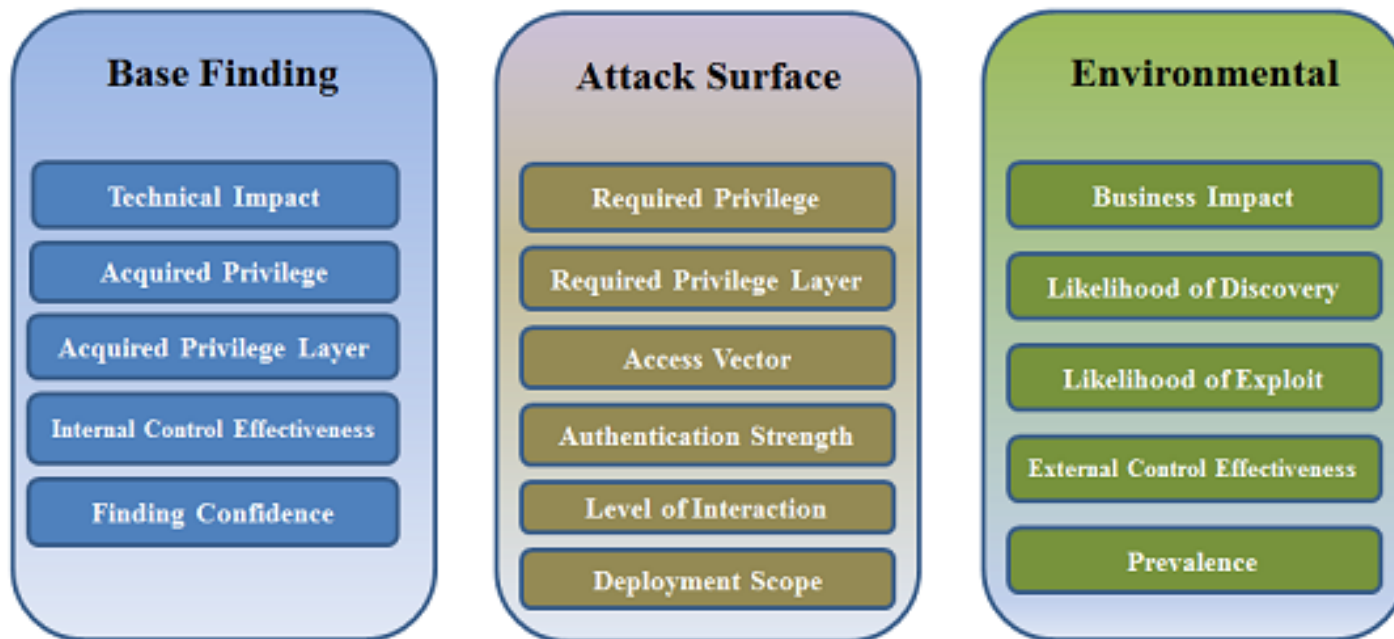
Vulnerabilidades – Métricas ambientales

- Idem métricas base
 - Modificadores base
 - Alcance
 - Impacto
- Agrega submétricas de impacto: Requerimientos de seguridad (bajo, medio, alto)
 - Requerimientos de Confidencialidad
 - Requerimientos de Integridad
 - Requerimientos de Disponibilidad



Common Weakness Scoring System (CWSS)

- Framework para scoring de vulnerabilidades de MITRE
- Consta de 3 grupos de métricas: Base, Superficie de ataque y Ambiente



[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

[About & Contact](#)

[Feedback](#)

[CVE Help](#)

[FAQ](#)

[Articles](#)

You can generate a custom RSS feed or an embedable vulnerability list widget or a json API call url.

Selected vulnerability types are OR'ed. If you don't select any criteria "all" CVE entries will be returned

☐ Vulnerabilities with exploits

☐ Cross Site Request Forgery

☐ Sql injection

☐ Memory corruption

☐ Gain information

☐ Code execution

☐ File inclusion

☐ Cross site scripting

☐ Http response splitting

☐ Denial of service

☐ Overflows

☐ Gain privilege

☐ Directory traversal

☐ Bypass something

Order By:

CVSS score >= :

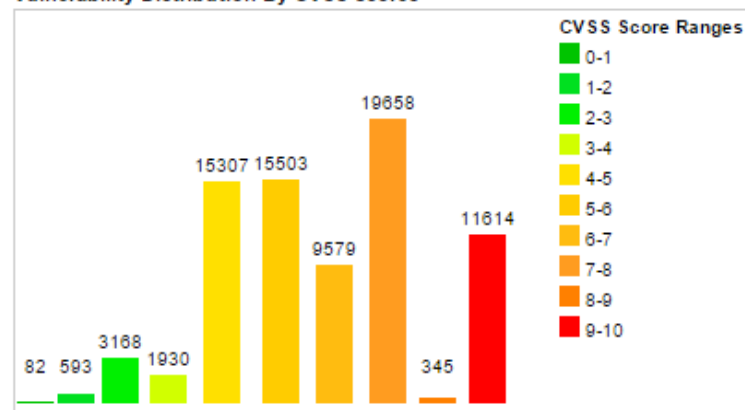
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	82	0.10
1-2	593	0.80
2-3	3168	4.10
3-4	1930	2.50
4-5	15307	19.70
5-6	15503	19.90
6-7	9579	12.30
7-8	19658	25.30
8-9	345	0.40
9-10	11614	14.90
Total	77779	

Weighted Average CVSS Score: 6.8

Vulnerability Distribution By CVSS Scores



CVSS Current Top 5 »

Top vulnerabilities with the highest CVSSv3 Temp Scores of the current month. The evaluation happens multiple times per day. (09/04/2016 - 10/04/2016)

- 9.5 Google Android libutils buffer overflow [CVE-2016-3861]
- 9.5 AVer EH6108H+ Hybrid DVR Telnet Service Default Credenti...
- 9.4 Revive Adserver Reflected privilege escalation
- 9.4 Google Android Mediaserver privilege escalation [CVE-2016-...
- 9.4 Siemens SIPROTEC/SIPROTEC Compact EN100 Ethernet M...

Exploit Price Current Top 5 »

Top vulnerabilities with the highest current exploit price of the current month. The evaluation happens multiple times per day. (09/04/2016 - 10/04/2016)

- \$25k-\$50k Cisco IOS/IOS XE Zone-Based Firewall spoofing privi...
- \$25k-\$50k Cisco IOS/IOS XE Cisco Application-Hosting Framewo...
- \$25k-\$50k Google Android Mediaserver privilege escalation [CVE...
- \$25k-\$50k Microsoft Windows win32k.sys privilege escalation [C...
- \$25k-\$50k Microsoft Windows win32k.sys privilege escalation [C...

Recent Entries »

Number 1 vulnerability database worldwide with more than 91000 entries available. Our specialists document the latest vulnerabilities on a daily basis since 1979. Besides technical details there are additional threat intelligence information like current risk levels and exploit price forecasts provided.

10/03/2016	MEDIUM	CVE-2016-8280	Huawei eSight directory traversal
10/03/2016	LOW	CVE-2016-8278	Huawei USG9520/USG9560/USG9580 URL Handler denial of service
10/03/2016	LOW	CVE-2016-8277	Huawei USG9520/USG9560/USG9580 Command Parameter Handler Restart denial of service
10/03/2016	MEDIUM	CVE-2016-8276	Huawei USG2100/USG2200/USG5100/USG5500 PPPoE buffer overflow
10/03/2016	LOW	CVE-2016-7572	Drupal Configuration Export Handler system temporary information disclosure

Día cero (Zero Day)

- Vulnerabilidad de día 0
- Exploit de día 0
 - Ventana de exposición



Exploit Database

[Home](#)[Exploits](#)[Shellcode](#)[Papers](#)[Google Hacking Database](#)[Submit](#)[Search](#)

Remote Code Execution Exploits


This exploit category includes exploits for remote services or applications, including client side exploits.

6,186 total entries


<< prev **1** 2 3 4 5 6 7 8 9 10 next >>

Date ▼	D	A	V	Title	Platform	Author
2015-07-21	↓	-	✓	SysAid Help Desk 'rdslogs' Arbitrary File Upload	java	metasploit
2015-07-21	↓	-	🕒	Internet Download Manager - OLE Automation Array Remote Code Execution	windows	Mohammad Reza .
2015-07-17	↓	-	✓	D-Link Cookie Command Execution	hardware	metasploit
2015-07-14	↓	-	🕒	Impero Education Pro - SYSTEM Remote Command Execution	windows	slipstream
2015-07-13	↓	-	✓	Accellion FTA getStatus verify_oauth_token Command Execution	hardware	metasploit
2015-07-13	↓	-	✓	VNC Keyboard Remote Code Execution	multiple	metasploit
2015-07-13	↓	-	✓	Adobe Flash opaqueBackground Use After Free	windows	metasploit
2015-07-13	↓	-	✓	Western Digital Arkeia Remote Code Execution	multiple	metasploit
2015-07-08	↓	-	✓	Adobe Flash Player ByteArray Use After Free	multiple	metasploit
2015-07-08	↓	-	✓	Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow	multiple	metasploit

NIST NVD



Sponsored by
DHS National Cyber Security Division/US-CERT



NIST
National Institute of
Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53 Controls	Product Dictionary	Impact Metrics	Data Feeds	Statistics
Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments

Common Vulnerability Scoring System Version 2 Calculator

This page provides a calculator for creating [CVSS](#) vulnerability severity scores. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score. A [concise](#) form of this page is available to CVSS experts.

[Update Scores](#)

[Reset Scores](#)

[View Equations](#)

CVSS Base Score	Undefined	Environmental Score Metrics This section addresses metrics that describe the effect of a vulnerability within an organization's environment. These metrics must be calculated separately for each organization.
Impact Subscore	Undefined	
Exploitability Subscore	Undefined	
CVSS Temporal Score	Undefined	General Modifiers Organization specific potential for loss (CollateralDamagePotential) Percentage of vulnerable systems (TargetDistribution)
CVSS Environmental Score	Undefined	
Overall CVSS Score	Undefined	


Base Score Metrics

These metrics describe inherent characteristics of the vulnerability.

Not Defined

Not Defined


Traducción oficial NVD al español



English [Iniciar sesión INCIBE](#)

Texto a buscar [Buscar](#)



CERTSI Protege tu empresa OSI ENISE Qué es INCIBE



[Buscador de vulnerabilidades](#)

Texto:

Fecha de publicación

Desde:  (dd/mm/aaaa) Hasta:  (dd/mm/aaaa)

Debe seleccionar un fabricante para cargar los productos

Fabricante: [Ayuda](#)


Producto: [Ayuda](#)




Gravedad: [Ayuda](#)

Tipo de Vulnerabilidad: [Ayuda](#)

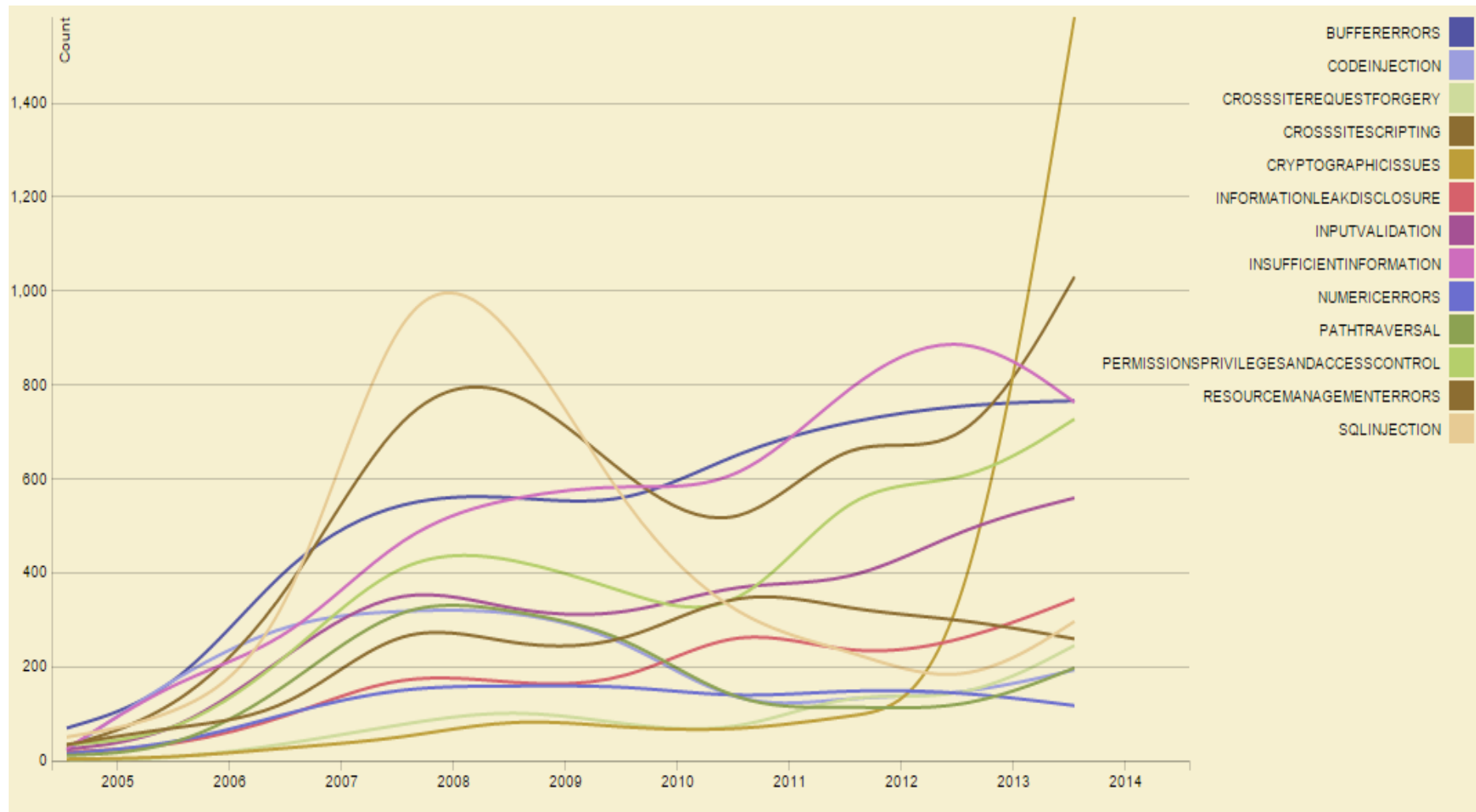
☐ Con enlace al parche:

Filas:

 **AVISOS** **AVISOS SCI**

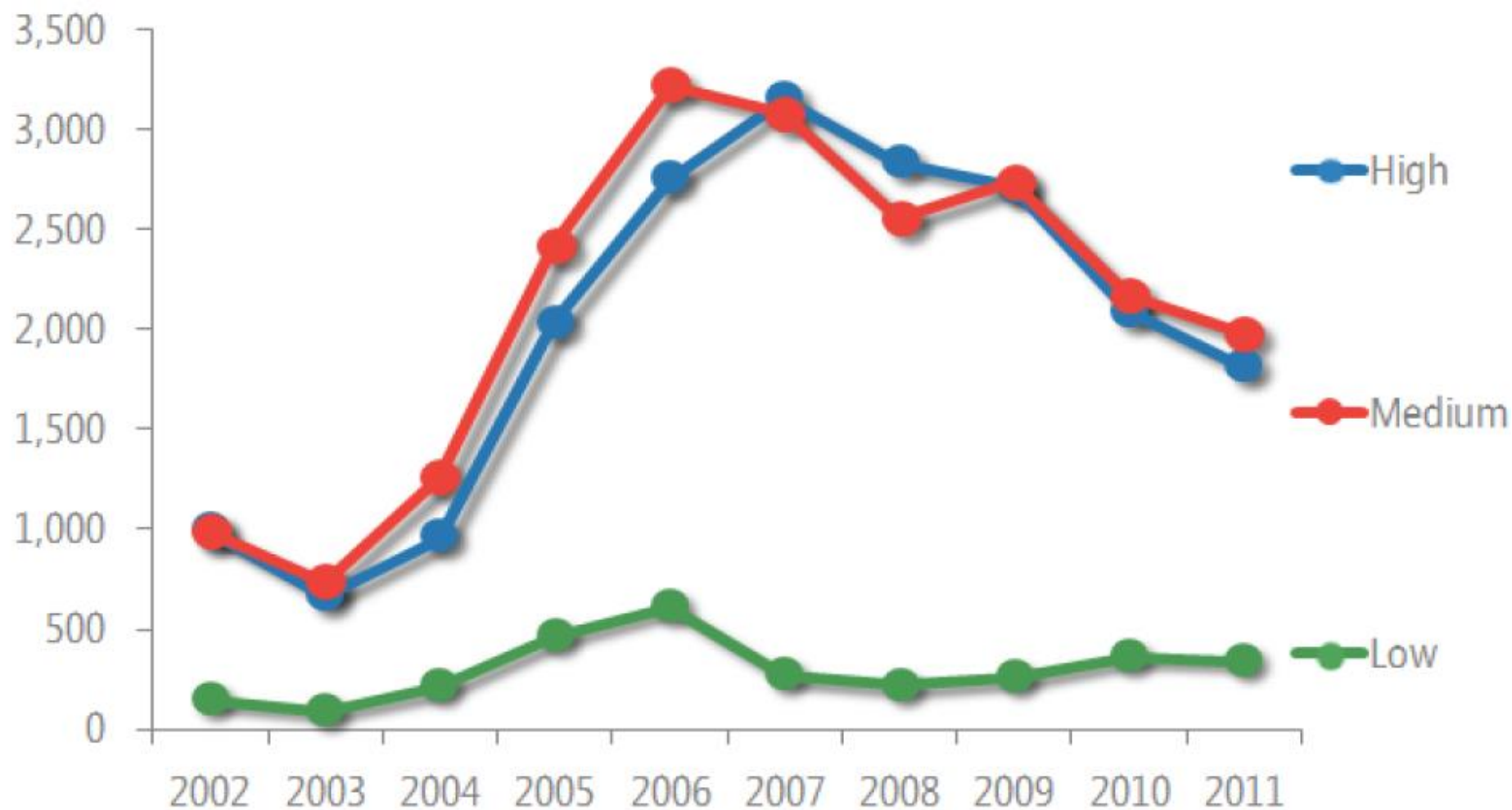
-  Elevación de privilegios en routers D-Link 27/04/2015
-  Varias vulnerabilidades en HP Storage Data Protector 22/04/2015
-  Actualización de seguridad 4.1.2 para

Cantidad de vulnerabilidades por categoría (NVD-NIST)



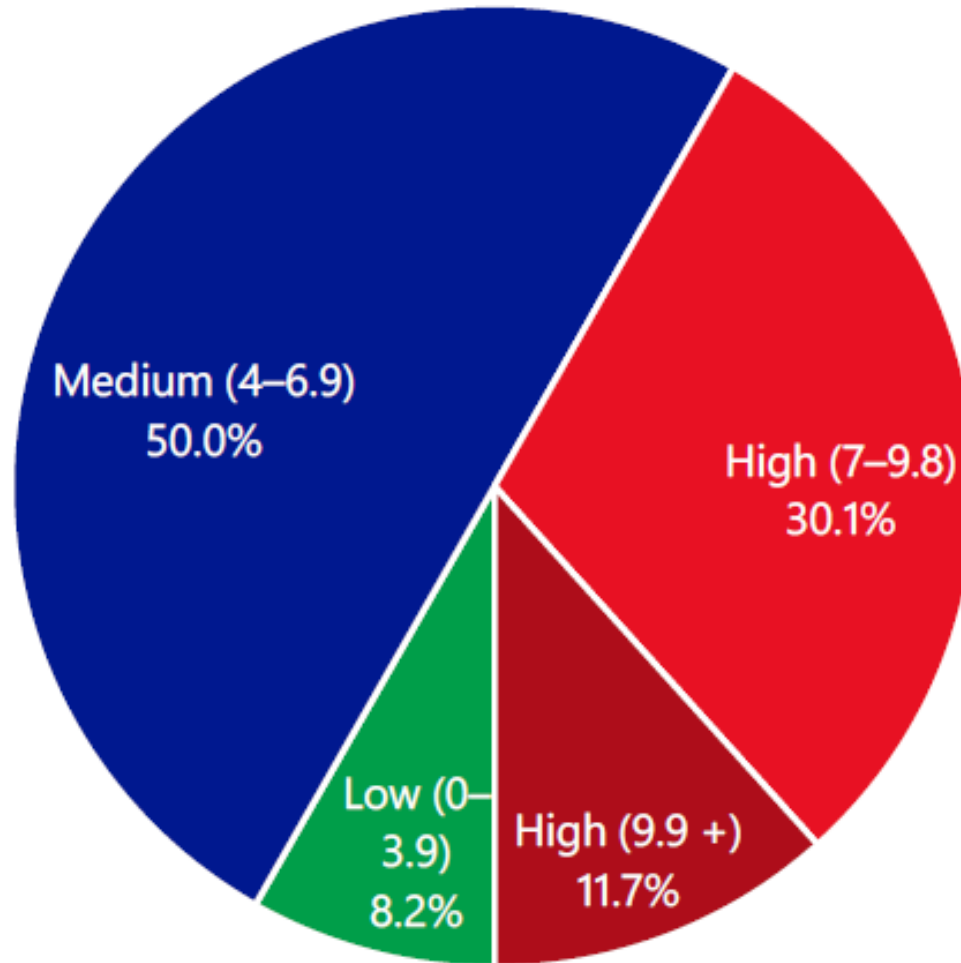
[illegible]

Vulnerabilidades por gravedad (2002-2011)



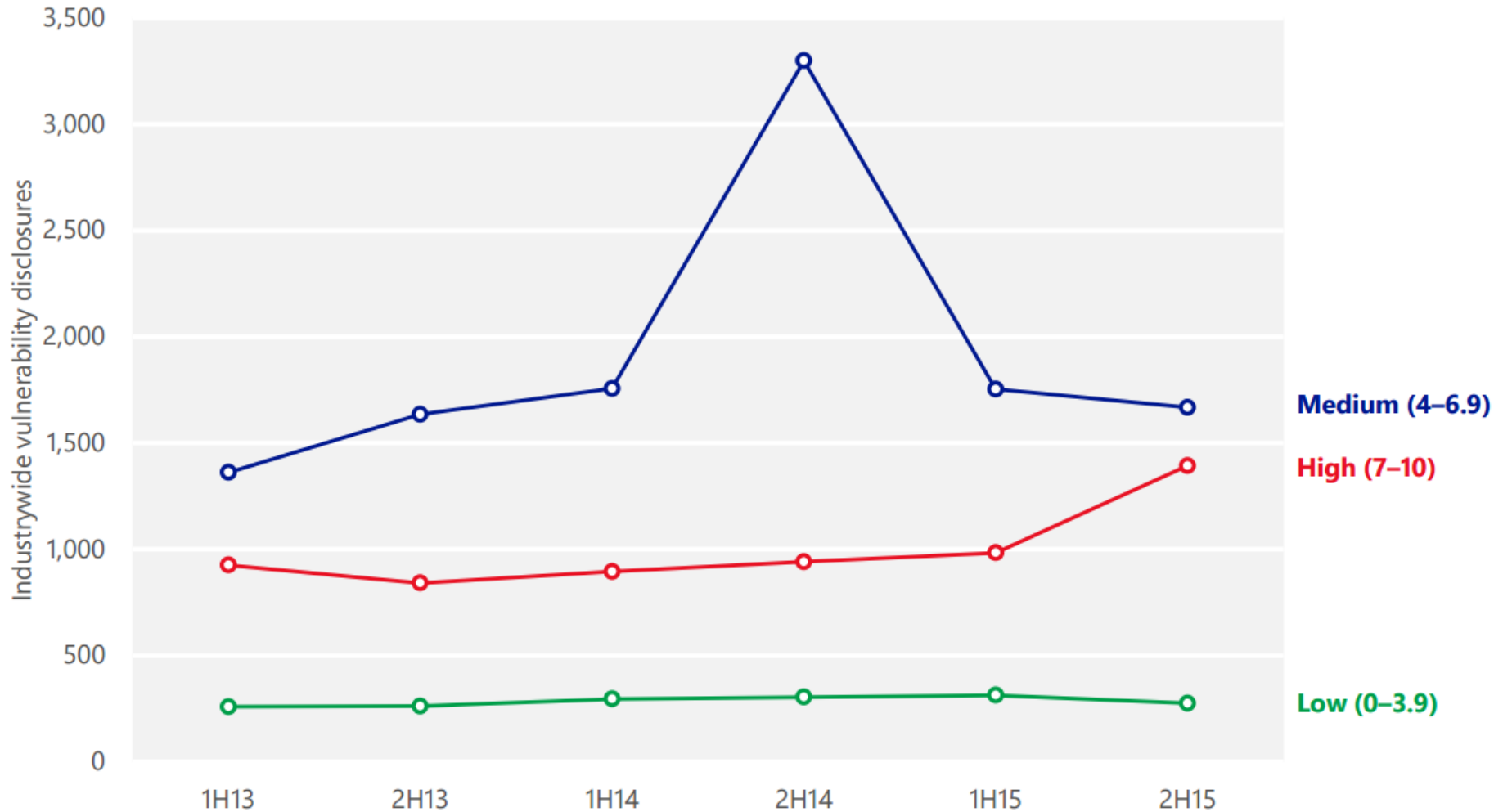
Fuente: Microsoft Security Intelligence Report

Gravedad de vulnerabilidades 2015 (CVSS)



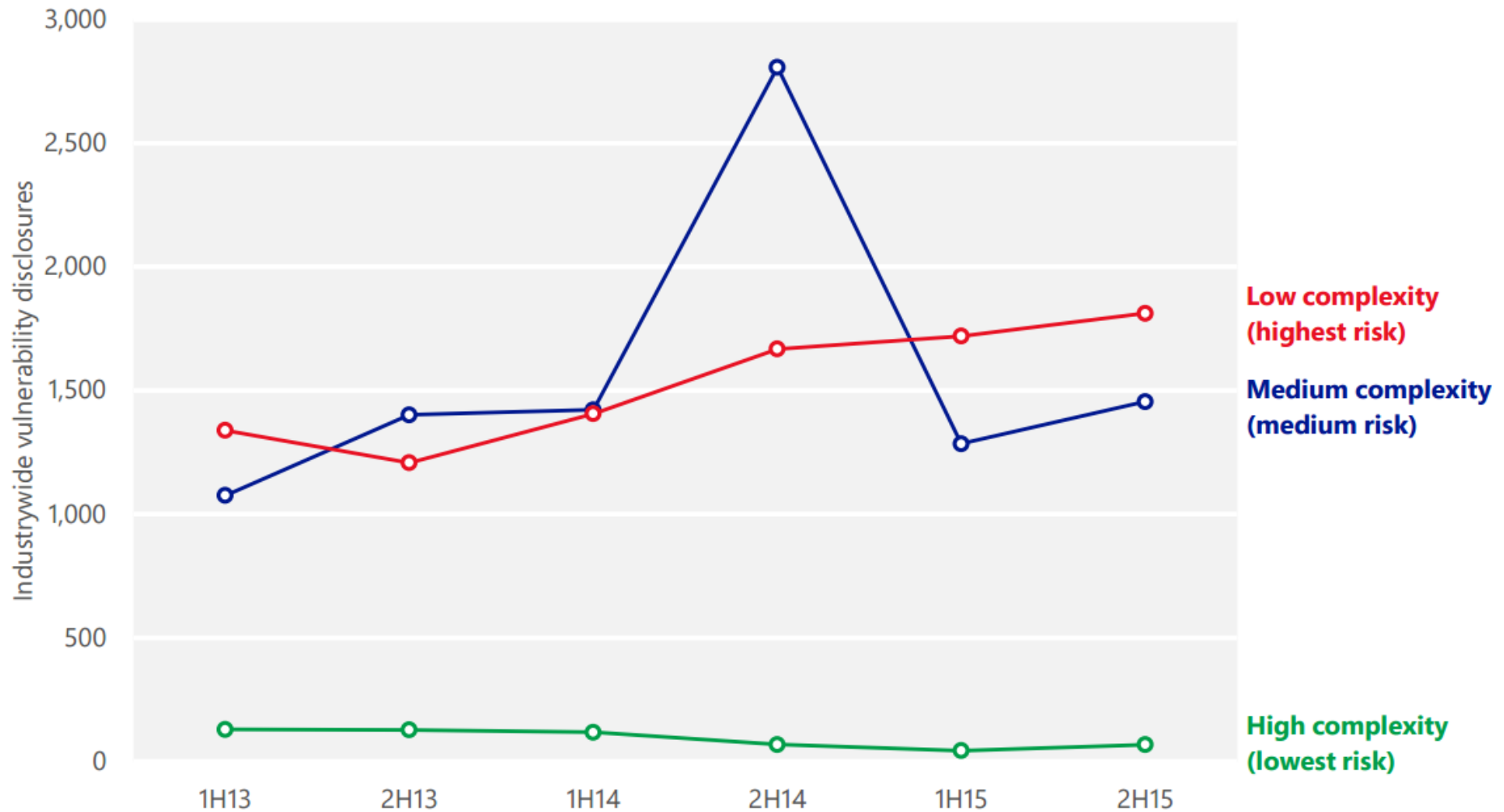
Fuente: Microsoft Security Intelligence Report

Gravedad de vulnerabilidades 2012-2015 (CVSS)



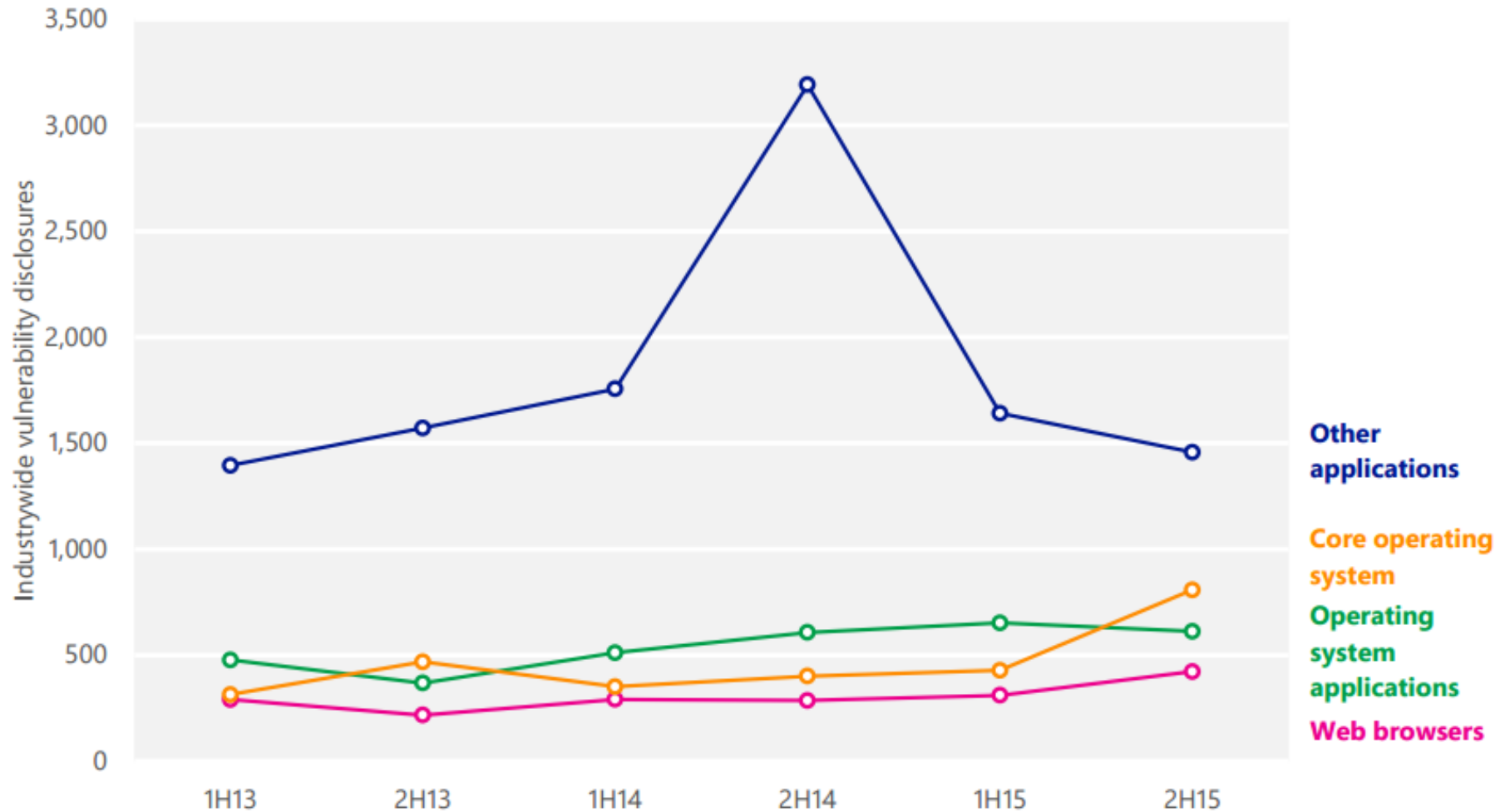
Fuente: Microsoft Security Intelligence Report

Cantidad por complejidad de explotación (2012-2015)



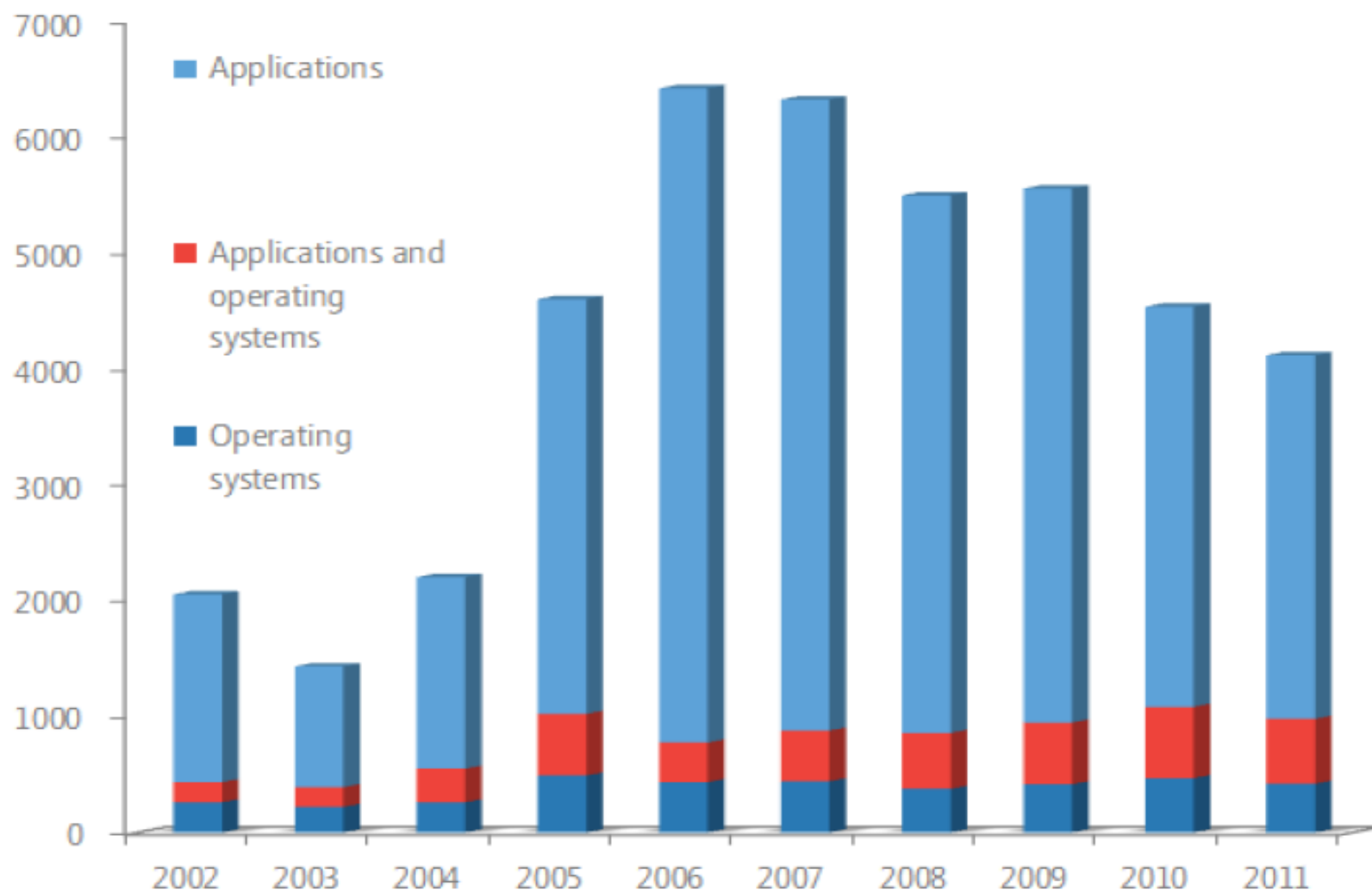
Fuente: Microsoft Security Intelligence Report

Cantidad por tipo de software (2012-2015)



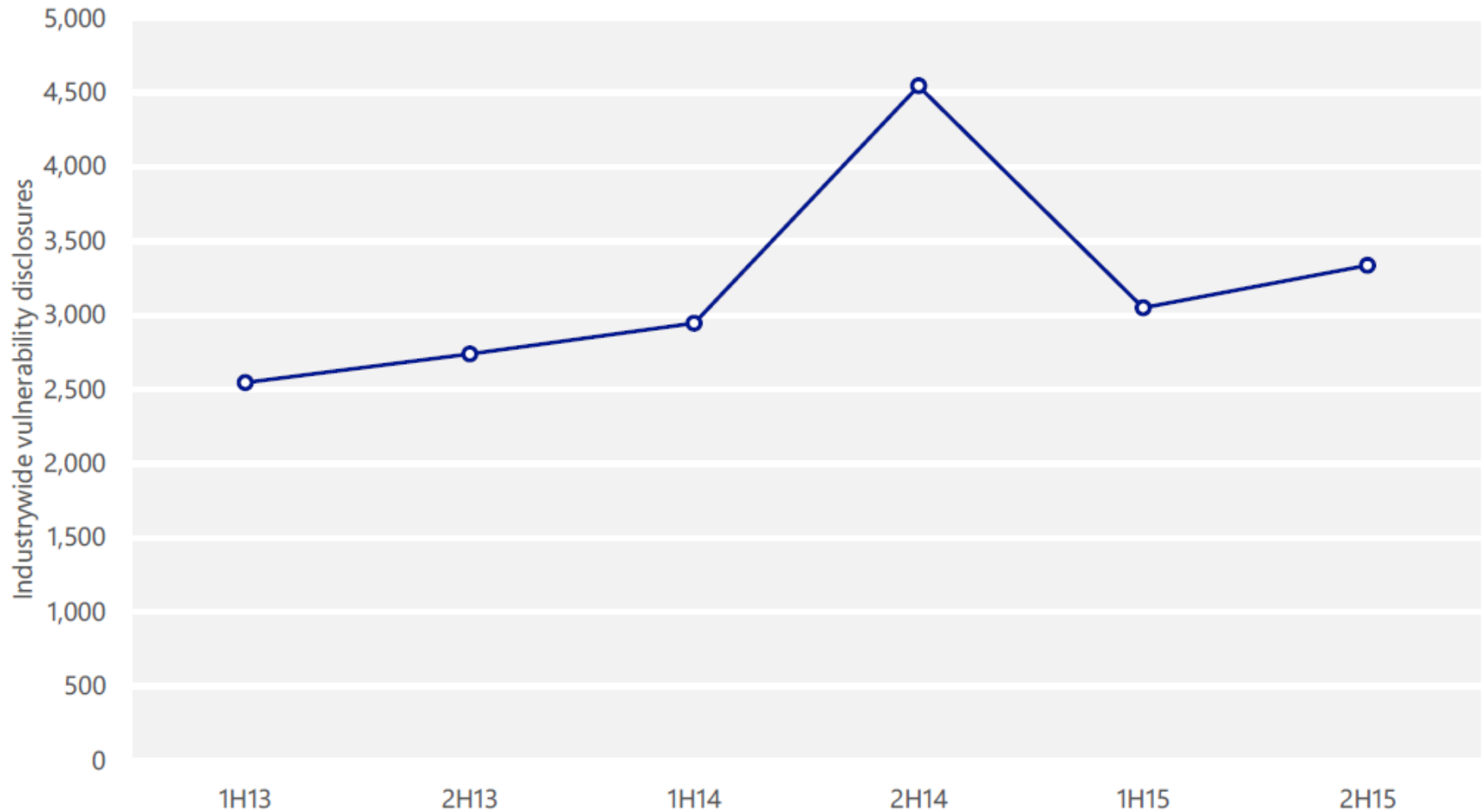
Fuente: Microsoft Security Intelligence Report

Cantidad por tipo de software (2002-2011)



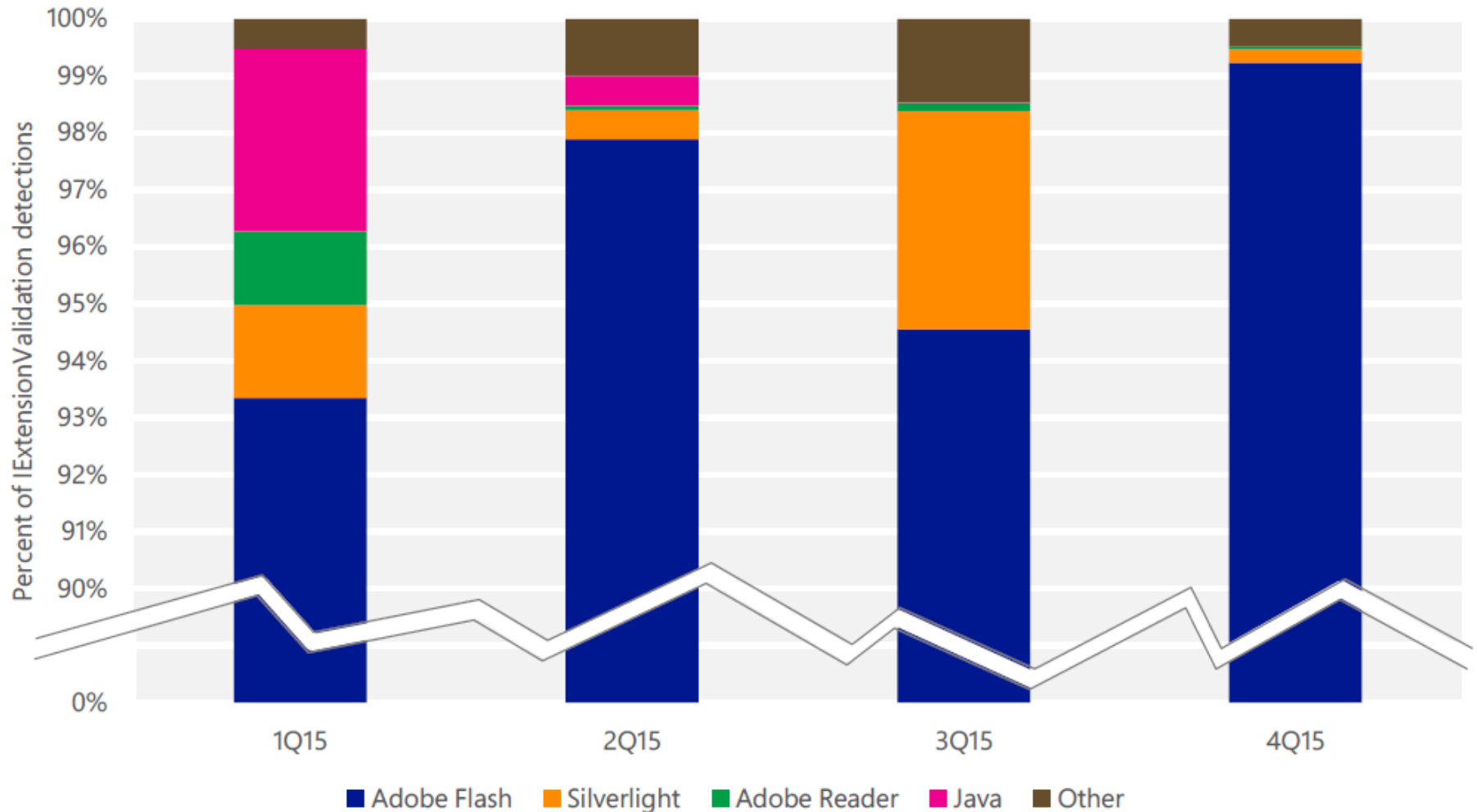
Fuente: Microsoft Security Intelligence Report

Cantidad total de vulnerabilidades (2012-2014)



Fuente: Microsoft Security Intelligence Report

Controles ActiveX maliciosos (2014-2015)

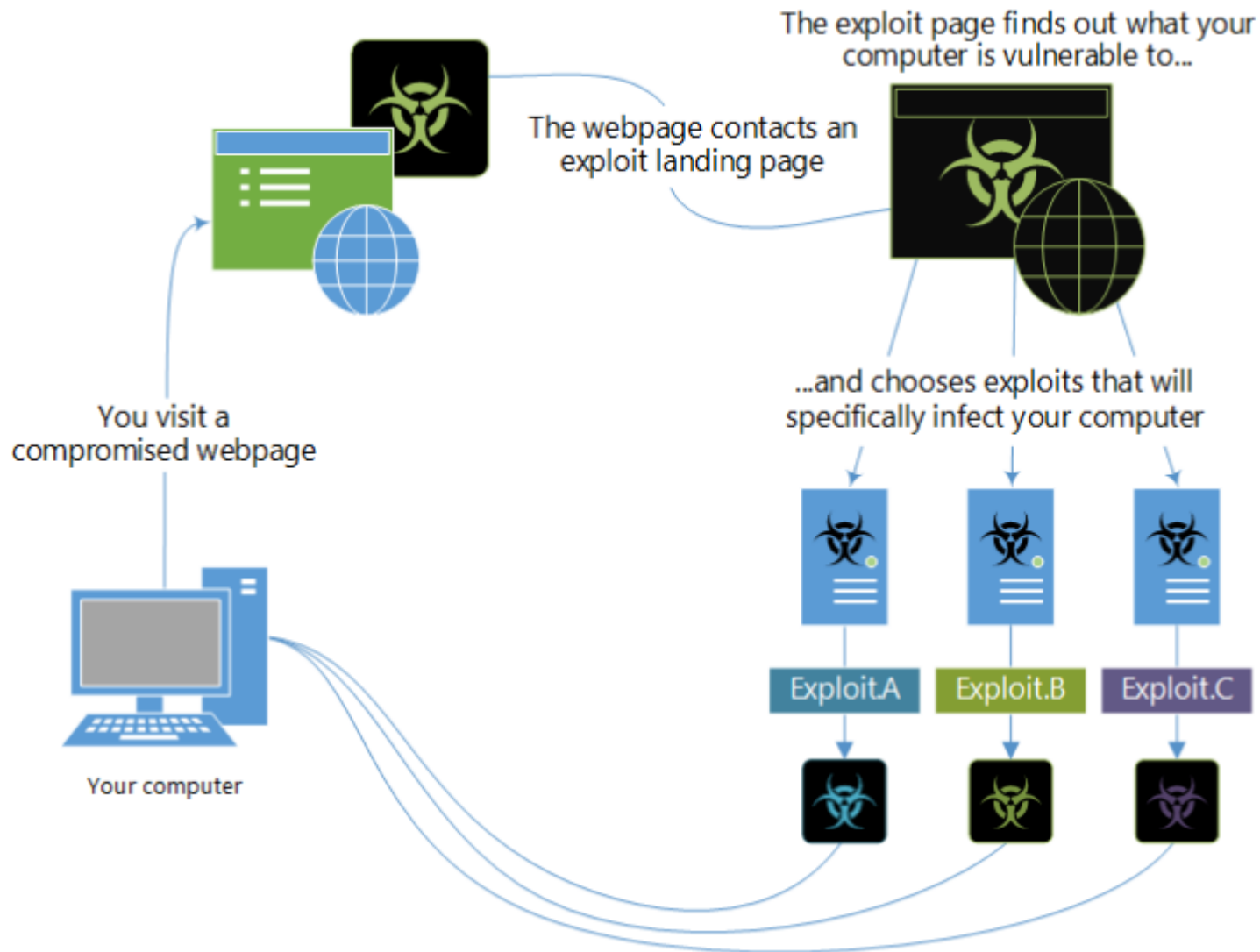


Fuente: Microsoft Security Intelligence Report

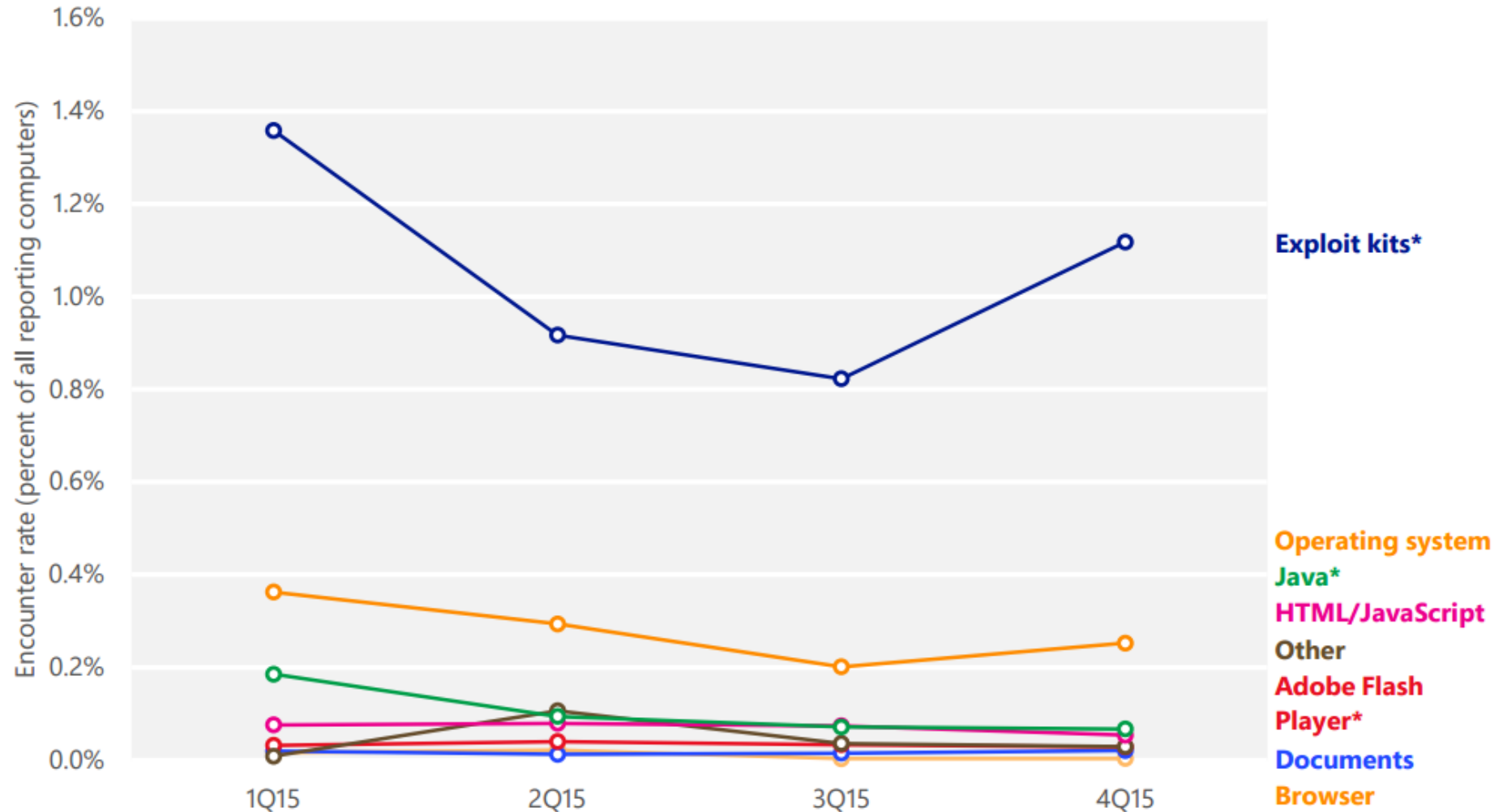
Exploit Kits (EK)

- Paquete de exploits para atacar clientes que navegan por un sitio
- Se basa en la identificación de vulnerabilidades en clientes
- Normalmente corren en un webserver
- Primer EK conocido: Mpack (2006)
- Se venden como software o como SaaS

Funcionamiento de Exploit Kits



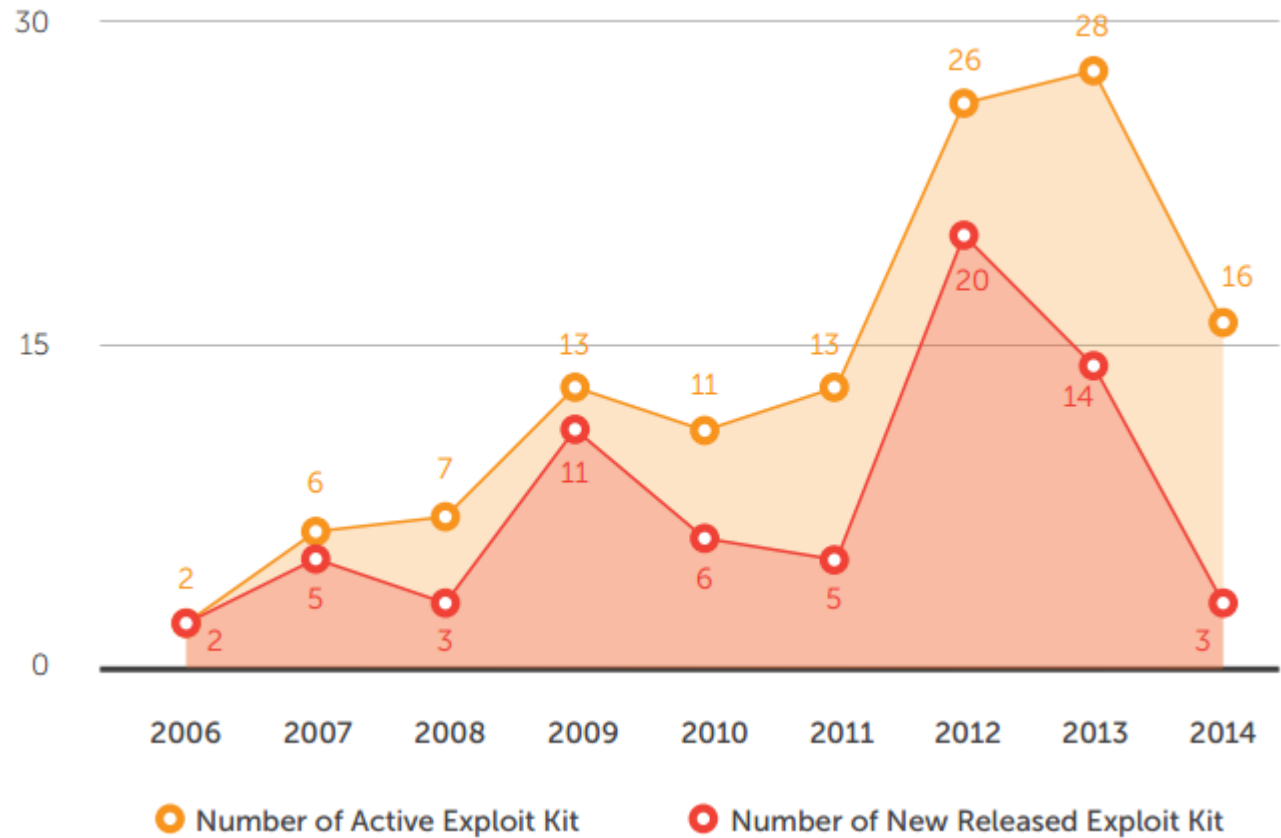
Exploits (2015)



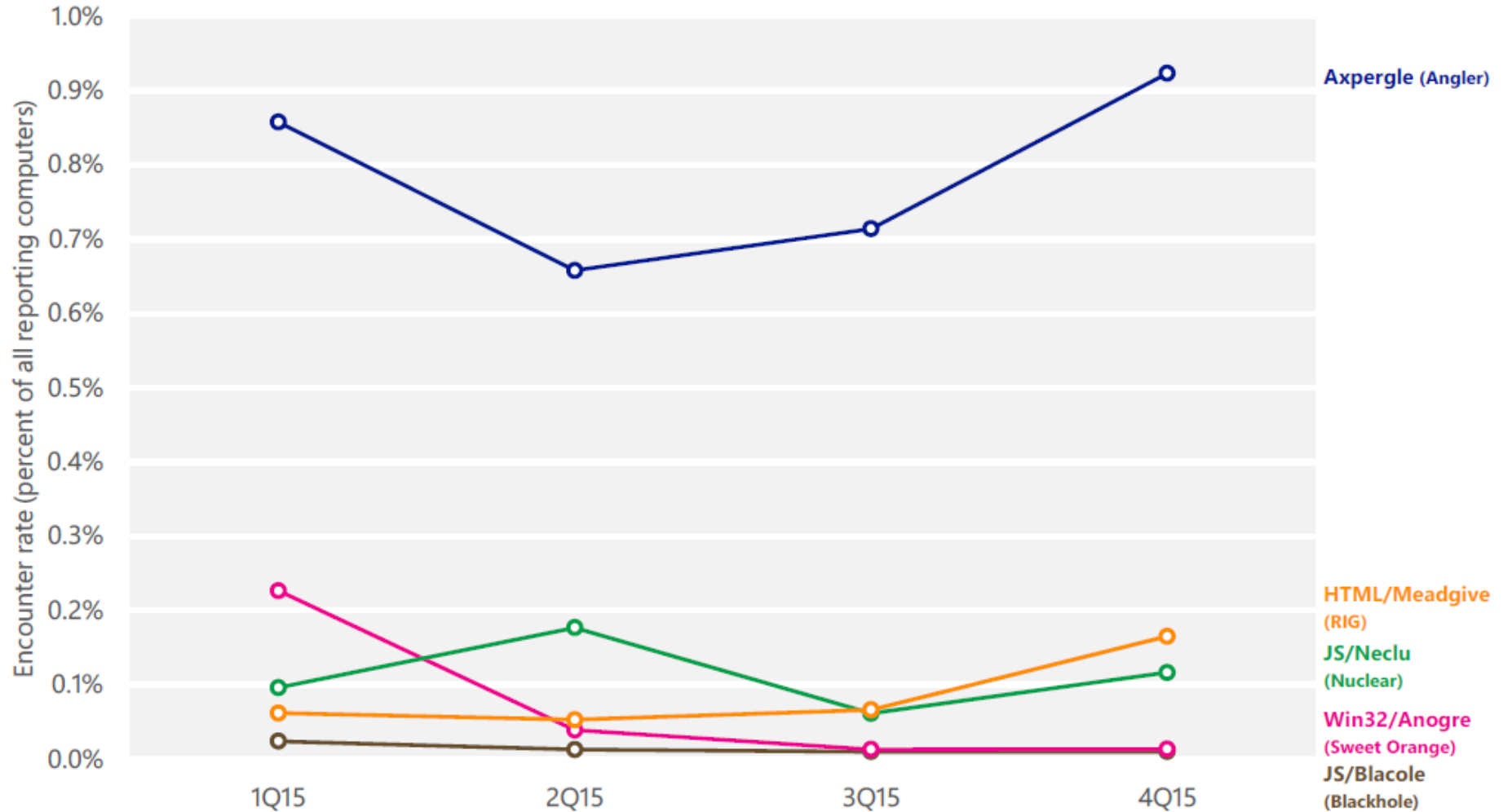
Fuente: Microsoft Security Intelligence Report

Exploit Kits (EK)

- Angler
- RIG
- Nuclear
- Sweet Orange
- Neutrino
- Magnitude
- Phoenix
- Crimepack
- Nuclearpack
- Blackhole



Exploit Kits (2015)



Fuente: Microsoft Security Intelligence Report

Mpack Exploit Kit

Server time/date snapshot: 9-Sep-2007 01:38:35
192.168.75.100 (Unknown country)



MPack v0.94 stats

Attacked hosts (total - uniq)	
IE XP ALL	18 - 4
QuickTime	0 - 0
Win2000	4 - 1
Firefox	1 - 1
Opera7	1 - 1

Traffic (total - uniq)	
Total traff	24 - 7
Exploited	2 - 2
Loads count	6 - 3
Loader's response	300% - 150%
Efficiency 25% - 42.86%	

Browser stats (total)	
MSIE	22 91.7%
Opera7	1 4.2%
Firefox	1 4.2%

Modules state	
Statistic type	Textfile-based
User blocking	OFF
Country blocking	OFF

Country	Traff	Loads	Efficiency
 US - United states	23 95.8%	5 83.3%	21.74%
 RU - Russian federation	1 4.2%	1 16.7%	100%

Referer stats (>3)	
http://www.mymalicious.page/index.php	19 79.2%
http://www.myothermalicious.page/index.php	4 16.7%

Phoenix Exploit Kit



Phoenix Exploit's Kit 3.0 full

△CONCORDIA, INTEGRITAS, INDUSTRIA...

Simple browser statistics

Browser	Visits	Exploited	Percent
MSIE	28866	13220	45.8%
Firefox	5536	1260	22.76%
Other	2020	158	7.82%
Opera	178	15	8.43%

Main Statistics

Unique Visits	Exploited	Percent
36600	14653	40.04%

Exploit statistics

Exploit	Exploited	Percent
JAVA TC	1785	4.88%
JAVA SMB	5195	14.19%
JAVA RHINO	4120	11.26%
PDF COLLAB	596	1.63%
PDF PRINTF	32	0.09%
JAVA RMI	251	0.69%
PDF LIBTIFF	304	0.83%
IE CSS	10	0.03%
IEPEERS	125	0.34%
JAVA TRUST	1196	3.27%
HACKING ATTEMPT	51	0.14%
MDAC	913	2.49%
HACKING ATTEMPT	46	0.13%
FLASH 10	29	0.08%

Menu

- [Simple statistics](#)
- [Advanced statistics](#)
- [Countries statistics](#)
- [Referers statistics](#)
- [Sources statistics](#)
- [Clear statistics](#)
- [Upload .exe](#)
- [Exit](#)

Crimepack Exploit Kit



crimepack

MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • iFRAME • CLEAR STATS • SETTINGS • LOGOUT

overall stats

unique hits	loads	exploit rate
16971	3500	21%




exploit stats

iepeers	msiemc	pdf	libtiff	mdac	java	webstart	activex	other	aggressive
170	62	487	29	364	0	2339	0	49	0

os stats

os	hits	loads	rate
windows 2k	51	5	10%
windows 2k3	29	3	10%
windows xp	13312	2868	22%
windows vista	3535	591	17%

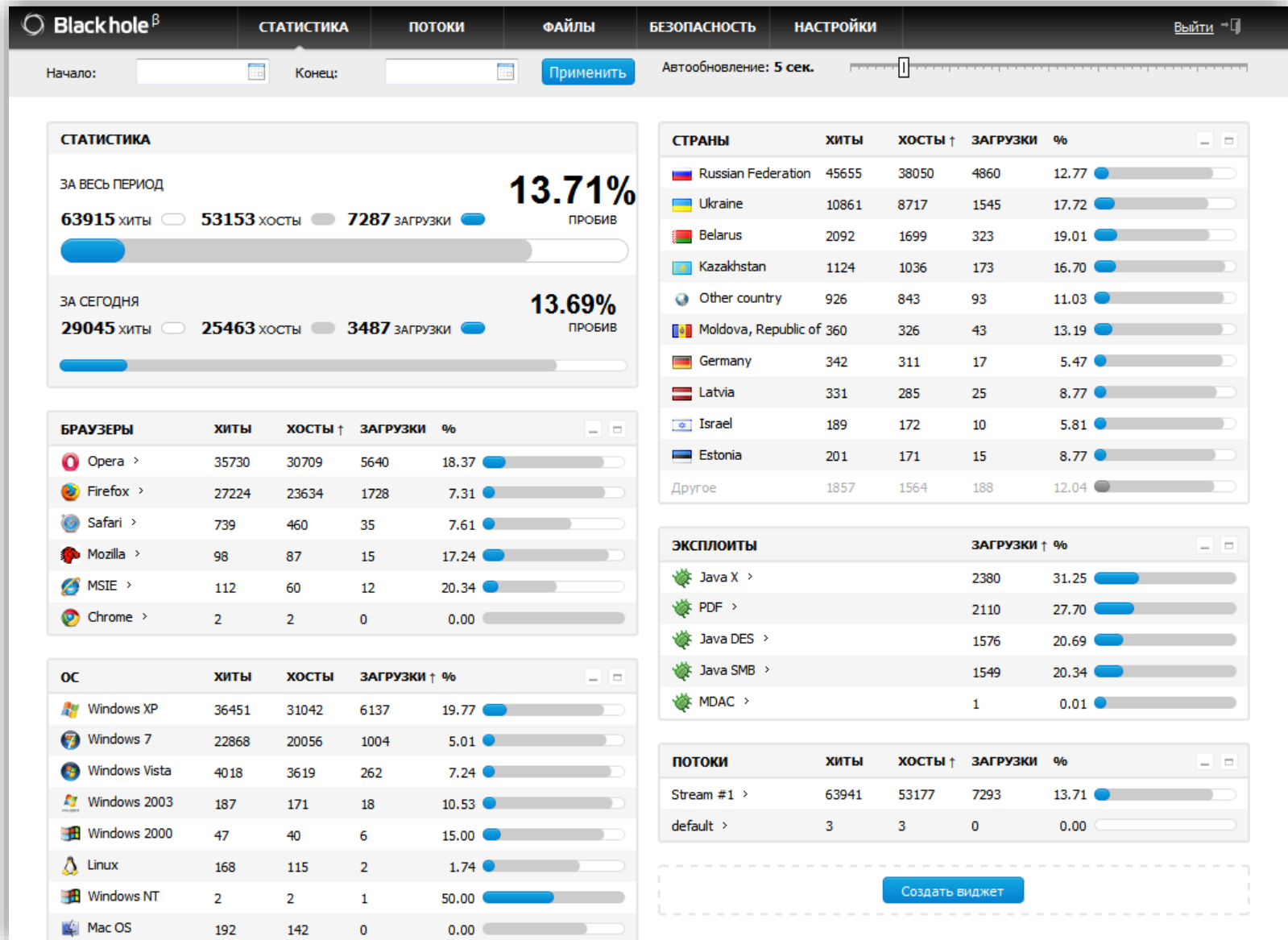
browser stats

			
10786 (2645 loads) 25%	4503 (737 loads) 16%	139 (9 loads) 6%	1514 (9 loads) 5%

Nuclear Pack Exploit Kit



Blackhole Exploit Kit



Compradores de vulnerabilidades & exploits

- Fabricantes (vendors)
- Empresas de seguridad
- Gobiernos
- Mercado negro
- Intermediarios



HackerOne

SANDBOX

Sandbox Escapes

Minimum bounty:
\$5,000.00

Start hacking 

Flash

Flash



Python



Ruby

php

PHP

django

Django



Ruby on Rails

Perl

Perl

Zero Day Initiative (TippingPoint)

TippingPoint Zero Day Initiative



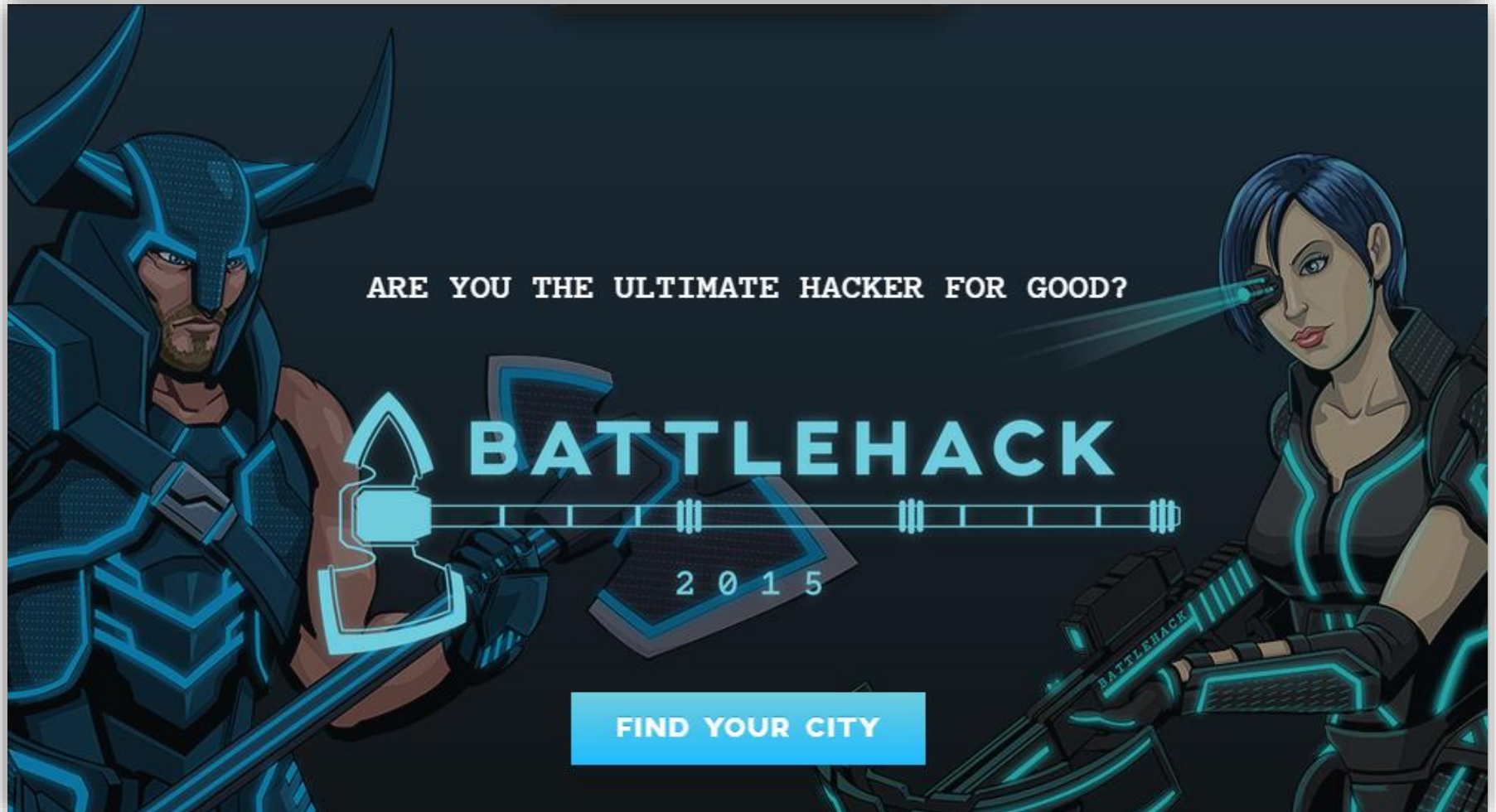
The Zero Day Initiative (ZDI), founded by TippingPoint, is a program for rewarding security researchers for responsibly disclosing vulnerabilities. Depending on who you are, here are a few links to get you started:

- **Researchers:** Learn [how we pay](#) for your vulnerability discoveries, [register](#) for the ZDI or [login](#).
- **Vendors:** Read our [disclosure policy](#) or join our [security partner program](#)
- **Press, Curiosity Seeker:** [Learn more](#) about ZDI or read answers to some [frequently asked questions](#)

Please contact us at [zdi \[at\] tippingpoint \[dot\] com](mailto:zdi@tippingpoint.com) with any questions or queries. For sensitive e-mail communications, please use our [PGP key](#).

[About](#) | [Upcoming Advisories](#) | [Published Advisories](#) | [Researcher Login](#) | [Twitter](#)

Battlehack – Competencia internacional



Bounty Bugs Populares



Microsoft Bounty Programs



Call out to all Microsoft friends, hackers, researchers! Want to make our popular products better? And earn money doing so? Step right up.

Microsoft is now offering direct payments in exchange for identifying security exploitation techniques.

Microsoft has championed many initiatives to advance security, including the Security Development Lifecycle (SDLC) process to build more secure products.



mozilla

[HOME](#) > [MOZILLA SECURITY](#) >

Bug Bounty Program

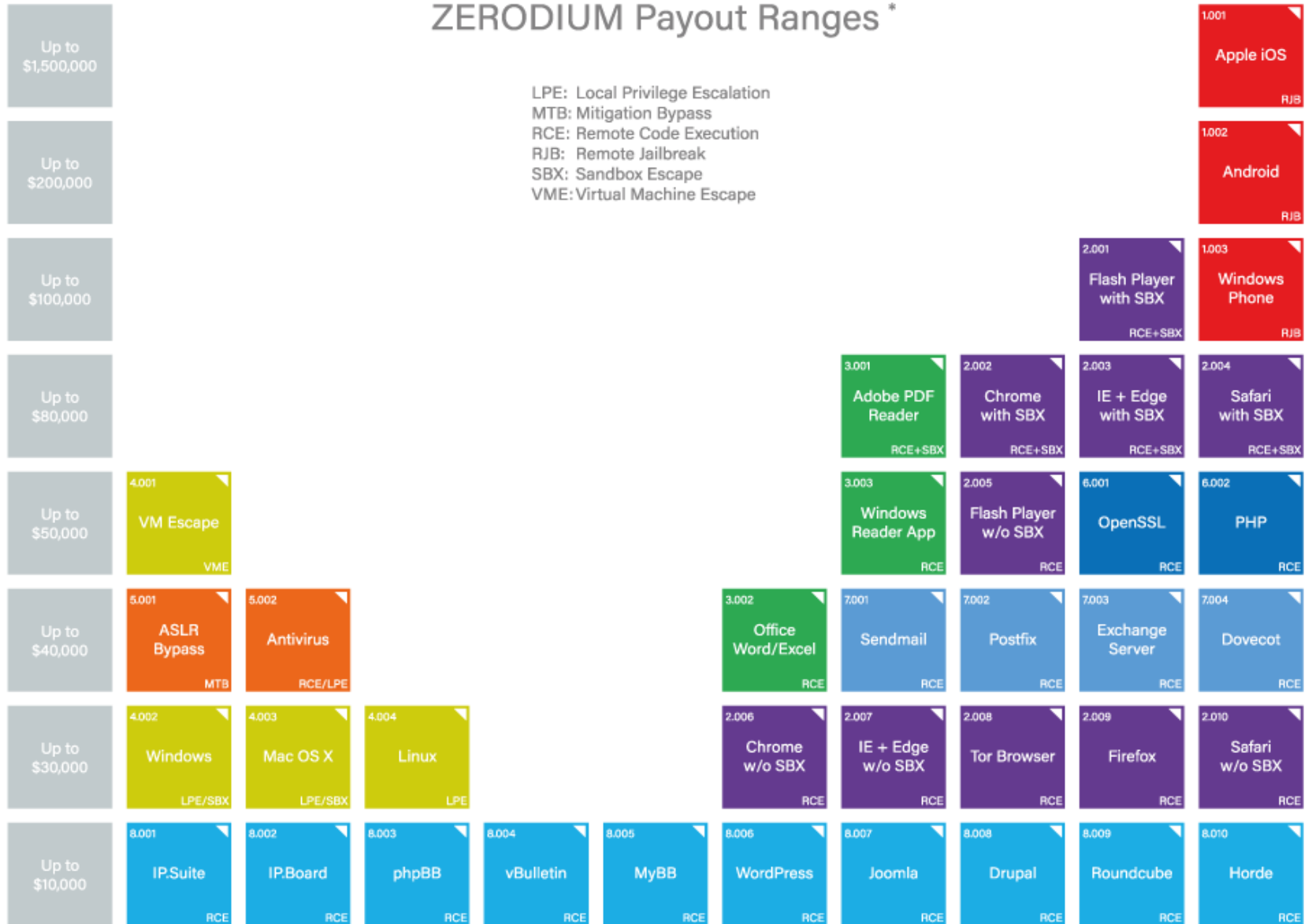
Google Vulnerability Reward Program (VRP)

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	<i>Command injection, deserialization bugs, sandbox escapes</i>	\$20,000	\$20,000	\$20,000	\$1,337 - \$5,000
Unrestricted file system or database access	<i>Unsandboxed XXE, SQL injection</i>	\$10,000	\$10,000	\$10,000	\$1,337 - \$5,000
Logic flaw bugs leaking or bypassing significant security controls	<i>Direct object reference, remote user impersonation</i>	\$10,000	\$7,500	\$5,000	\$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	<u>Web</u> : <i>Cross-site scripting</i> <u>Mobile</u> : <i>Code execution</i>	\$7,500	\$5,000	\$3,133.7	\$100
Other valid security vulnerabilities	<u>Web</u> : <i>CSRF, Clickjacking</i> <u>Mobile</u> : <i>Information leak, privilege escalation</i>	\$500 - \$7,500	\$500 - \$5,000	\$500 - \$3,133.7	\$100

Zerodium

ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape



Lista de programas de recompensa



LIST OF BUG BOUNTIES & DISCLOSURE PROGRAMS

The most comprehensive collection of bug bounties & disclosure programs provided by companies world wide for all the security researchers out there.



¿Preguntas?

Federico Pacheco



@FedeQuark



www.federicopacheco.com.ar



info@federicopacheco.com.ar