ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

آلوده شدن بازی Starscarft 2 توسط کرم Win32/Rebhip.A

تنظیم کننده:

سمانه غنی- سعیده نکوخیز

ویرایش: ۱

شماره سند: V-89/5-2

www.ircert.cc

ITRC

مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

کد آسیب پذیری: V-89/5-2

نام محصول آسیب پذیر: بازی Starscarft 2

نوع سیستم عامل: Windows 2000, ME, VISTA, 98, 95, XP

کشف توسط: MMPC

تاریخ کشف: 28 July 2010

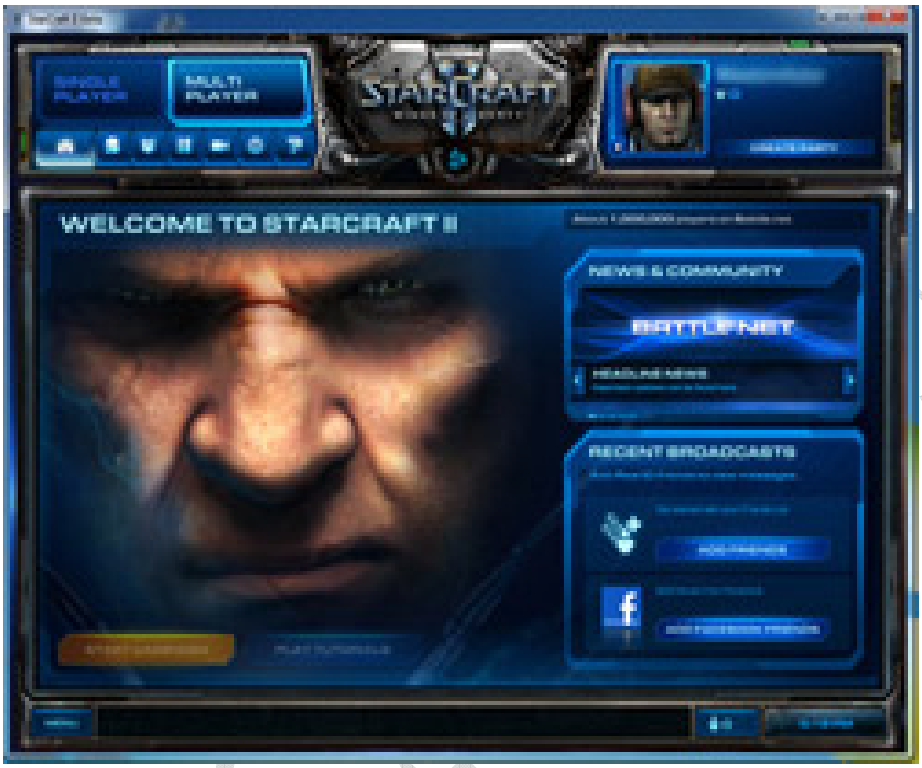
سطح خطر: متوسط

شرح:

در سال ۱۹۹۴ بود که شرکتی به نام Blizzard کار خود را برای انتشار نرم افزارهای سرگرمی (بازی) آغاز کرد و به سرعت به یکی از عامه پسندترین شرکت ها تبدیل شد. این شرکت با عرضه ی بازی هایی مثل War Craft خود را به دنیای بازی های رایانه ای معرفی کرد و چند جایزه به عنوان بهترین بازی سال دریافت کرده و اکنون با سرویس بازی های آنلاین خود (Battle.net) و با میلیون ها کاربر فعال در سراسر دنیا به بزرگ ترین شرکت در عرصه ی بازی های آنلاین تبدیل شده است.

بازی StarCraft II یک بازی مهیج با گرافیک مناسب و ساخت این شرکت می باشد. با توجه به اینکه این بازی سر و صدای زیادی در بین بازیکن ها داشت انتقاد های زیادی از آن صورت گرفت. این بازی مخالف و موافق های زیادی پیدا کرد و تنها دلیل آن سه‌گانه شدن بازی و همچنین حذف قابلیت LAN بازیکن ها بود که باعث شد از درجه ی این بازی کم شود.

هوش مصنوعی این بازی نسبت به نسخه قبلی و حتی War craft III خیلی بهتر شده و طبق گفته‌های Dustin Browder طراح ارشد بازی و هوش مصنوعی ان این بازی طوری طراحی شده که نمونه ی ان را در هیچ یک از بازی های هم سبک ندیده ایم.



این بازی برای PC عرضه شده و فعلا تصمیمی مبنی بر عرضه ی آن بر روی کنسول ها از سوی Blizzard گرفته نشده است. این بازی با ویندوز Vista و XP سازگاری کامل دارد و مانند بازی های دیگر Blizzard علاوه بر PC برای Mac هم توسعه داده می شود و همچنین بازی با DirectX 10 سازگار خواهد بود و با توجه به لوگوی معروف Havok می توانم بگوییم که این بازی از فیزیک Havok برای واقع گرایانه تر شدن بازی استفاده می کند و قادر است تا واحدهای بسیار بزرگ و با تعداد زیادی را ارائه دهد. همچنین در بازی ابزارهای scripting و Full map making نیز وجود دارد و به Player آزادی عمل زیادی می دهد.

Softpedia گزارش کرده است که مایکروسافت یک هشدار برای همه علاقه مندان به دریافت رایگان غیرقانونی نسخه های بازی StarCraft II صادر کرده است. فایل های جعلی با این بازی مرتبط شده اند که حاوی بدافزار می باشد.

این فایل های آلوده خدماتی را برای کدهای مخرب از منابع مختلفی مانند بیت تورنت ها و وب سایت هـای تخصصی فراهم می کنند. این بدافزار شامل کرم Win32/Rebhip.A می باشد که این کرم از طریق دستگاه های قابل جابه جایی گسترش پیدا می کند و از طریق ضربه زدن به کلید ورود به سیستم قـادر بـه سـرقت اطلاعات حساس از کامپیوتر می باشد.

این مسیر C:\Documents and Settings\[User]\Application Data یک مسیر متغییر است که حاوی یک پوشه از فایل های سیستمی است، که به عنوان یک مخزن مشترک برای داده های نرم افزارهای خاص می باشد.

اسامی مستعار کرم Win32/Rebhip.A به صورت زیر می باشد:

Generic PWS.di [McAfee]

Mal/Behav-328 [Sophos]

Trojan.Win32.Llac.bdm [Kaspersky Lab]

Malware.Spyrat [PC Tools]

W32.Spyrat [Symantec]

Mal/Behav-043, Mal/Behav-328, Mal/Behav-103 [Sophos]

Mal/Bifrose-S [Sophos]

Trojan Horse [Symantec]

Trojan.Generic [PC Tools]

Backdoor.Graybird [PC Tools]

Backdoor.Graybird [Symantec]

Backdoor.Win32.Delf.seq [Kaspersky Lab]

Backdoor.Win32.Poison.becc [Kaspersky Lab]

BackDoor-CEP.gen.au [McAfee]

Constructor:Win32/Bifrose.A [Microsoft]

Generic.dx!eus [McAfee]

Infostealer.Gampass [Symantec]

Mal/Behav-010 [Sophos]

Mal/Behav-010, Mal/Behav-024 [Sophos]

Mal/Behav-328, Mal/Behav-103, Mal/Behav-043 [Sophos]

Mal/Behav-328, Mal/Emogen-I [Sophos]

Mal/EncPK-LL, Mal/Behav-328 [Sophos]

Mal/Generic-A [Sophos]

Trojan.Win32.Llac.bcx [Kaspersky Lab]

Trojan.Win32.Llac.bju [Kaspersky Lab]

Trojan.Win32.Llac.ga [Kaspersky Lab]

Trojan.Win32.Scar.vuy [Kaspersky Lab]

Trojan-Dropper.Win32.Decay.eaf [Kaspersky Lab]

Trojan-Dropper.Win32.Decay.edw [Kaspersky Lab]

کرم Win32/Rebhip.A فایل های مخرب زیر را در سیستم اضافه می نماید:

- <system folder>\WinDefence\windefence32.exe
- <system folder>\taskmanager\task.exe
- <system folder>\install\system.exe
- <system folder>\backup\winbackup.exe
- <system folder>\windows\windows.exe
- %windir%\install\update.exe
- C:\Documents and Settings\<User>\Local Settings\ Temp\uuu.uuu
- C:\Documents and Settings\<User>\Local Settings\ Temp\xxx.xxx
-

کرم Win32/Rebhip.A از طریق کلیدهای زیر رجیستری را تغییر می دهد:

- HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer\Run C:\WINDOWS\system32\WinDefence\windefence32.exe"
- HKCU\Software\SlysBitch "FirstExecution" "<current date and time>" (for example: "21/12/2009 — 03:58″)
-

نحوه رفع مشکل:

یک برنامه ضد ویروس را بر روی سیستم کامپیوتر خود نصب نمایید.

به طور مرتب برنامه ضد ویروس نصب شده بر روی سیستم کامپیوتر خود را بروز رسانی نمایید.

در صورت شناسایی این کرم توسط برنامه های ضد ویروس آن را از سیستم خود حذف نمایید.

از دریافت غیرقانونی نسخه های رایگان بازی StarCraft II خودداری نمایید.

منابع:

http://blogs.pcmag.com/securitywatch/2010/07/pirated_copies_of_starcraft_2.php

http://www.im-infected.com/worm/wormwin32rebhip-a.html

http://www.threatexpert.com/threats/worm-win32-rebhip-a.html

http://www.scanforfree.com/80/worm-win32-rebhip-a-removal.html

مرکز آپای دانشگاه شیراز