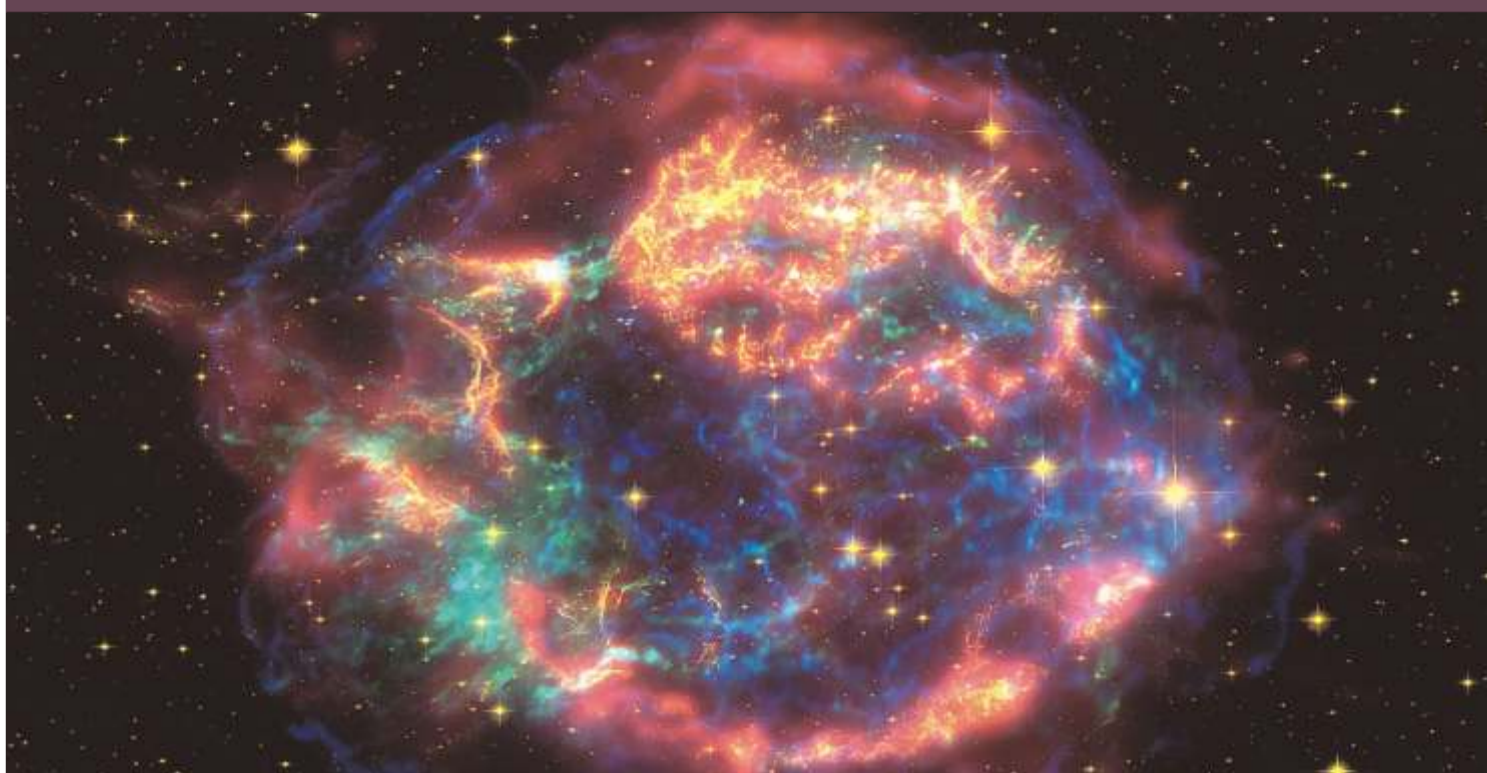


CASSIOPEE A OU LES SURSAUTS D'UNE ÉTOILE MOURANTE



Le télescope spatial Spitzer a capté un sursaut d'activité chez une étoile théoriquement morte. Cassiopee A est formé des restes d'une étoile devenue supernova qui a explosé il y a 325 ans; l'événement avait alors été observé par l'astronome Tycho Brahe. Cependant, un écho lumineux (infrarouge) témoigne d'une fin de vie agitée pour l'étoile à neutrons qui demeure au centre de Cassiopee A. D'après l'ampleur de l'écho, les chercheurs ont estimé qu'il résultait d'une éruption datant de 1953. Dans un article de «Science», les astronomes expliquent que Cassiopee A pourrait même être un magnétar, catégorie récemment définie d'étoiles mortes dont les surfaces sont parcourues de secousses et de ruptures laissant échapper de grandes quantités de rayons gamma.

NASA/JPL-CALTECH/IRAS/ESA

→ CIVILISATION DE 7000 ANS ←

Le quotidien britannique «The Independent» a révélé qu'une civilisation très ancienne aurait construit des dizaines de temples monumentaux il y a 7000 ans, soit environ 2000 ans avant la construction des pyramides d'Égypte et les mégalithes de Stonehenge. Des archéologues ont découvert plus de 150 temples sur une zone de 600 km de long, partagée entre l'Allemagne, l'Autriche, la Slovaquie et la République tchèque.

→ AUTOCENSURE EN CHINE ←

Après l'autocensure appliquée par Google et Yahoo!, c'est au tour de Microsoft de faire de même avec son nouveau portail chinois. Des expressions comme «indépendance de Taïwan», «Démocratie», «liberté», «droits de l'homme», «manifestations» ne pouvaient plus être utilisées lundi. Les internautes qui tentaient d'entrer ces mots se voyaient invités à en utiliser d'autres.

→ MAL DE L'ALTITUDE ←

La plus importante expédition scientifique suisse de ces dernières années est partie dimanche à l'assaut des 7546 mètres du Muztagh-Ata, un sommet situé dans l'ouest de la Chine, afin d'étudier sur le terrain le mal de l'altitude. L'expédition, qui doit durer cinq semaines, rassemble 38 alpinistes suisses et des médecins spécialistes du mal de l'altitude.

→ RIMONABANT CONTRE LE DIABÈTE ←

Selon les résultats d'une étude, le médicament Rimonabant, développé par le groupe pharmaceutique français Sanofi-Aventis, a des effets favorables sur la glycémie et les risques cardio-métaboliques chez les patients diabétiques de type 2. Il s'agit de la quatrième et dernière étude de la phase III d'un an, qui précède la commercialisation.

→ INFORMATIQUE

Ordinateurs et sécurité: à quand la protection totale?

Professionnalisation et rapprochement des différentes activités liées au piratage limitent la marge de manœuvre du particulier.

OLIVIER WIENER*

Votre antivirus est mis à jour toutes les 3 heures. Vous scannez régulièrement vos disques durs à la recherche de ces programmes qui vous causent tant de soucis. Et vous vous croyez à l'abri? Détrompez-vous! Même en effectuant ces deux opérations de manière très régulière, vous n'êtes pas protégés pour autant. Les pirates informatiques sont aux aguets, à la recherche de la moindre faille. Celui qui veut pénétrer vos secrets peut utiliser plusieurs méthodes. Une de ces techniques consiste par exemple à vous envoyer un «ver» par email. Si ce logiciel est connu et référencé par votre antivirus, pas de problème; si ce n'est pas le cas, les ennuis commencent assez vite...

Avec un peu de chance, et s'il est correctement installé, votre pare-feu ou antivirus détecte un programme inconnu et dangereux lorsqu'il tente de faire sortir des données vers internet, en général votre carnet d'adresse. Il est alors relativement facile de le bloquer et de nettoyer votre cher ordinateur. Malheureusement, la plupart du temps, vous ne vous rendez simplement compte de rien. Un bon pirate ne laisse en effet que rarement des traces de ses activités, et essaie généralement de rester le plus discret possible.

Du piratage à l'espionnage, il n'y a qu'un pas...

A part le défi technique, prendre le contrôle d'un ordinateur à distance, effacer des données ou effectuer des calculs nécessitant des processeurs puissants, sont des activités certainement moins intéressantes que de collecter des informations sensibles, des mots de passe ou le résumé de vos habitudes et intérêts sur des thèmes donnés. Ces informations ont une valeur, et une valeur substantielle même! Ainsi d'énormes intérêts et moyens motivent les pirates

puisque certaines sociétés sont prêtes à payer cher pour ce genre d'information. En plus, les liens qui unissent «hackers» et «spammers» ont été démontrés, notamment par la société Sophos. Les attaques des uns profitent aux autres, et ceux-ci peuvent ensuite, par effet ricochet, inonder de «pourriels» (courriers non désirés, ou spams) des millions d'adresses email. Lorsque l'on sait que les «meilleurs» spammers gagnent entre 400.000 et 600.000 dollars par mois, ce n'est pas étonnant qu'ils aient les moyens de financer quelques pirates... Selon ZDNet, un marché existe même dans ce domaine: la valeur

actuelle d'un ordinateur piraté est de 5 cents.

Les outils indépendants sont plus efficaces

Heureusement, quelques outils sont disponibles pour se protéger. Un bon antivirus et un bon pare-feu, vous l'aurez compris, ne suffisent plus. Il faut installer également de bons outils contre les logiciels espions, sans oublier un filtre antispams efficace. De manière générale, préférez les outils spécialisés (et indépendants) aux solutions «tout en un» qui peinent à démontrer leur efficacité. Bien entendu, ces logiciels sont mis à jour de

manière régulière. Et en cas de doute, utiliser son bon sens, en se posant la question: «Transposée au monde réel, est-ce que cette démarche paraîtrait suspecte?» Les plus grosses failles d'un système informatique ne résident souvent pas dans la technique, mais plutôt dans le comportement de ses utilisateurs. Les pirates ont compris qu'il était bien plus facile de s'appuyer sur certaines faiblesses de l'âme: naïveté, avidité ou curiosité par exemple. En effet, quel chef d'entreprise résisterait à la tentation de visiter le site d'un client potentiel (site qui contiendrait bien entendu un ver), et quel

employé ne serait pas intéressé par une promotion exceptionnelle, surtout si celle-ci lui a été transmise par le chef du personnel (un faux, bien entendu)? C'est souvent par email que débute ce type d'attaque. Ensuite, le simple fait de répondre, d'ouvrir la pièce jointe, ou de visiter le site enclenche la démarche... La parade réside donc aussi dans la prévention, l'information et la formation. Sensibilisés au risque, patrons et employés sont en effet bien mieux armés pour lutter contre ce fléau.

Entre paranoïa et schizophrénie

A l'heure actuelle, il semble bien que l'industrie informatique ne propose que deux choix: la paranoïa ou la schizophrénie. Pour ceux qui choisissent le premier, croisement des informations, double vérification, mises à jour systématiques des outils de protections, et contrôles réguliers des machines sont le lot quotidien. Pour les seconds, la séparation physique des machines connectées à internet devient inévitable, ainsi que son cortège de conséquences négatives: travaux à double, mises à jour rendues difficiles voire impossibles, transfert de données entre postes de travail laborieux, etc. Dans les deux cas, une procédure de sauvegarde rigoureuse des données est nécessaire pour contrer les effets extrêmes d'une attaque – mais nous entrons ici dans un autre débat. On le voit bien, la situation actuelle est inquiétante. Or seule une véritable volonté (et donc des moyens) au niveau international pourrait enrayer ce phénomène, ce qui n'est, visiblement et malheureusement, pas près de se produire dans l'immédiat.

→ * Fondateur de C2SP, Genève – www.c2sp.com. Retrouvez chaque mois cette rubrique consacrée à l'évolution de l'informatique et d'internet.

3 questions à Cédric Renouard

→ Chef de projet chez Illion

Créée en 2002 et basée à Genève, la société Illion est spécialisée dans la maîtrise des risques criminels (piratage informatique, criminalité financière, intrusion physique). Parmi ses clients, elle compte notamment des banques et des sociétés financières d'envergure internationale. Pour son chef de projet, seule une approche intégrant un ensemble de risques peut résister à une attaque bien organisée.

→ Pour une PME ou une multinationale, quels sont les types de risques que vous intégrez dans votre démarche?

Cédric Renouard: Il n'est plus suffisant aujourd'hui de ne se préoccuper que contre les dangers purement techniques. En effet, le patrimoine de l'entreprise est menacé par un ensemble de risques variés et complexes. Pour les contrer efficacement, il convient de bénéficier d'excellentes connaissances sur les méthodes des pirates professionnels. Mais il est aussi indispensable d'inscrire la prévention dans un contexte global et de comprendre les mécanismes de fraude financière ainsi que les faiblesses liées aux atteintes à la propriété.

Pourquoi, par exemple, surprotéger son réseau informatique, s'il est facile de s'introduire physiquement dans le bâtiment et de dérober un ordinateur portable sur un bureau? Cela correspondrait en fait à prévoir une porte blindée tout en laissant ses fenêtres grandes ouvertes!

→ Et ensuite?

Pour prévenir efficacement toute atteinte au patrimoine informationnel d'un client, nous commençons toujours par évaluer ses exigences en sécurité, de manière à déterminer l'instant à partir duquel une attaque n'est plus rentable. Pour chaque faille découverte, nous sommes ainsi capables d'évaluer précisément son risque financier propre, et de formuler les solutions les mieux adaptées pour corriger les carences mises en évidence. Par exemple, si une effraction à votre domicile vous causerait un préjudice maximum de 3 millions, et que la probabilité d'être cambriolé est de 10%, alors vos dispositifs et services de sécurité ne doivent pas coûter plus que 300.000 francs. Bien entendu, les processus de maîtrise du risque se doivent d'être constamment adaptés et optimisés, en fon-

ction des nouvelles techniques criminelles sans cesse imaginées. De surcroît, une fois que le risque d'atteinte au patrimoine informationnel est réduit à un niveau résiduel, nous sommes capables de le faire couvrir par une police d'assurance – dont la prime dépend naturellement de la maîtrise du risque déjà acquise.

→ Aujourd'hui, qui sont les pirates?

Le niveau de complexité technique, la connaissance des procédures internes des sociétés ciblées et le type de préjudices subis (extorsion, chantage, détournements, etc.) constituent autant de preuves évidentes d'une maîtrise de cette activité par le crime organisé. Pour ce qui est de la haute criminalité, la récente intrusion dans un établissement bancaire d'envergure internationale pour détourner un montant de 500 millions de dollars est un signe inquiétant, qui montre l'ampleur et les enjeux de cette thématique. D'autant que cette tentative n'a échoué, visiblement, que par méconnaissance de certains mécanismes non liés directement à la sécurité informatique, comme les contrôles antiblanchiment. – (OW)

L'AGEFI

VOUS PARTEZ EN VACANCES

MEMBRE VOUS SUIT PARTOUT

WWW.AGEFI.COM

Vous ne voulez pas recevoir un simple échantillon de L'AGEFI? Pour cela, communiquez-nous votre numéro personnel d'abonné, l'adresse de livraison temporaire du journal, et les dates de début et de fin. Faites votre demande soit par tél. +41 21 321 41 81, par mail. agefi@agefi.com, par fax +41 21 321 41 11. Expédition par poste uniquement.