

Microsoft Digital Crimes Unit

Sebastian Palacios
Abogado Unidad de Seguridad Digital



La Ciberseguridad es
una preocupación
de todos



71%

de compañías admiten
haber sido víctimas de un
ciber-ataque en el 2015

556M

víctimas anuales del
cibercrimen

160M

de registros de información
personal filtrada dentro de los
8 mayores ataques
diberneticos del 2015

\$3B

es el costo economico
estimado que va a
provenir de la industria del
cibercrimen en el 2020.

\$400.000M

anuales le cuestan los ciber-
ataques a las empresas.

140+

Tiempo promedio entre
una infección y su
detección.

RATES AND COMMERCIAL VALUES OF UNLICENSED PC SOFTWARE INSTALATIONS

LATINOAMÉRICA								
 Argentina	69 %	69 %	69 %	71 %	\$554	\$950	\$657	\$645
 Bolivia	79 %	79 %	79 %	80 %	\$98	\$95	\$59	\$40
 Brasil	47 %	50 %	53 %	56 %	\$1770	\$2851	\$2848	\$2254
 Chile	57 %	59 %	61 %	64 %	\$296	\$378	\$382	\$315
 Colombia	50 %	52 %	53 %	55 %	\$281	\$396	\$295	\$244
 Costa Rica	59 %	59 %	58 %	59 %	\$90	\$98	\$62	\$33
 República Dominicana	76 %	75 %	76 %	77 %	\$84	\$73	\$93	\$66
 Ecuador	68 %	68 %	68 %	67 %	\$137	\$130	\$92	\$65
 El Salvador	81 %	80 %	80 %	80 %	\$63	\$72	\$58	\$46
 Guatemala	79 %	79 %	79 %	80 %	\$169	\$167	\$116	\$74
 Honduras	75 %	74 %	73 %	74 %	\$36	\$38	\$24	\$17
 México	52 %	54 %	57 %	60 %	\$980	\$1211	\$1249	\$1056
 Nicaragua	82 %	82 %	79 %	79 %	\$23	\$23	\$9	\$5
 Panamá	72 %	72 %	72 %	73 %	\$117	\$120	\$74	\$42
 Paraguay	84 %	84 %	83 %	82 %	\$89	\$115	\$73	\$29
 Perú	63 %	65 %	67 %	70 %	\$210	\$249	\$209	\$124
 Uruguay	68 %	68 %	68 %	68 %	\$57	\$74	\$85	\$40
 Venezuela	88 %	88 %	88 %	87 %	\$402	\$1030	\$668	\$685
Otros países de Latinoamérica	83 %	84 %	84 %	83 %	\$331	\$352	\$406	\$430
TOTAL DE LATINOAMÉRICA	55 %	59 %	61 %	62 %	\$5797	\$9422	\$7459	\$6210

Nivel de Madurez en Ciberseguridad

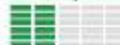


Organization of
American States
Here I fight for better people

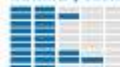


Chile

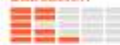
Política y estrategia



Cultura y sociedad



Educación



Marcos legales



Tecnología



El Ministerio del Interior y Seguridad Pública, el Secretario General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen la política de seguridad cibernética a nivel gubernamental. Si bien el país no ha emitido una estrategia nacional de seguridad cibernética, la sensibilización entre las instituciones gubernamentales es generalizada. La infraestructura gubernamental presenta tecnología de seguridad actualizada y los partes interesados pertinentes regularmente analizan los activos y vulnerabilidades de la infraestructura Crítica Nacional. El Estado también coordina la planeación de gestión de crisis y ha puesto en marcha medidas de redundancia.

Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control. Uno de los principales desafíos de Chile de cara al futuro es el fortalecimiento de su capacidad de respuesta a incidentes: el CSIRT-CL que se encuentra en funcionamiento desde 2004 ofrece respuesta a incidentes para los sitios web del gobierno pero no está institucionalizado formalmente a nivel nacional para abordar todo tipo de violaciones.

Chile ha establecido un marco jurídico global para hacer frente a los delitos cibernéticos. El Decreto Supremo n° 1299 describe las normas y define los roles para el manejo de la delincuencia cibernética, la Ley n° 19.223 introduce los delitos informáticos al Código Penal y la Ley n° 19.628 cubre la privacidad y protección de datos. Aunque el sector privado no está obligado por ley a divulgar las violaciones, el gobierno trabaja en estrecha colaboración con las empresas para informar y responder a incidentes cibernéticos. De acuerdo con las autoridades de Chile, la

suplantación de identidad (phishing), malware y piratería informática son los tipos más frecuentes de ataques cibernéticos en el país. El Departamento de Investigación de Organizaciones Criminales (OIC-9) y el Laboratorio de Criminalística de los Carabineros (LABOCAR), la policía nacional de Chile, llevan a cabo investigaciones y análisis forense digital respectivamente. Estas unidades han detenido con éxito numerosos criminales cibernéticos en los últimos años. Por último, los tribunales tienen una capacidad adecuada para manejar evidencia electrónica.

La mentalidad de seguridad cibernética es inconsistente en la sociedad chilena. En 2013, para crear conciencia, el Ministerio de Educación inició la campaña de Internet Segura para educar a los jóvenes sobre la privacidad y el uso seguro de Internet. También está en marcha una campaña, llamada Consumidor Digital, para que los ciudadanos tengan cuidado de los riesgos del comercio electrónico y para que entiendan sus derechos como consumidores. La Universidad de Chile ofrece títulos avanzados en seguridad cibernética y también están disponibles diversos cursos en línea y capacitación para empleados. Comparativamente, el sector privado se ha vuelto cada vez más consciente de los riesgos de seguridad cibernética y ha puesto en marcha planes para abordarlos.

POPULACIÓN TOTAL DEL PAÍS	17.762.647
Adornos a teléfonos celulares	23.683.351
Personas con acceso a Internet	12.769.105

Penetración de Internet

72%



STARTUP

FORMATIVE

ESTABLISHED

STRATEGIC

DYNAMIC



Estudios

Falsificación de Software y Malware

1 de cada 3

Software falsificado
contiene Malware

0.79

Correlación entre el
software sin licencia y las
amenazas de seguridad

+60%

Posibilidad de encontrar
malware en un equipo
comprado con software pirata

País	Tasa Software sin Licencia	Tasa de Malware
Argentina	69	25
Brazil	50	31
Chile	59	22
Colombia	52	29
Dominican Republic	75	30
Ecuador	68	35
Guatemala	79	22
Mexico	54	31
Peru	65	37
Uruguay	68	19
Venezuela	88	32

Liderando la lucha contra el cibercrimen

El Impacto del Cibercrimen

Reseña de la DCU

La Amenaza de Malware

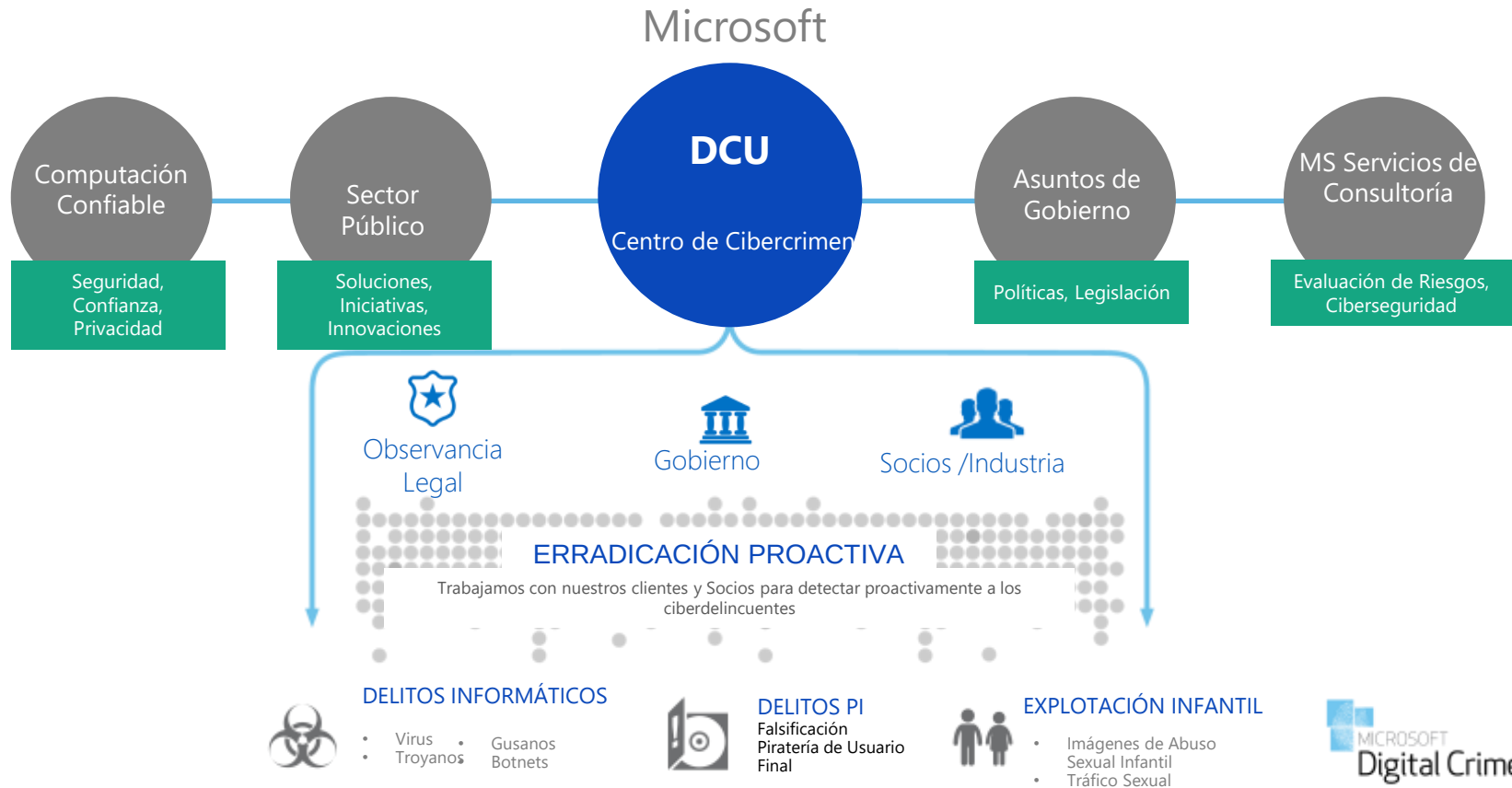
Combatiendo Delitos contra la PI

Combatiendo la Explotación Infantil Online

Cómo puedes ayudar?



Una nueva era en la lucha contra el cibercrimen



DCU Malware Takedowns and Disruptions

Conficker

February 2010
Botnet Worm

Worm spread via USB and internet. Would infect other devices in common network. Global cyber-security elites joined forces.

Microsoft-led model of industry-wide efforts.

Waledac

February 2010
Spam

Trojan that collects email addresses, distributes spam, posts data to web, downloads executable files.

Proving model of industry-led efforts. Severed 70-90K devices from the botnet.

Rustock

March 2011
Spam

Rootkit-enabled back door Trojan which distributed spam e-mail. Support by stakeholders across industry sectors.

Involved US & Dutch law enforcement and CN-CERT.

Kelihos

September 2011
Spam, Bitcoin Mining, Distributed DoS Attacks

Trojan that distributes spam, steals logins, bitcoins, downloads and executes files.

Partnership between Microsoft and security software vendors. First operation with named defendant.

Zeus

March 2012
Identify Theft, Financial Fraud

Steals identity, financial info, controls PC, turns off firewall, installs other malware, ransomware.

Cross-sector partnership with financial services. Focused on disruption because of technical complexity.

Nitol

September 2012
Malware Spreading Botnet, Distributed DoS Attacks

Introduced in the supply chain relied on by Chinese consumers.

Settled with operator of malicious domain.

Bamital

February 2013
Advertising Click-Fraud

Hijacked user's search results, took victims to dangerous sites.

Takedown in collaboration with Symantec. Proactive notification and cleanup process.

Citadel

June 2013
Identity Theft, Financial Fraud

Committed online financial fraud responsible for more than \$500M in losses.

Public-private sector partnerships critical for coordinated disruption.

ZeroAccess aka Sirafef

December 2013
Advertising Click-Fraud

Hijacks search results, takes victim to dangerous sites. Cost online advertisers upwards of \$2.7M each month.

Successful disruption in partnership with Europol EC3, FBI, A10 Networks.

GameOver Zeus

June 2014
Identity Theft / Financial Fraud

Extremely sophisticated trojan which steals banking credentials. Spread via spam or phishing messages.

Worked in partnership with law enforcement providing technical remediation.

Bladabindi & Jenxcus

June 2014
Identity Theft, Financial Fraud, Privacy Invasion

Malware using Dynamic DNS for command. Involved password and identity theft, webcam and other privacy invasions.

Over 200 different types of malware impacted.

Caphaw

July 2014
Identity Theft / Financial Fraud

Focused on online financial fraud responsible for more than \$250M in losses.

Coordinated disruption with public-private sector partnerships.

Ramnit

February 2015
Identity Theft / Financial Fraud

Module-based malware which concentrates on stealing credential information from banking websites.

International public-private partnership, shut down C&C servers, redirected 300 domains.

Simda

April 2015
Identity Theft / Financial Fraud

Uses remote access to steal personal and banking info, as well as install other malware.

Partnered with Interpol and industry partners and activated CME platform to disrupt global malware attack.

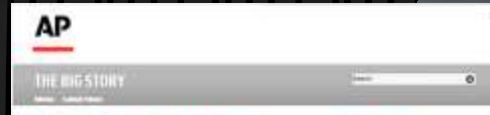
Dorkbot

December 2015
Identity Theft / Financial Fraud

Disables security, steals credentials, personal info, distributes other malware. Spreads via USB, messaging, and social networks.

Partnership with Homeland Security and international agencies.

Microsoft leads disruption of largest infected global PC network



Police shut down network 'used to steal bank details'



A network of computers that has spread malware to millions of machines has been shut down, justice have said.

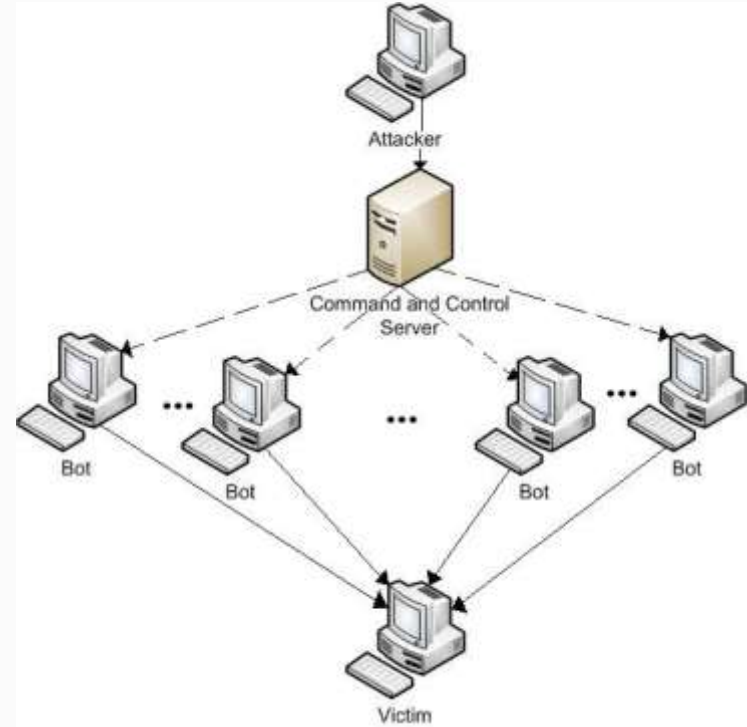


Qué son los “Botnets”?

Los “Botnets” son redes de computadores infectados con diferentes tipos de “malware” que pueden ser controlados por un individuo u organización.

Los “Botnets” generalmente son controlados por personas inescrupulosas con el objeto de perpetrar graves ataques contra la infraestructura tecnológica de individuos u organizaciones, comprometiendo su seguridad informática.

Por lo anterior es necesario controlarlos y mitigar su impacto negativo.



Malware, botnets y crimen organizado

Crimen
Organizado



Software Pirata



Botnet



En 2013 el estudio de IDC estimó que los usuarios gastarían 22 billones US\$ Y 1.5 billones de horas para reparar fallas de seguridad derivadas de software pirata, acaecidas el año 2013.

Malware, botnets y crimen organizado

Crimen Organizado



Cadena de Suministro insegura

Botnet



Ciberdelincuentes construyeron el botnet Nitol infectando productos digitales como PCs y software, distribuidos a través de cadenas inseguras de suministro.

Una cadena de suministro entre el fabricante y el consumidor se vuelve insegura cuando un distribuidor o revendedor recibe o vende productos de fuentes desconocidas o no autorizadas.

Crimen
Organizado



Botnet



Malware
captura
nuevas
máquinas



Distribución
de Spam



Ataque de
Denegación
de Servicio



Malware, botnets y crimen organizado

La creación y distribución de malware daña a los usuarios de internet.

Un solo botnet le puede permitir a un ciberdelincuente cometer decenas de billones de actos ilegales en un solo día.

Estos pueden incluir el envío de Spam, Ataques de Denegación de Servicio, infección de otros computadores con Malware.

Citadel

Red diseñada compuesta por más de 1,400 botnets para robar información financiera.

Arrojó pérdidas por más de \$500 MM de dólares.

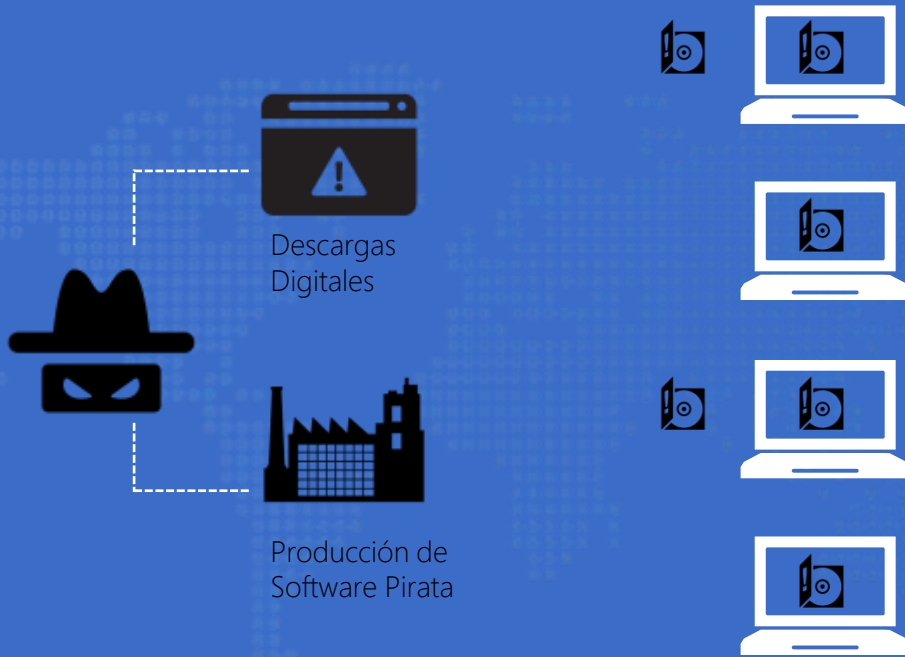
Se detectó el origen de la red en Rusia y Europa Oriental.

Alianza con Asociaciones de Instituciones Financieras, Socios de industria y el FBI permitió debaratar esta red en Junio del 2013.

Microsoft sostiene que su acción disruptiva contra las botnets fue un éxito y confía en que se cortó la mayor parte de las redes de Citadel se dispuso a atacar.

La disrupción de botnets ayuda a reducir la amenaza de futuros ataques, desbaratando la infraestructura creada por los ciberdelincuentes.

Software Pirata: Fuente clave de malware



Delincuentes están adoptando la piratería de software:

Es lucrativo

Propaga malware

1 de cada 3 computadores con software pirata instalado será infectado por malware.

Es menos riesgoso para los delincuentes y tiene una baja barrera de entrada.

Liderando la lucha contra el cibercrimen

El Impacto del Cibercrimen

Reseña de DCU

La Amenaza de Malware

Combatiendo Delitos contra la PI

Combatiendo la Explotación Infantil Online

Cómo puedes ayudar?



Combatiendo Delitos PI



Combate tanto la venta física de sw pirata o falsificado como la venta on-line, tanto el sublicenciamiento de usuarios finales como la venta en canal de equipos con sw no licenciado pre-instalado.

Término por acuerdo de 3265 infracciones de derecho de autor el 2013 y removi6 2,5 millones de archivos de sw pirata MS ofrecido en línea.

La coordinación con web hosts, ISPs, Registros de Nombres de Dominio y compañías de tarjetas de crédito es clave para cortar la capacidad de procesar los pagos.

Distribución de Software Pirata y Falsificado



E-commerce de SW
pirata y falsificado



Mercados Online



Descargas en un Click

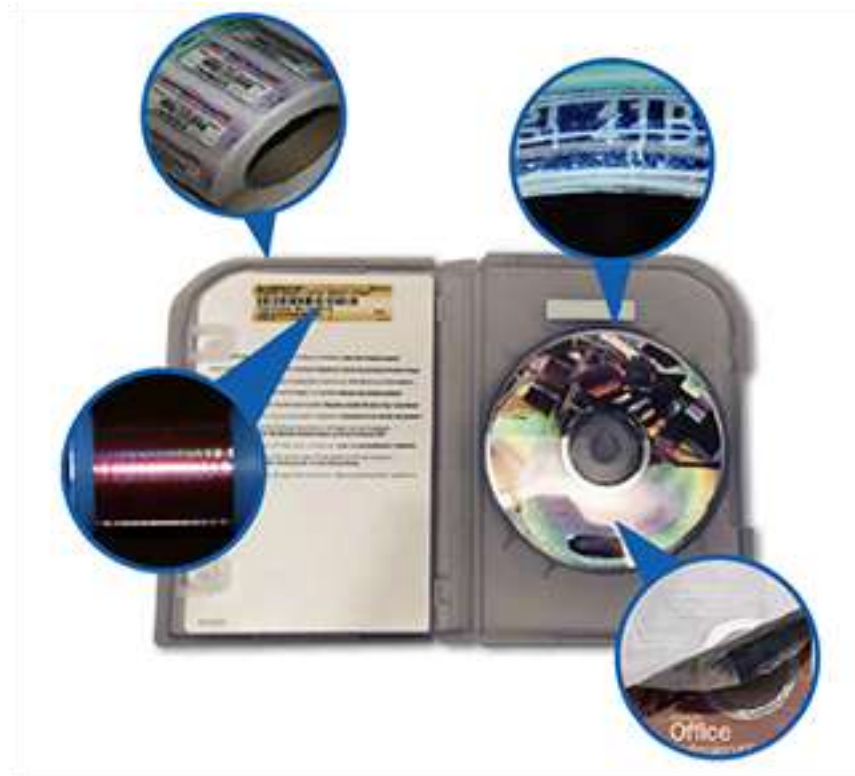


Descargas BitTorrent P2P



PC Malls

Ciberforenses



Detectando software pirata

Revisión de Material sospechoso obtenido a través de compras de prueba, allanamientos y entregas de los clientes

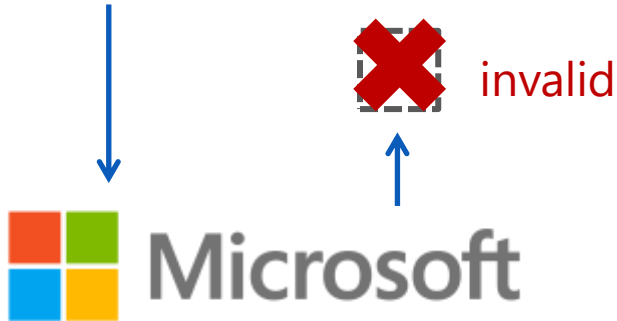
Inspección de material físico y digital

Lector de rayos infrarrojos o UV para chequear cadena de seguridad.

Claves de los productos son chequeadas en base de datos de claves robadas.

La evidencia se almacena y los resultados son reportados

Ciberforenses: identificación y rastreo de claves robadas

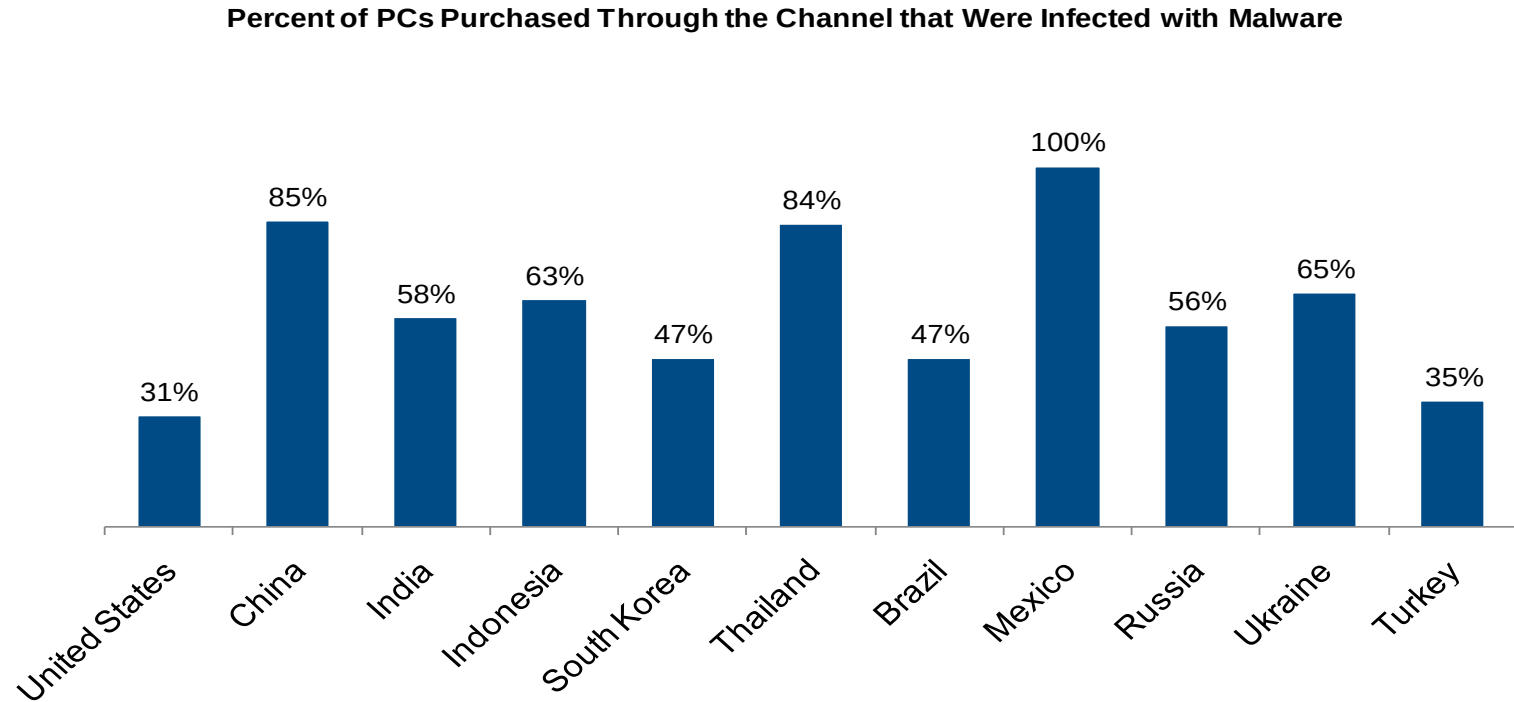


Claves de productos robadas son una herramienta relevante para los delincuentes.

Cada hora, aprox. 100,000 PCs intentan activar productos utilizando una clave.

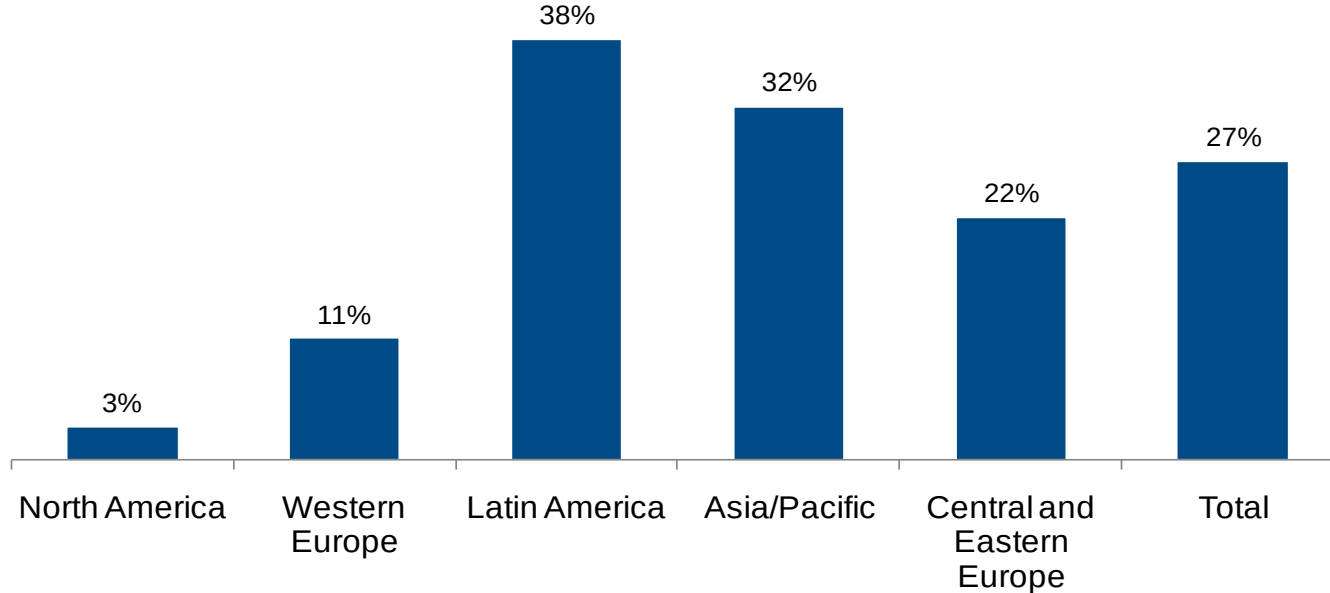
Aproximadamente el 45% de las activaciones se frustra debido a las claves robadas.

% PC's Purchased @ Non-reputable Markets (IDC Study 2014)

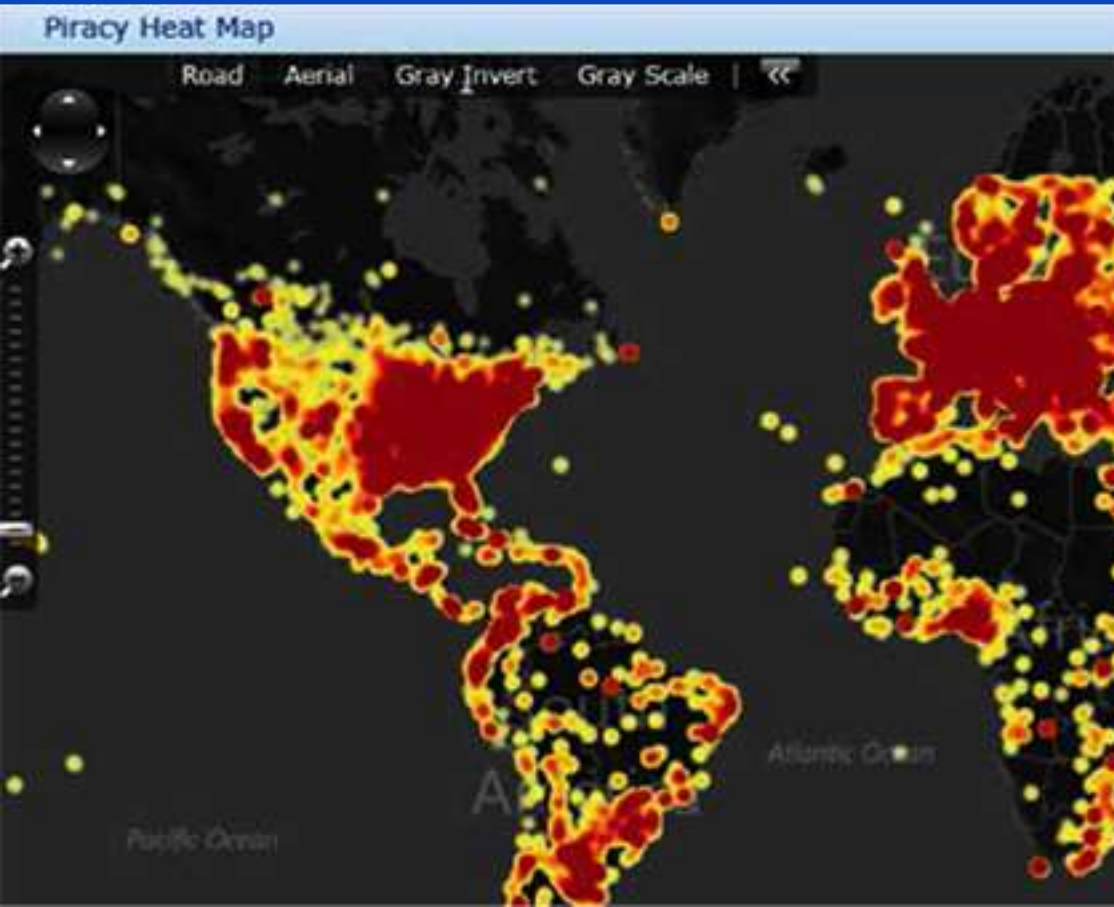


% of employees install unauthorized software

**Percent of Employees Installing Their Own Software Without the Enterprise's Knowledge
on Work Computers Within the Last Two Years**



Ciberforenses: identificación y rastreo de claves robadas



Activaciones frustradas son mapeadas en tiempo real.

Se establece fácilmente los patrones de distribución de claves robadas

Foco se pone en "hotspots" globales, donde se origina el fraude.

Remoción agresiva de software pirata



Bajadas Online

Monitoreo global 24/7 global de la web

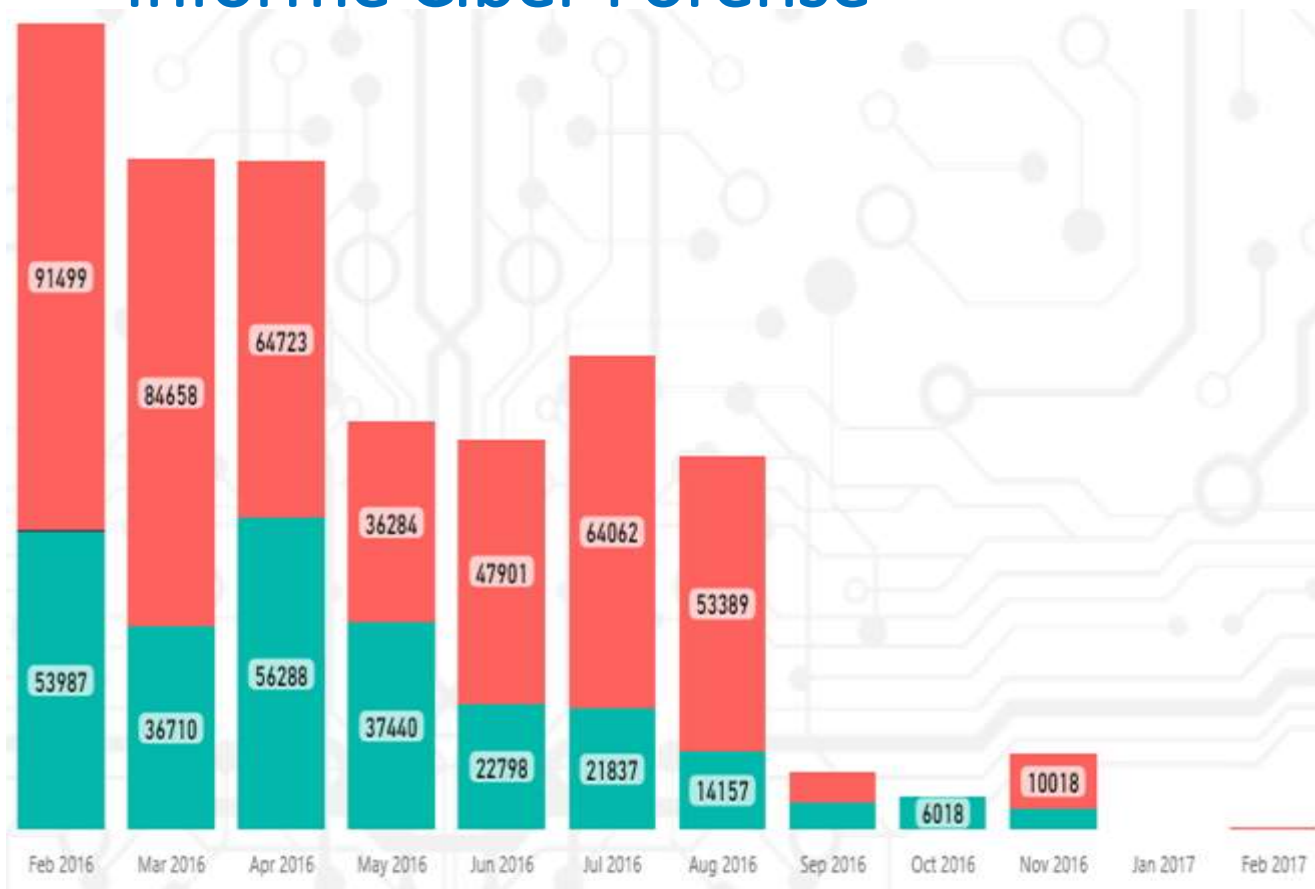
Estar al día de la mutación y evolución de estos ilícitos.

Individualizamos y detectamos sitios ilegales existentes entre los más de 600 millones de sitios web a nivel mundial.

Con una red de servidores en 70 países, analizamos anónimamente sitios ilegales.

Removemos más de 2 millones de archivos ilegales y cerramos más de 100 cuentas comerciales cada mes.

Informe Ciber Forense



Total de Conexiones

716,312

IPAddress	Malware Connecio...
200.54.110.202	249512
200.54.110.204	231529
200.75.16.154	146851
200.54.110.201	66927
200.54.110.206	7471
200.54.110.208	6874
200.54.110.212	4527
200.54.109.220	2403
200.54.110.203	218
Total	716312

● B106 ● Conficker ● Dorkbot

Liderando la Lucha contra el Cibercrimen

El Impacto del Cibercrimen

Reseña de DCU

La Amenaza de Malware

Combatiendo Delitos de IP

Combatiendo Explotación Infantil Online

Cómo puedes ayudar?



Cómo puedes ayudar?



Políticas Públicas

Asegurar un entorno legislativo que disuada el cibercrimen.

Proteger las economías, los empleos e innovación, priorizando la erradicación del cibercrimen.

Interrumpir la demanda de sw pirata.

Implementar tecnología que alerte sobre amenazas a la ciberseguridad.

Tolerancia cero al abuso infantil online.

Cómo puedes ayudar?



Observancia Ley Penal

Desmantelar operaciones de suministro de productos piratas.

Dar de baja botnets asociados a organizaciones criminales.

Remover tiendas en línea ilegales que venden productos y dispositivos falsificados.

Establecer nuevas tácticas para combatir la explotación infantil online.

Utilizar data recogida en acciones civiles para acelerar el procesamiento de ciberdelincuentes.

Cómo puedes ayudar?



Socios de Industria

Implementar tecnología que alerte sobre amenazas a la ciberseguridad.

Interrumpir la demanda de sw pirata.

Fortalecer las cadenas de suministro.

Cero tolerancia al abuso infantil online.

Requerir a otros socios que adopten medidas similares.

Cómo tener éxito?



Los ciberdelincuentes continuarán reinventándose. Para detenerlos:

Invertir en las últimas herramientas tecnológicas.

Conocer la infraestructura de los ciberdelincuentes y educar al respecto.

Forjar fuertes alianzas público-privadas,

“

Businesses and users are going to embrace technology only if they can trust it.

Satya Nadella
CEO Microsoft