【欧州連携センター情報】

2014 年８月 20 日

大規模なパスワード盗難事件が発生：ロシアのグループによる犯行

米サイバーセキュリティ会社のホールド・セキュリティは、ロシアのハッカー・グループが米国を含む各国の企業から約 12 億個の ID・パスワードのセットを盗んだと発表した。大企業から中小企業まで様々な規模の企業が運営する約 42 万のサイトから、ID とパスワードを盗難したという。グループは合計で 45 億セットを盗難したが、重複を除くと、5 億件の電子メールアカウントにリンクした 12 億セットが盗難された模様。

ホールド・セキュリティは、7 ヵ月間の調査の結果、この盗難を跡付けた。同社はこのグループを「CyberVor」（Vor はロシア語で盗人という意味）と命名。CyberVor はもとは、ブラック・マーケットで電子メールアドレスのリストを購入、それを元に、フィッシングをしたり、マルウェアに感染させるなどの犯行を繰り返していた。今年に入ってグループは手口を変化させ、やはりブラックマーケットでボットネットのデータアクセスを取得、ボットネットを構成するいわゆるゾンビ PC を足場に多数のサイトのセキュリティ検証を行い、SQL システムの脆弱性があるサイトを割り出し、そのセキュリティホールを通じてパスワードなどを盗難したという。

ホールド・セキュリティは、グループが取得したすべてのデータが利用可能というわけではないとしつつ、すべてのサイトに対し、SQL システムにセキュリティ・ホールがないか検証するよう勧告している。

（AFP 2014 年８月６日）

【原文】

Des pirates informatiques russes ont volé 1,2 milliard de mots de passe (Hold Security)
Origine : États-Unis
06/08/2014 06h47 GMT - USA-RUSSIE-PIRATAGE-TECHNOLOGIES-INTERNET-INFORMATIQUE - Service économique - AFP

WASHINGTON, 6 août 2014 (AFP) - Un groupe de pirates informatiques russes s'est emparé d'environ 1,2 milliard de mots de passe sur internet de sociétés américaines et étrangères à travers le monde, a indiqué mardi la firme Hold Security.
Les pirates ont mis la main sur les noms d'utilisateurs et les codes d'accès de quelque 420.000 sites internet, qui vont des plus grandes enseignes au plus petit site internet, souligne Hold Security dans un communiqué, confirmant une information du New York Times.

Au total, la masse de mots de passe récoltée par les pirates atteint 4,5 milliards, dont 1,2 milliard de "visiteurs uniques" permettant d'avoir accès à quelque 500 millions de comptes e-mail.
Hold Security précise être arrivée à ces conclusions après sept mois de recherches.
"Même si le groupe (de pirates) n'a pas de nom, nous l'avons surnommé +CyberVor+, +Vor+ signifiant +voleur+ en russe", a précisé Hold Security.
Dans un premier temps, "CyberVor" a racheté des données sur le marché noir, s'en servant ensuite pour pirater les sites en utilisant des pourriels et des virus redirigeant les utilisateurs des sites qu'ils utilisaient vers celui des pirates.

"Avec des centaines de milliers de sites touchés, la liste comprend les sites les plus importants dans tous les secteurs mais aussi des petits, voire des sites personnels", souligne Hold Security.
"4,5 milliards semble un chiffre énorme mais il faut penser au nombre de sites qui demandent une identification par courriel et presque tout le monde réutilise le même mot de passe plus d'une fois", souligne la société, tout en précisant que toutes les données dérobées par les pirates ne sont pas nécessairement encore utilisables.
Hold Security recommande à tous les sites de vérifier qu'ils n'ont pas été victimes d'une faille de leur système SQL (Structured Query Language, langage de requête structurée).
Selon le New York Times, cette intrusion, qui pourrait être la plus vaste jamais réalisée, est partie d'un groupe de pirates basés en Russie, quelque part entre le Kazakhstan et la Mongolie.
Selon le Times, les pirates, âgés d'une vingtaine d'années, ne seraient pas plus d'une douzaine.
rl/gde/jld/ggy

※和文作成にあたっては、ニュースソースである下記のサイトの情報を併せ参照。
http://www.holdsecurity.com