ARKOON
NETWORK SECURITY

L'impact des attaques 0day

L'impact des attaques 0day est mésestimé par le grand public. On les imagine réservées au gotha du monde numérique : espionnage et intelligence industrielle seraient les seuls utilisateurs de ces techniques. La réalité se rapproche plus d'un produit grand public classique, évoluant entre innovation, croissance, maturité et obsolescence.

Matière première de l'industrie du cyber-crime

Des chercheurs, souvent individuels, découvrent des failles non référencées et créent un POC (« proof of concept ») prouvant leur capacité à l'exploiter. Cette exploitation consiste en l'exécution d'un code *arbitraire* sur la machine victime. Le POC est essentiel car il démontrera que n'importe quel virus ou code malicieux pourra être exécuté grâce à l'exploitation de la faille. La valeur financière d'un tel POC dépend :

- Du nombre de victimes potentielles. Ce nombre est très lié à la popularité du logiciel présentant la faille : les programmes de traitement de texte, les lecteurs de documents et les systèmes d'exploitation arrivent donc en tête des recherches
- De la facilité d'utilisation de la faille. Les exploitations présentant un caractère aléatoire, les acheteurs du POC voudront maximiser la probabilité de réussite de l'attaque

Le métier de chercheur étant très différent de celui de voleur, vandale, ou racketeur, on comprendra aisément que les premiers fournissent le produit de leur labeur tel quel, et qu'ils ne s'impliquent pas dans leur utilisation finale. Ainsi, ils ne développent généralement pas de virus, vers, ou autres trojans : leur activité se concentre sur les failles, qui permettront in fine à d'autres acteurs de lancer les codes malicieux qu'ils auront eux-mêmes produits.

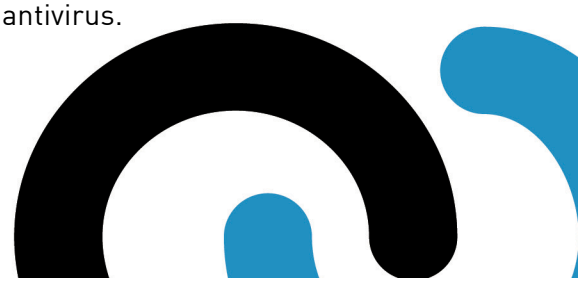
De la matière première au produit fini : l'ajout du *payload*

Le *payload*, ou charge viral, est le code malicieux que chacun ajoutera au POC en fonction de ses besoins. L'exploitation de la vulnérabilité n'a pas d'autre objectif que l'exécution de cette charge virale chez la victime. L'attaque finale consistera donc en un paquet contenant : le code nécessaire à l'exploitation de la faille, et le virus (ou assimilé) satisfaisant les besoins de l'attaquant.

Chaque acteur de la florissante économie du cyber-crime a ses propres besoins : spammeurs, carders, racketeurs, vandales, espions, tous sont susceptible de créer un payload différent. De grandes tendances se dessinent cependant :

- Certains veulent récupérer des données chez leurs victimes directes. Le payload est alors un simple espion capturant les frappes clavier, volant les mots de passe, exfiltrant fichiers et emails
- Certains préfèrent construire un grand réseau de machines infectées avant de lancer une quelconque action. Ces créateurs de *botnets* vendront ou loueront plus tard leur réseau à des clients cherchant des relais de spam, ou voulant lancer des attaques de type DOS

Il est important de noter qu'un autre acteur intervient souvent dans l'ajout du payload : le *packer*. Ce spécialiste des technologies antivirus a pour mission de fournir des méthodes, souvent cryptographiques, permettant de multiplier les formes que peuvent prendre un unique payload. Cette fonction contourne la contre-mesure la plus communément utilisée : la signature antivirus. En étant capable de modifier en permanence l'apparence du payload sans pour autant altérer sa finalité, le packer complique fortement le travail des éditeurs d'antivirus.



Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com

Un cycle de vie complet

Les utilisateurs de l'attaque se divisent en deux groupes distincts.

Première phase : attaques ciblées

Le premier groupe d'utilisateurs *achètera* l'attaque et tirera partie de cette exclusivité pour l'exploiter sur des cibles stratégiques permettant un fort retour sur investissement. Les premières victimes des attaques 0day sont donc sans surprise :

- les banques,
- les industries stratégiques où le vol et la revente de données sont une réalité,
- les gouvernements / administrations / services publics,
- les organisations politiquement militantes (défense des droits de l'homme, organisation écologie etc.),
- Certaines entreprises ne pouvant pas se permettre d'interruption de service (marchés financiers etc.) où le racket, économiquement, se justifie

Cette première phase présentera donc une faible croissance du nombre de victimes mais aura des répercussions financières importantes.

Seconde phase : publication et croissance

Le second groupe d'utilisateurs n'achètera pas la vulnérabilité et attendre plutôt qu'elle tombe dans le domaine public. Grâce à la publication du POC, des acteurs non spécialisés automatiseront l'exploitation de l'attaque et lanceront alors une offensive massive sur des victimes indéfinies : particuliers, petites et grandes entreprises, organisations publiques. Les revenus attendus par attaque sont faibles, mais le volume colossal d'assauts générera des gains satisfaisants.

A ce stade, nous pouvons distinguer deux possibilités :

1. Le POC a été publié en même temps que le patch de l'éditeur ou
2. Le POC a été publié spontanément

Dans le premier cas, le correctif de l'application permet de bloquer l'exploitation de la faille. L'attaque connaîtra un succès important car le taux de déploiement de ce correctif sera initialement faible, mais elle rejoindra vite la troisième phase de sa vie : le déclin.

Dans le second cas, l'attaque produira des effets ravageurs car, bien que connue et diffusée massivement, elle ne bénéficiera toujours pas de correctif efficace.

Dans tous les cas, les éditeurs d'antivirus commenceront à fournir quelques contre-mesures sur base de signatures. Malheureusement, ne pouvant se concentrer efficacement que sur les payloads – et non la faille – ces technologies seront dépassées par l'extrême croissance du nombre de nouveaux payloads par jour. Suivre la cadence imposée par les packers du monde entier sera en pratique impossible. La courbe de croissance du nombre de victimes frémira certes quelque peu et finira même par infléchir, mais aucune décroissance ne sera permise par cette simple contre-mesure.

En conclusion, la seconde étape de la vie de l'attaque verra donc d'abord son expansion rapide et exponentielle, puis une croissance plus linéaire jusqu'à l'apogée de sa diffusion.

Troisième phase : le déclin

La fin de la phase 0day et le début du vrai déclin interviendra lors de la mise à disposition d'un correctif par l'éditeur du logiciel incriminé.

Le nombre de machines équipées du correctif allant croissant, il deviendra de moins en moins simple d'infecter les cibles. Cette phase sera donc caractérisée par un désintéressement progressif des assaillants au profit d'attaques plus récentes et plus efficace.

La bataille pour les machines qui n'auront pas bénéficié de la mise à jour corrective aura tout de même lieu : packers et éditeurs d'antivirus feront toujours la course à la signature. Comme dans la seconde phase, l'eff[illegible]contre-mesure reste re[illegible]ion

Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com

des packers permettra aux signatures de montrer quelque efficacité.
En définitive, seule l'augmentation du nombre de machines patchées finira par endiguer l'attaque jusqu'à atteindre la dernière phase : l'obsolescence.

Quatrième phase : obsolescence et presque-mort

Une attaque ne meurt jamais : certains assaillants se concentrent sur des cibles obsolètes et ne bénéficiant pas de mise à jour. Il n'est pas rare d'entendre qu'une organisation s'est faite attaquée au travers d'une faille corrigée depuis 3 ans, sur un logiciel ayant depuis sauté trois numéros version.
En dépit de ces quelques exploitations marginales, l'exploitation de la faille disparaîtra quasiment avec l'obsolescence du logiciel incriminé. Il paraît évident par exemple que le nombre d'attaque sur Windows 95 a fortement diminué ces dernières années...

Conclusion

Le cycle de vie des failles utilisables montre que la phase 0day de leur exploitation touche l'ensemble de la population : professionnels et particuliers sont susceptibles d'en être victimes. De même, il n'apparaît pas nécessaire de présenter un intérêt stratégique particulier pour être attaqué : la seconde phase du cycle se disperse indifféremment sur toutes les cibles voulant bien se présenter.

Siège Social
T : +33 (0)4 72 53 01 01 • F : +33 (0)4 72 53 12 60 •
1, place Verrazzano • 69009 Lyon •
S.A au capital de 5 491 228€ RCS Lyon 428 173 975
www.arkoon.net

SkyRecon Systems
T : +33 (0)1 57 63 67 00 • F : +33 (0)1 57 63 67 37 •
An Arkoon comany • Immeuble le Pelissier
220, Avenue Pierre Brossolette • 92240 Malakoff
www.skyrecon.com