EL MERCADO DE LAS VULNERABILIDADES INFORMÁTICAS

LA DESREGULACIÓN DE LA VIGILANCIA DIGITAL

OBJETIVOS

Presentación + pronombres

- Esbozar un ecosistema de los diferentes actores involucrados en la compra y venta de vulnerablididades y exploits
- Avanzar más allá de las agencias gubernamentales y estados. Complejizar la escena.
- Investigación en curso + debate a posteriori.

Idioma: español + términos en ingles Voluntarixs para tomar notas

ESTRUCTURA DE LA SESIÓN

1) Glosario
2) Actores
3) Análisis del gráfico: qué se comercializa, cómo, por quién.
4) Regulación
5) Cierre con debate de cómo mejorar gráfico.

GLOSARIO

¿QUÉ ES UNA VULNERABILIDAD?

Es un falla o limitación en el diseño, procedimiento o implementación de un sistema.

Una vulnerabilidad "explotable": falla que representa un riesgo de seguridad.

¿QUÉ ES UN “EXPLOIT”?

Una porción de código, una serie de caracteres o secuencia de comandos que permiten aprovecharse de una vulnerabilidad para lograr un funcionamiento no esperado de un programa o ganar acceso a un sistema.

¿QUÉ ES UN ATAQUE ZERO DAY?

Ante una vulnerabilidad que todavía no fue parcheada o mitigada. También se lo considera cuando no es pública información de la vuln ni en general ni el vendor: por lo que no existe parche o solución.

Un ataque de día es un exploit que la aprovecha de esa vulnerabilidad.

¿QUÉ ES VENDOR?

Lxs encargados de desarrollar y mantener el código del software vulnerable. Son lxs que hacen los parches.

¿QUÉ ES PARCHE?

Los cambios que se le hacen a un programa para corregir los errores que lo vuelven vulnerable.

¿QUÉ ES DISCLOSURE?

- Revelación de información acerca de una vuln con o sin info de cómo explotarla.
- Proceso por el cual info de una vuln se comparte con 3eros.
- **Full disclosure:** hacer pública una vuln antes de que el vendor tenga un parche. Con/Sin POC.
- **POC:** con código que funciona como Prueba de Concepto: resumen de cómo se explotaría: descriptivo y funcional. Explica en términos técnicos como aprovecharse de la vuln.

DISCLOSURE COORDINADO

Disclosure coordinado o "responsable": lxs vendors tienen el control de la información sobre la vulnerabilidad.

¿CÓMO SE CLASIFICAN LAS VULNERABILIDADES?

CLASIFICACIÓN POR EL TIPO DE EXPLOIT:

DoS (ataque de denegación de servicio):

Escalar privilegios:

Ejecución remota de código:

CLASIFICACIÓN SEGÚN DESDE DONDE SE EXPLOTA:

Desde internet: *ej. Atacar un servicio web publico*

Desde la misma red: *ej. ataque sobre una lan o vpn*

Local desde la misma maquina: *ej. escalar privilegios*

CLASIFICACIÓN SEGÚN COMPLEJIDAD PARA EXPLOTARLA:

Necesita autenticacion? *Ej. ataque con credenciales/token.*

Necesita phishing? *Ej. click a un enlace malicioso.*

Necesita acceso físico? *Ej. ataque por WIFI o USB.*

IDENTIFICADORES:

Hay varios identificadores de vulnerabilidades, los mas comunes

- Common Vulnerabilities and Exposures (CVE)
- National Vulnerabilitiy Database (NVD)

MERCADO

- Que mercados hay?
- Qué se comercializa?
- Quien comercializa?

QUE MERCADOS HAY?

- Mercados anonimos/informales
- Mercados privados
- Mercados publicos con y sin disclosure

Intercambios por $$$ o por hall of fame.

QUE SE COMERCIALIZA?

- Vulnerabilidades
- Exploits
- BotNets
- Exploitkits y Malware varios
- Accesos a dispositivos/redes

QUIEN COMERCIALIZA?

- Independientes/Anonimos
- Organizaciones privadas (empresas de venta de SW de vigilancia HT)
- Corporaciones
- Intermediarios: como Brokers for profit (Zerodium)
- Vendors: Programas Vuln disclosure
- Plataformas Bug Bounty
- Agencias gubernamentales.
- APTs

INTERMEDIARIOS: BROKERS PAGOS

Compran a investigadores independientes (Zero days y no zero days.)

Venden a clientes (corporaciones -solo "defensivo"- y/o gobiernos) x suscripciones anuales: junto mitigaciones/recomendaciones de seg. Con o sin disclosure a vendor.

Los vendors y usuaries estan forzados a subscribirse para evitar no tener informacion importante.

Ej: Zerodium (suscripción sale usd 500.000 al año), Crowdfense

BUG BOUNTIES: PROGRAMAS DE RECOMPENSA DE BUGS

Vendors y Programas bug bounty: Hay distintos tipos de Bug Bounties, organizados por el mismo vendor (ej: google, facebook, mozilla)

Plataformas de BB un tercero (HackerOne) que media entre la investigadora y el vendor. La mayoria de las vulnerabilidades encontradas en las plataformas son de poco impacto como xss o xxe. Ejemplo: bugcrowd, HackerOne

AGENCIAS GUBERNAMENTALES

- Desarrollan sus propios exploits para vulns existenten
- Encuentran sus propios zero days
- Compra a privados algunos de sus exploits/zero days

ANÁLISIS DEL GRÁFICO DE ACTORES

REGULACION

CONVENIO BUDAPEST

- Convenio en Cybercrimen firmado en 2001.

PROBLEMAS

- Criminaliza la investigacion y desarrollo de herramientas de seguridad.
- **Paises en America:** Argentina, Canada, Chile, Colombia, Costa Rica, Panama, Paraguay, Peru, Republica Dominicana, Estados Unidos

ACUERDO DE WASSENAAR

Acuerdo multilateral de control de exportacion de armas y tecnologias duales

PROBLEMAS

- En el 2013 se agrego sistemas de vigilancia e intrusion de forma tan amplia que incluia a la gran mayoria de tecnologias usadas en investigacion y desarrollo en infosec.
- En el 2015 se hicieron modificaciones para mejorar los cambios del 2013, Ahora no entran tecnologias para vulnerability disclosure o cyber incident response. esto sigue siendo limitado.

A MODO DE CIERRE

- La mayoría del tiempo la usuarix es vulnerable.

Cómo se pone a disposición info de vulns al público para que estén seguros más rápido.

Tener plataforma de bugbounties: wall of honour. Tener un mecanismo de disclosure. Y aceitar mecanismos de emparchado. Darle la importancia que se merecen a parches.
Uso privado de info restringida sobre vulns con objetivos pol y economicos.

- Comoditización: de vulnerabilidades en mercados que permiten su compra-venta como un bien más. Vulnerabilidades/exploits como unidades de intercambio con un precio asignado, con una demanda y un comprador.

- Es importante la seguridad ofensiva / investigación en seguridad / analisis de vulnerabilidades para la detección de vulnerabilidades de alto impacto, para elevar la seguridad de todxs. Que no se criminalice. Necesitamos que si hay regulación que vayan en esa línea.
- Hay poca info de este mercado: hackeos a Hacking Team (2015) y Gamma International (2014) permiten conocer más. Se necesita mas informacion publica.