آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

تحلیل فنی بدافزار اَبسون‌کین[1]

گروه تحلیل بدافزار مرکز آپا دانشگاه بین‌المللی امام خمینی (ره)

۱۷ اردیبهشت ۱۳۹۸

[1] Absonkaine.

مقدمه

بدافزار[۲] برنامه‌ای رایانه‌ای با هدف ایجاد آزار یا خسارت برای کاربران در فضای مجازی است. برخی از بدافزار صرفا به دنبال اذیت قربانیان خود با انجام کارهایی نظیر تکرار فراوان یک پردازش هستند. این در حالی است که هدف برخی دیگر از آنها ایجاد خسارت‌های مختلف در حوزه‌های نرم‌افزار، سخت افزار یا اطلاعات قربانیان است.

نوع بدافزار:

پس از بررسی‌های صورت گرفته بدافزار آبسون‌کین یک باج‌افزار تشخیص داده شده است. باج‌افزارها گونه‌ای از بدافزارها با هدف ایجاد محدودیت دسترسی در سیستم‌های قربانی بوده که برای حذف مشکلات پدید آمده از کاربر درخواست باج می‌کند. برخی از آن‌ها تنها روی فایل‌های دیسک‌سخت رمزگذاری کرده و برخی دیگر سیستم قربانی را قفل می‌کنند. پس از این فرآیند یک پیام روی نمایشگر قربانی نمایش داده شده که از کاربر واریز مبالغی را جهت حذف محدودیت‌ها درخواست می‌کند. شاخص مبالغ و پرداختی‌های باج‌افزار معمولاً با ارزهای دیجیتالی نظیر بیت کوین مشخص می‌شود. البته برخی از باج‌افزارهای جدید پرداخت هزینه‌های خود را از طریق کارتهای هدیه آیتونز[۳] و یا آمازون نیز انجام می‌دهند. لازم به ذکر است که بر اساس تجربه پرداخت باج ، ضمانت بازگشایی رمز یا ارسال ابزار برای بازگرداندن فایل‌ها (یا دسترسی به سیستم آلوده) را برای کابر فراهم نخواهد ساخت.

ارزیابی نحوه‌ی شیوع و عملکرد باج‌افزار آبسون‌کین:

باج‌افزار آبسون‌کین از طریق هرزنامه‌های حاوی پیوست‌های آلوده یا با استفاده از آسیب پذیری‌های موجود در سیستم عامل یا نرم‌افزارها منتشر می‌شود. مجرمان سایبری با استفاده از یک پست‌الکترونیکی با اطلاعات سرآیند جعلی از شرکت‌های حمل و نقلی مانند DHL یا FedEx سعی بر فریب قربانیان خود می‌کنند. متن پست‌الکترونیکی از تلاش ناموفق شرکت‌های مذکور برای تحویل یک بسته به قربانی حکایت دارد. فرآیندی که معمولا کنجکاوی افراد را به دنبال داشته و منجر به کلیک آن‌ها بر روی پیوست‌های مخرب می‌گردد.

[۲] Malware

[۳] iTunes

این باج‌افزار تمام سیستم‌های ویندوز موجود از جمله‌های نسخه‌های ۷، ۸،۱ و ۱۰ را هدف قرار می‌دهد. آبسون‌کین پس از ورود به سیستم قربانی با یک نام تصادفی خود را در مسیر *%AppData%* یا *%LocalAppData%* ایجاد می‌کند. فایلی که پس از اجرا تمام حافظه دستگاه قربان را برای رمزگذاری فایل‌هایی با پسوند خاص جستجو می‌کند. این پسوندها شامل اسناد کاربردی مهم و فایل‌هایی با فرمت .doc، .docx، .xls، .pdf و غیره هستند. با شناسایی و رمزگذاری، فرمت هر یک از فایل‌ها به ".phoenix" تغییر یافته و دیگر کاربران قادر به اجرا و مشاهده آن‌ها نخواهند بود. پس از این فرآیند یک پیام باج‌خواهی به منظور بازگشایی فایل‌ها به قربانیان نمایش داده شده و از آن‌ها درخواست برقراری ارتباط با یک پست الکترونیکی را می‌کند (absonkaine@aol.com). در مکاتبه قربانی با این پست الکترونیکی میزان باج بر اساس بیت‌کوین مشخص می‌گردد.

پس از فرآیند رمزگذاری فایل‌های قربانی، این بدافزار فایل اجرایی خود را حذف اما زمینه‌ی ماندگاری را بر روی سیستم قربانی فراهم می‌کند. در واقع این بدافزار خود را در لیست برنامه‌های شروع ویندوز قرار داده و رفتارهایی مشابه با سرقت[۴] اطلاعات شخصی از خود بروز می‌دهد. متاسفانه تاکنون ابزار موثری برای رمزگشایی فایلهای آلوده معرفی نشده اما استفاده از ابزارهای بازیابی اطلاعات در برخی موارد می‌تواند مفید باشد.

[۴] Stealing personal data

شکل ۱- پیام باج خواهی بدافزار آبسون‌کین

تحلیل ایستا

در تحلیل ایستا سعی بر بررسی اطلاعات بدافزار بدون اجرای آن و تنها از طریق بازگشایی کُد/ دیس‌اسمبلر[۵] خواهد شد. در این روش می‌توان با کمک ابزارهای دیس‌اسمبلر و نرم‌افزارهای بررسی ساختار سرآیند اجرایی اطلاعات خوبی را بدست آورد.

.مشخصات فایل اجرایی:

در جدول زیر مشخصات فایل اجرایی و نتایج حاصل از توابع مختلف درهم‌سازی باج‌افزار آبسون‌کین ذکر شده است:

نام فایل	Absonkaine.exe
نوع داده	Win32 EXE
اندازه فایل	71 KB (72704 bytes)
زبان	C++
کامپایلر	Visual Studio 2010 SP1
MD5	62d3580c88222c59a276a2df8445758c
SHA-1	8a707b397796972317bcaa55bdef23b305824840
SHA-256	3bbac55728d38c1bcaac6b6fece73fb7a66ac3a0a71093bcacd4577c351db989
SSDEEP	1536:RFOPbkyoTwtPto0Rl0DsN9/zLec5oGFACZrqdKQNYDwOozDmAU:RYPxAwtPtoe/zLaGmCZrqcQSsznU

جدول ۱ : مشخصات فایل اجرایی بدافزار آبسون‌کین

[۵] Disassemble.

اطلاعات فایل اجرایی قابل حمل[۶]:

فایل اجرایی قابل حمل قالب اصلی فایل‌های قابل اجرا در ویندوز بوده و در همه‌ی سکوهای وین۳۲[۷] قابل اجراست. در واقع بارکننده فایل اجرایی قابل حمل در هر سکوی وین۳۲، قابل تشخیص بوده حتی زمانی که ویندوز از پردازنده‌ای غیر از اینتل[۸] استفاده می‌کند. اطلاعات موجود در رکوردهای کنترلی و سرآیند یک فایل اجرایی می‌تواند نکات زیادی را در مورد نحوه‌ی سازماندهی فایل مورد نظر مشخص کند. در ادامه نتایج بررسی های صورت گرفته بر فایل اجرایی باج‌افزار آبسون‌کین آورده شده است.

اطلاعات موجود در سرآیند[۹]:

ماشین مقصد	Intel 386 or later processors and compatible processors
تاریخ کامپایل	2019-03-21 12:42:34
نقطه شروع	26002
تعداد بخش‌ها	6

جدول ۲ : اطلاعات موجود در سرآیند فایل اجرایی بدافزار آبسون‌کین

[۶] Portable Executable.
[۷] Win32.
[۸] Intel.
[۹] Header.

فایل اجرایی این بدافزار دارای ۵ بخش[۱۰] است، که مشخصات آنها در جدول زیر ذکر شده است:

نام بخش	آدرس مجازی	اندازه مجازی	اندازه خام	آنتروپی	MD5
.text	۴۰۹۶	۳۹۲۴۰	۳۹۴۲۴	۶,۵۳	5b5a16464fe3da5ed9205c7fa39498ee
.rdata	۴۵۰۵۶	۹۷۹۲	۱۰۲۴۰	۴,۷۷	22a87ecc4c6bb581558598241a04c858
.data	۵۷۳۴۴	۷۷۴۸	۴۶۰۸	۴,۲۲	82ac11b8597a8ec8fd4581d7ed682d51
.rsrc	۶۵۵۳۶	۴۳۶	۵۱۲	۵,۰۹	27a705a02aee3351e851d9a3f4e2749a
.reloc	۶۹۶۳۲	۲۷۰۶	۳۰۷۲	۵,۲۱	271cd188a14b5fffa48cebc766f1bb68
.cdata	۷۳۷۲۸	۱۳۴۱۲	۱۳۸۲۴	۷,۸۷	50428e7518bdaf4b485564401e1a2656

جدول ۳ : بخش‌های مختلف فایل اجرایی بدافزار آبسون‌کین

توابع ورودی:

کتابخانه‌های پویای دی.ال.ال.[۱۱] یک ساختار استاندارد برای برنامه‌های ویندوز مایکروسافت است (فایل‌های lib و ocx و drv هم تقریباً مشابه دی.ال.ال. هستند). این فایل‌ها شامل توابع، کدها و منابع (تصویر، آیکون و غیره) مورد نیاز برای توسعه‌دهندگان و برنامه‌نویسان هستند. از دیگر خواص آن‌ها می‌توان به استفاده همزمان چندین برنامه کاربردی از یک کتابخانه اشاره کرد. طبق بررسی‌های صورت گرفته، باج‌افزار آبسون‌کین از دی.ال.ال. های زیر به عنوان توابع ورودی فایل اجرایی بهره می‌برد.

[۱۰] Section.

[۱۱] Dynamic-Link Library

عنوان توابع ورودی	توصیف عملکرد
ADVAPI32.dll	توابع و فراخوانی‌های امنیتی را برای دستکاری رجیستری ویندوز فراهم می‌کند.
KERNEL32.dll	برای برنامه های بسیاری از API های پایه Win32، امکان مدیریت حافظه، عملیات ورودی/ خروجی (I / O)، ایجاد نخها و پردازش‌ها، هماهنگ سازی توابع را فراهم می‌کند.
MPR.dll	فایل mpr.dll یک جزء نرم‌افزاری از سیستم عامل ویندوز مایکروسافت است.این کتابخانه سیستم عامل را قادر به تفسیر اطلاعات مربوط به ارائه دهندگان شبکه می‌سازد. علاوه بر کمک به برقراری اتصالات امکان اولویت‌بندی و گزینه‌های اضافی پیکربندی نیز توسط این کتابخانه انجام می‌شود.
SHELL32.dll	فایل shell32.dll یک جزء نرم‌افزاری از سیستم عامل ویندوز مایکروسافت است. ویندوز شل به عنوان رابط کاربری گرافیکی برای سیستم عامل های ویندوز عمل کرده و برخی از توابع API Windows Shell را کنترل می کند.
USER32.dll	USER32.DLL جزئی از Windows USER را اجرا کرده که برنامه‌ها از آن برای عملیات‌هایی مانند ایجاد و مدیریت پنجره‌ها، دریافت پیام‌های پنجره (که عمدتا ورودی کاربر مانند رویدادهای ماوس، صفحه کلید و یا اطلاعیه‌های سیستم عامل است)، نمایش متن در یک پنجره و نمایش پیام جعبه‌ها استفاده می‌کنند.
WS2_32.dll	این کتابخانه توابع شبکه TCP / IP و سازگاری با دیگر API های شبکه را فراهم می کند.

جدول ۴ : کتابخانه‌های دی.ال.ال. مورد استفاده توسط باج‌افزار آبسون‌کین

فایل اجرایی باج‌افزار آبسون‌کین ، دارای یک فایل منبع با مشخصات ذکرشده در جدول زیر است.

نوع	RT_MANIFEST
سایز	۳۴۶ بایت
زبان	English - United States
آنتروپی	۴,۸۰

جدول ۵ : مشخصات فایل منبع موجود در بدافزار آبسون‌کین

تحلیل پویا:

در این روش با اجرای بدافزار مربوطه بر یک سیستم و بررسی رفتار آن سعی بر جمع‌آوری اطلاعات نحوه ی اجرا و تاثیرات بدافزار بر روی عملکر سیستم خواهد شد. تحلیل‌های این بخش براساس اجرای باج‌افزار آبسون‌کین در محیط محافظت شده‌ی ماشین مجازی ویندوز ۷ (۳۲ بیتی) بدست آمده است. نتایج حاصل از رصد فعالیت‌های فایل سیستم این باج‌افزار به صورت زیر است.

فایلهای مورد استفاده:

- C:\WINDOWS\system32\winime32.dll
- C:\WINDOWS\system32\ws2_32.dll
- C:\WINDOWS\system32\ws2help.dll
- C:\WINDOWS\system32\psapi.dll
- C:\WINDOWS\system32\imm32.dll
- C:\WINDOWS\system32\lpk.dll
- C:\WINDOWS\system32\usp10.dll
- C:\WINDOWS\system32\shell32.dll
- C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
- C:\WINDOWS\WindowsShell.Manifest
- C:\WINDOWS\system32\comctl32.dll

فعالیت‌های رجیستری:

رجیستری[۱۲] یک پایگاه داده داخلی در سیستم عامل ویندوز مایکروسافت بوده که از نسخه ان.تی. این سیستم عامل به بعد وظیفه حفظ تنظیمات و پیکربندی‌های ویندوز و برنامه‌های کاربردی را بر عهده دارد. رجیستری اطلاعات را به صورت‌های گوناگون مثل باینری[۱۳] در پایگاه داده خود ذخیره کرده و هر برنامه کاربردی نصب شده در صورت عدم وجود محدودیت از طرف مدیر سیستم[۱۴] می‌تواند از اطلاعات آن استفاده کند. برنامه‌های کاربردی می‌توانند اطلاعات عمومی خود را در رجیستری ویندوز ذخیره کرده تا توسط خود برنامه یا سایر موارد، مورد استفاده قرار گیرد.

[۱۲] Registry.
[۱۳] DWORD.
[۱۴] Administrator.

این باج‌افزار کلیدهای رجیستری زیر را باز می‌کند.

- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
- \Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
- \Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
- \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\Transparent Enabled
- \REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MPR.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHELL32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\comctl32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KERNEL32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msvcrt.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2HELP.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2_32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHLWAPI.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PSAPI.DLL
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\winime32.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM32.DLL
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USP10.dll
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LPK.DLL
- \REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe\RpcThreadPoolThrottle
- \REGISTRY\MACHINE\Software\Policies\Microsoft\Windows NT\Rpc

ماندگاری در سیستم:

با ارزیابی‌های صورت گرفته باج‌افزار مذکور فعالیت‌های زیر را برای حفظ ماندگاری خود در سیستم انجام می‌دهد:

- تغییر در تنظیمات یا ایجاد یک مقدار در رجیستری به منظور قابلیت اجرای خودکار
- تغییر در تنظیمات دیواره آتش
- حذف و پایان بسیاری از فرآیندها
- غیرفعال‌سازی شناسایی خطا در هنگام بوت سیستمی (معمولا برای پنهان‌سازی تغییرات سیستم استفاده می‌شود)
- خود را در لیست برنامه‌های شروع[۱۵] قرار می‌دهد.

تجزیه و تحلیل ترکیبی

نتایج حاصل از مشاهده فعالیت فرآیند و سرویس‌های باج‌افزار به قرار زیر است:

- Absonkaine.exe (PID: 3124)
  - Absonkaine.exe (PID: 748)
    - cmd.exe (PID: 3796)
      - netsh.exe (حساب فعلی دیوار آتش را خاموش می‌کند) (PID: 312)
      - netsh.exe (opmode دیوار آنش را غیرفعال می‌کند) (PID: 2172)
    - cmd.exe (PID: 3316)
      - vssadmin.exe (PID: 2160)
      - WMIC.exe (PID: 756)
      - bcdedit.exe bcdedit /set {default} غیرفعال‌سازی خطای بوت (PID: 1252)
    - mshta.exe "%USERPROFILE%\Desktop\info.hta" (PID: 3048)
    - mshta.exe "%PUBLIC%\desktop\info.hta" (PID: 3356)
    - mshta.exe "C:\info.hta" (PID: 3352)
    - cmd.exe (PID: 3472)
      - vssadmin.exe (PID: 3656)
      - WMIC.exe (PID: 4080)
      - bcdedit.exe bcdedit /set {default} غیرفعال‌سازی خطای بوت (PID: 3828)

[۱۵] Start up

تحلیل ترافیک شبکه:

بررسی ترافیک شبکه، یکی از راه‌های بررسی عملکرد بدافزارهاست. نتایج تحلیل شبکه باج‌افزار آبسون‌کین به صورت زیر می‌باشد:

تحلیل ترافیک شبکه	
درخواست‌های DNS	هیچ درخواست DNS مرتبط ارسال نشده است.
تماس گرفتن با میزبان‌ها[۱۶]	با هیچ میزبان مرتبطی تماس نمی‌گیرد.
ترافیک HTTP	هیچگونه درخواست HTTP ساخته نمی‌شود.

جدول ۶ : ترافیک شبکه در بدافزار آبسون‌کین

[۱۶] Hosts

تشخیص روش‌های بدافزار

شاخص	عملکرد
اجرا	• باز کردن service control manager • ارجاع دادن به WMI/WMIC[۱۷] • دستیابی به اطلاعات سیستم از طریق WMIC
ماندگاری	• تغییر در تنظیمات یا ایجاد یک مقدار در رجیستری به منظور قابلیت اجرای خودکار
افزایش امتیاز	تزریق در فرآیند: • نگارش داده در یک فرآیند راه دور
دفاع	حذف فایل: • حذف نسخه‌های کامل ماشین مجازی[۱۸] (اغلب توسط باج‌افزارها انجام می‌شود) تغیر رجیستری: • تغیرات در تنظیمات پراکسی و تغیر در خدمات ویندوز تزریق در فرآیند: • نگارش داده در یک فرآیند راه دور
کشف	کشف دستگاه های جانبی : • جستجوی اطلاعات مربوط به حجم کل دیسک‌سخت درخواست‌های رجیستری: • بررسی اطلاعات زبان‌های مورد پشتیبانی • بررسی پرسش‌های امنیتی تنظیمات حساس IE • بررسی نام فعال رایانه • بررسی GUID ماشین رمزنگاری • جستجوی تنظیمات پنهان اینترنت (اغلب برای مخفی سازی رد پا در index.dat یا حافظه اینترنت استفاده می شود)

جدول ۷ : روش‌های مورد استفاده در بدافزار آبسون‌کین

[۱۷] Windows Management Instrumentation

[۱۸] volume snapshot

خروجی سامانه ویروس‌توتال[۱۹] :

ویروس‌توتال (متعلق به شرکت گوگل) برای پویش فایل‌های مشکوک به آلودگی توسط بدافزارها مورد استفاده قرار می‌گیرد. دراین وبگاه بیش از ۷۰ ضد ویروس مختلف برای پویش فایل‌ها تدارک دیده شده‌اند. با بررسی صورت گرفته در حال حاضر ۵۴ مورد از ۷۲ ضد ویروس موجود در سامانه ویروس‌توتال قادر به شناسایی این باج‌افزار بوده و آن را حذف یا غیرفعال می‌کنند. متاسفانه هنوز ابزاری مناسب برای رمزگشایی فایل‌های آسیب‌دیده توسط این باج‌افزار شناسایی نشده است.

Acronis	Suspicious	Ad-Aware	Trojan.Agent.DVAM
AegisLab	Trojan.Win32.Generic.4lc	AhnLab-V3	Malware/Win32.Generic.C3132305
Alibaba	Trojan:Win32/Phobos.26f985c6	ALYac	Trojan.Ransom.Phobos
Antiy-AVL	Trojan/Win32.Agent	Arcabit	Trojan.Agent.DVAM
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira	TR/Crypt.XPACK.Gen8	BitDefender	Trojan.Agent.DVAM
ClamAV	Win.Malware.Phobos-6938235-0	CrowdStrike Falcon	Win/malicious_confidence_80% (W)
Cybereason	Malicious.c88222	Cylance	Unsafe
Cyren	W32/Trojan.XFVB-3292	DrWeb	Trojan.PWS.Banker1.30220
Emsisoft	Trojan.Agent.DVAM (B)	Endgame	Malicious (high Confidence)
eScan	Trojan.Agent.DVAM	ESET-NOD32	A Variant Of Win32/Filecoder.Phobos.A
F-Secure	Trojan.TR/Crypt.XPACK.Gen8	FireEye	Generic.mg.62d3580c88222c59
Fortinet	W32/Phobos.Altr.ransom	GData	Trojan.Agent.DVAM
Ikarus	Trojan-Ransom.Phobos	Jiangmin	Trojan.Agent.bxfx
K7AntiVirus	Trojan (0054aab01)	K7GW	Trojan (0054aab01)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.Phobos
MAX	Malware (ai Score=100)	McAfee	RDN/Generic.grp
McAfee-GW-Edition	BehavesLike.Win32.Fujacks.lh	Microsoft	Trojan:Win32/Occamy.C
NANO-Antivirus	Trojan.Win32.Banker1.fondvt	Palo Alto Networks	Generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.815
Rising	Trojan.Filecoder!8.68 (CLOUD)	SentinelOne	DFI - Suspicious PE
Sophos AV	Mal/Generic-S	Sophos ML	Heuristic
Sophos AV	Mal/Generic-S	Sophos ML	Heuristic
Symantec	Downloader	Tencent	Win32.Trojan.Filecoder.Wpjn
TrendMicro	TROJ_GEN.R020C0WDE19	TrendMicro-HouseCall	TROJ_GEN.R020C0WDE19
VBA32	TrojanRansom.Blocker	VIPRE	Trojan.Win32.GenericIBT
ViRobot	Trojan.Win32.Ransom.72192.A	Webroot	W32.Adware.Gen
Zillya	Trojan.Agent.Win32.1084051	ZoneAlarm	HEUR:Trojan.Win32.Generic

شکل ۲ : خروجی وبگاه VirusTotal برای بدافزار آبسون‌کین

[۱۹] VirusTotal: Virustotal.Com.