باسمه تعالی

ZombieBoy ، بدافزاری با عملیات ماینینگ

فهرست مطالب

۱ مقدمه

در سال‌های اخیر به خصوص سال ۲۰۱۸، مجرمین قابلیت انتقال و استخراج پول الکترونیکی یا همان mining را به عنوان مولفه‌ی جدید به فایل‌های مخرب خود اضافه کرده‌اند. Crypto mining روندی است که در طی آن تراکنش‌های bitcoin و یا دیگر پول‌های الکترونیکی نظیر Monero انجام، تایید و بررسی می‌شوند. از این طریق مقداری پاداش به انجام‌دهنده تراکنش اعطا می‌شود. هر شخصی با دسترسی به اینترنت و منابع سخت‌افزاری لازم قادر به شرکت در این فرایند است.

بدافزارهای همراه با cryptocurrency در انواع و اشکال مختلف وجود دارند. باج‌افزارها، بدافزارهای mining، و cryptojacker[1]ها انواع مختلف آن هستند که نشان می‌دهند خطر ایجاد شده توسط آن‌ها روز به روز در حال افزایش است. هر سه نوع نام برده شده ارتباط نزدیکی با cryptocurrency دارند، که در مقایسه با انواع دیگر، وجه مزیت گمنامی را فراهم می‌کند. این پیشرفت در ارتباط بدافزارها با cryptocurrency قابل درک است. افزایش قابل توجه ارزش بسیاری از cryptocurrencyها باعث شده است که cryptomining در مقایسه با باج‌افزارها سودآوری بالاتری برای مجرمان سایبری داشته باشد، زیرا در برابر باج‌افزارها بسیاری از کاربران مبلغی پرداخت نمی‌کنند، بلکه با استفاده از backup فایل‌های خود را بازیابی می‌کنند. در نتیجه آلوده کردن سیستم به باج‌افزار تضمینی برای دریافت پول نیست، در حالی که miner بلافاصله بعد از نصب شروع به کار می‌کند و با استفاده از امکانات سخت‌افزاری سیستم کاربر به تولید درآمد برای مجرم سایبری می‌پردازد. در حالی‌که باج افزارها همچنان خطر مهمی تلقی می‌شوند، اما حملات بدافزار cryptomininig بسیار شایع‌تر از باج افزارها می‌باشد.

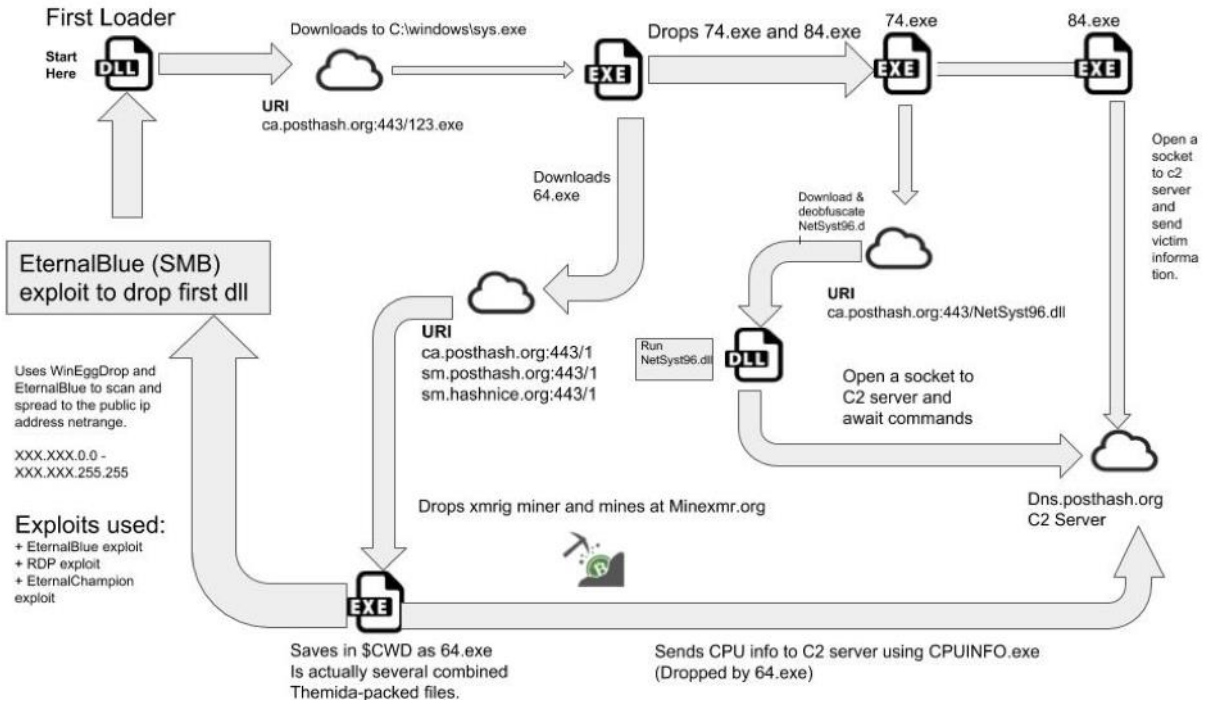
در ادامه، روند تولید بدافزارهای cryptomining خانواده دیگری از این بدافزارها به تازگی منتشر شده است که تشابه زیادی با بدافزار massminer که چند ماه پیش کشف شد دارد. این بدافزار به دلیل ابزاری که برای نشاندن قسمت اولیه بدافزار استفاده می‌شود و ZobmieBoyTools نام دارد، ZombieBoy نامیده شده است.

بدافزار مورد اشاره همانند MissMiner یک کرم ماینر پول الکترونیکی است که با استفاده از اکسپلویت هایی در سراسر اینترنت منتشر می‌شود. برای جستجوی هاست‌های آسیب‌پذیر در یک شبکه، ZombieBoy از ابزاری به نام WinEggDrop استفاده می‌کند. ابزار جستجو در MassMiner،

[1] Cryptojacker بد افزاری است که بدون آگاهی کاربران از سیستم آن ها برای عملیات crypto mining استفاده می کند.

MassScan نام داشت. بدافزار ZombieBoy مدام در حال بروزرسانی است و هر روز نسخه جدید و بهبود یافته‌ای از آن منتشر می‌شود.

روند کلی اجرای این بدافزار به شرح زیر است:



شکل ۱ – روند کلی اجرای بدافزار ZombieBoy

۲ دامنه‌ها

این بدافزار از چندین فایل سرور HTTP (HFS) برای نگهداری payload و بارگزاری آن در هاست قربانی استفاده می‌کند. URL هایی که بدافزار با آن‌ها برای دریافت payload ارتباط برقرار می‌کند تا این لحظه به شرح زیر است:

- ca.posthash.org:۴۴۳/
- sm.posthash.org:۴۴۳/
- sm.hashnice.org:۴۴۳/

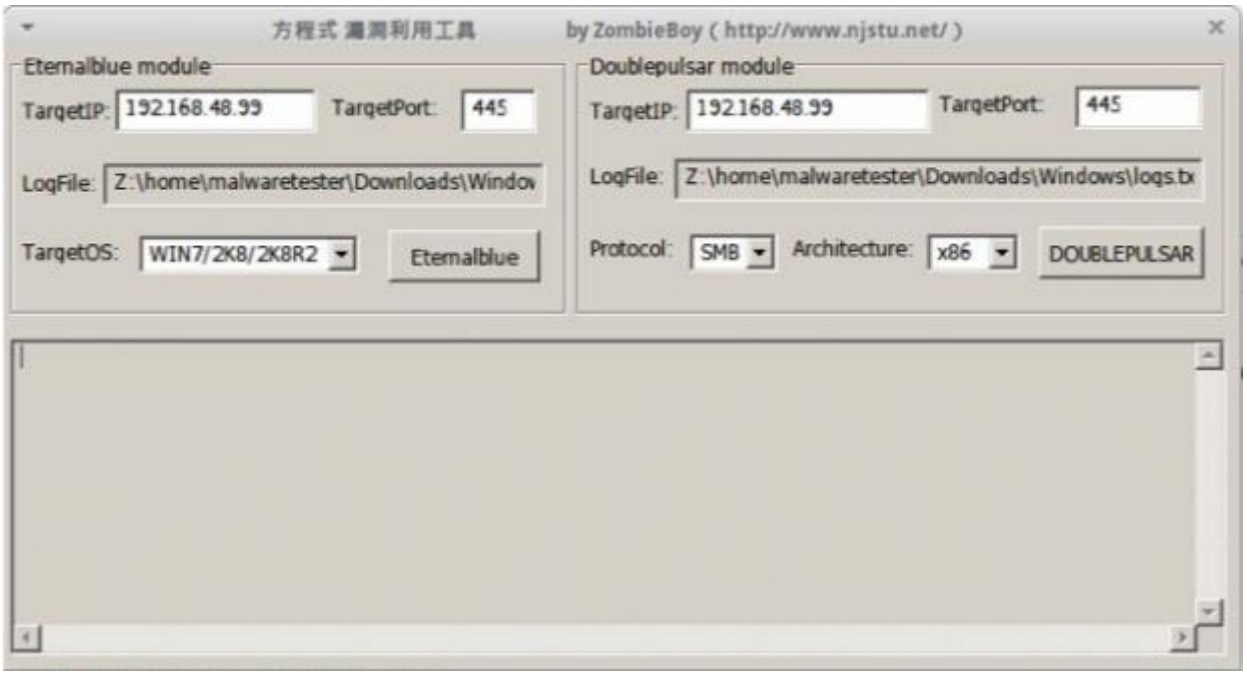
همچنین یک سرور دستور و کنترل (C&C) نیز دارد که آدرس آن dns.posthash.org می‌باشد.

این بدافزار از اکسپلویت‌های زیر به منظور نفوذ به سیستم قربانی استفاده می‌کند:

- CVE-۲۰۱۷-۹۰۷۳, RDP vulnerability on Windows XP and Windows Server ۲۰۰۳
- CVE-۲۰۱۷-۰۱۴۳, SMB exploit
- CVE-۲۰۱۷-۰۱۴۶, SMB exploit

۳ عملیات نصب بدافزار

بدافزار ZombieBoy نخست از اکسپلویت‌های EternalBlue/DoublePulsar به منظور نصب فایل DLL اصلی در سیستم قربانی استفاده می‌کند. برنامه‌ای که برای نصب این دو اکسپلویت استفاده می‌شود ZombieBoyTools نام دارد و به نظر می‌رسد که اصالتا چینی است زیرا زبان اصلی آن چینی است و همچنین برای توسعه یک سری بدافزار چینی (نظیر نسخه IRONTIGER APT از بدافزار Gh۰stRAT) مورد استفاده قرار گرفته است.

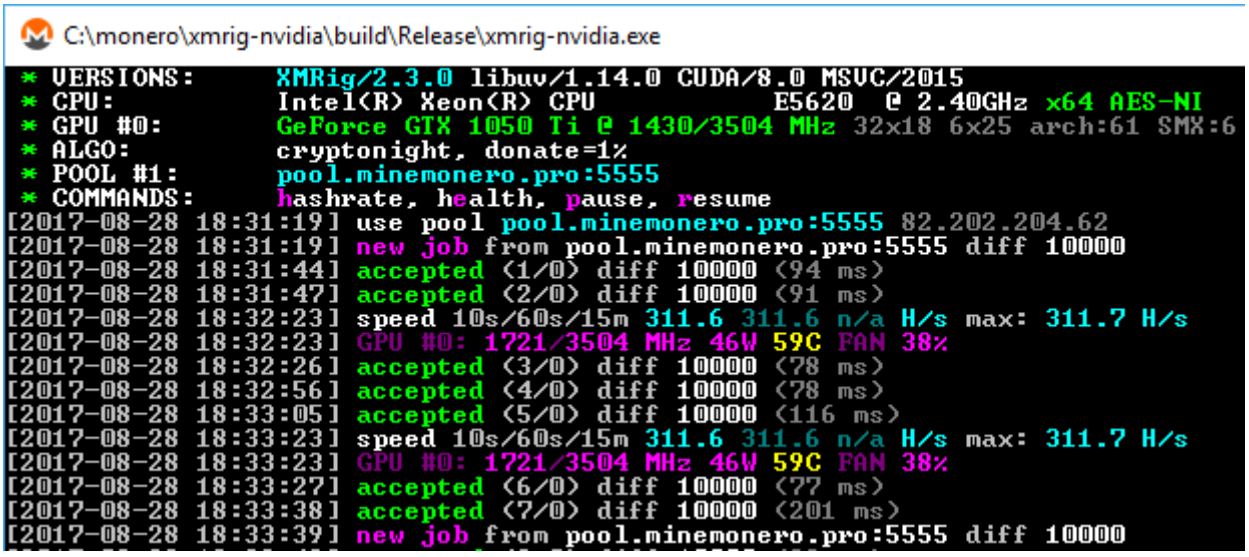


شکل ۲- تصویر ابزار ZombieBoyTools

بعد از اینکه اکسپلویت DoublePulsar با موفقیت اجرا شد، اولین فایل مربوط به بدافزار که یک dll است اجرا می‌شود. این dll خود فایل ۱۲۳.exe را از آدرس ca.posthash.org:۴۴۳ دریافت و در محل C:\%WindowsDirectory%\sys.exe ذخیره و سپس اجرا می‌کند.

۴ راه‌اندازی

فایل ۱۲۳.exe عملیات مختلفی پس از اجرا انجام می‌دهد. نخست، مولفه اول را از فایل سرور توزیع‌کننده آن دانلود می‌کند. با توجه به تحلیل کد درون ۱۲۳.exe نام فایل مولفه اول ۶۴.exe می‌باشد. اما پس از بارگزاری بر روی کامپیوتر قربانی به boy.exe تغییر نام می‌دهد. پس از بارگذری و ذخیره این مولفه، ۱۲۳.exe آن را اجرا می‌کند. کار اصلی مولفه ۶۴.exe توزیع مجدد بدافزار بر روی دیگر سیستم‌ها و همچنین اجرای ماینر پول الکترونیکی به نام XMRIG است.



شکل ۳ – نرم افزار ماینینگ XMRIG

علاوه بر این مولفه، ۱۲۳.exe دو مولفه دیگر به نام ۷۴.exe و ۸۴.exe را نیز دانلود و اجرا می‌کند. مولفه ۷۴.exe به نام scvhost.exe و در مسیر C:\Program Files(x۸۶)\svchost.exe ذخیره می‌شود. این مولفه به نظر می‌رسد نسخه‌ای از بدافزار قدیمی Gh۰stRAT است.

مولفه ۸۴.exe نیز در مسیر C:\Program Files(x۸۶)\StormII\mssta.exe ذخیره می‌شود و این نیز به نظر یک بدافزار RAT است که اصالت آن هنوز نامشخص است.

۵ مولفه ۶۴.exe

این مولفه اولین مولفه ای است که توسط ZombieBoy دانلود می شود. این مولفه از تکنیک های ضد تحلیل استفاده می کند. کل فایل توسط یک پکر به نام Themida پک شده است که کار را برای مهندسی معکوس دشوار می سازد. همچنین نسخه فعلی ZombieBoy محیط آزمایش و VM را تشخیص داده و در این صورت اجرا نمی شود.

۶۴.exe نزدیک به ۷۰ فایل را در محل قرار می دهد که شامل ماینر XMRIG و اکسپلویت ها است. همچنین خودش را به نام CPUInfo.exe در آن محل ذخیره می کند.

این مولفه با اتصال به آدرس ip.۳۲۲۲.net آدرس IP قربانی را بدست می آورد. سپس با استفاده از WinEggDrop که یک اسکنر TCP سبک است شروع به اسکن کردن شبکه هدف می کند. این اسکن به منظور یافتن پورت باز ۴۴۵ بر روی یک هاست انجام می شود. با استفاده از IP بدست آمده و همچنین IP محلی، این مولفه اقدام به پخش بدافزار بر روی دیگر سیستم های شبکه هدف می کند.

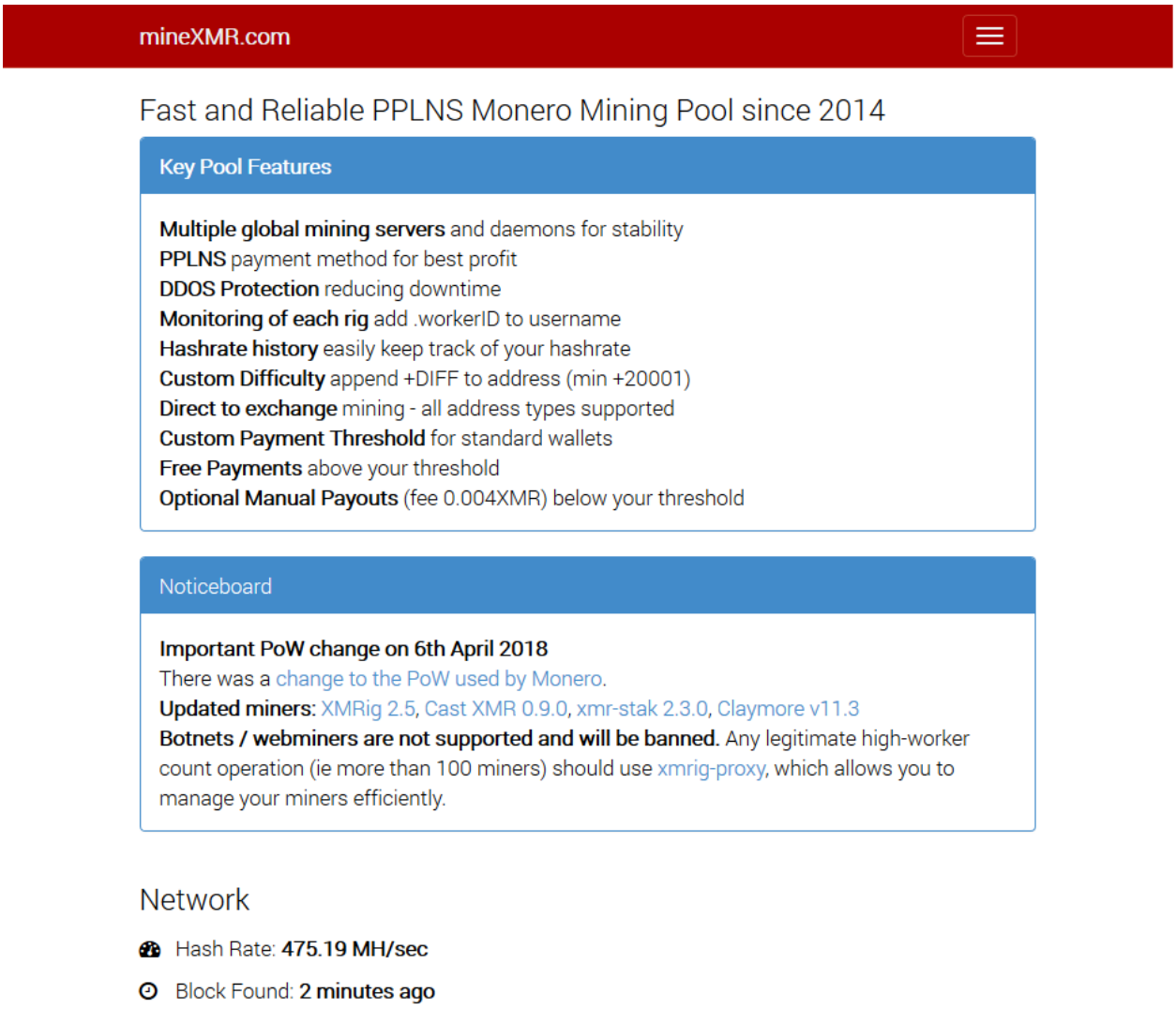
مولفه ۶۴.exe از اکسپلویت DoublePulsar برای نصب درب پشتی SMB و درب پشتی RDP استفاده می کند.

```
<parameter name="NetworkTimeout" description="Timeout for blocking network calls (in seconds).  Use -1 for no timeout." type="S16">
    <default>60</default>
</parameter>
<parameter name="TargetIp" xdevmap="TARGET_IP_V4_ADDRESS" description="Target IP Address" type="IPv4"/>
<parameter name="TargetPort" xdevmap="TARGET_PORT" description="Port used by the Double Pulsar back door" type="TcpPort">
    <default>445</default>
</parameter>

<paramchoice name="Protocol" xdevmap="DOUBLEPULSAR_PROTOCOL_TYPE" description="Protocol for the backdoor to speak">
    <default>SMB</default>
    <paramgroup name="SMB" description="Ring 0 SMB (TCP 445) backdoor">
    </paramgroup>
    <paramgroup name="RDP" description="Ring 0 RDP (TCP 3389) backdoor">
    </paramgroup>
</paramchoice>
```

شکل ۴- اکسپلویت DoublePulsar

علاوه بر این، ۶۴.exe برای mine کردن پول الکترونیکی XMR، از ابزار XMRIG استفاده می کند. قبل از بلاک شدن آدرس های این بدافزار در وبسایت minexmr.com، ZombieBoy چیزی در حدود ۴۳KH/s قدرت ماینینگ داشته است. با این سرعت چیزی بیش از ۱۰۰۰ در ماه می توانسته پول Monero را ماین کند.



شکل ۵- وبسایت minexmr.com

آدرس های جدیدی کشف شده است. البته دیگر این بدافزار از minexmr.com برای ماین کردن استفاده نمی کند.

آدرس های کشف شده:

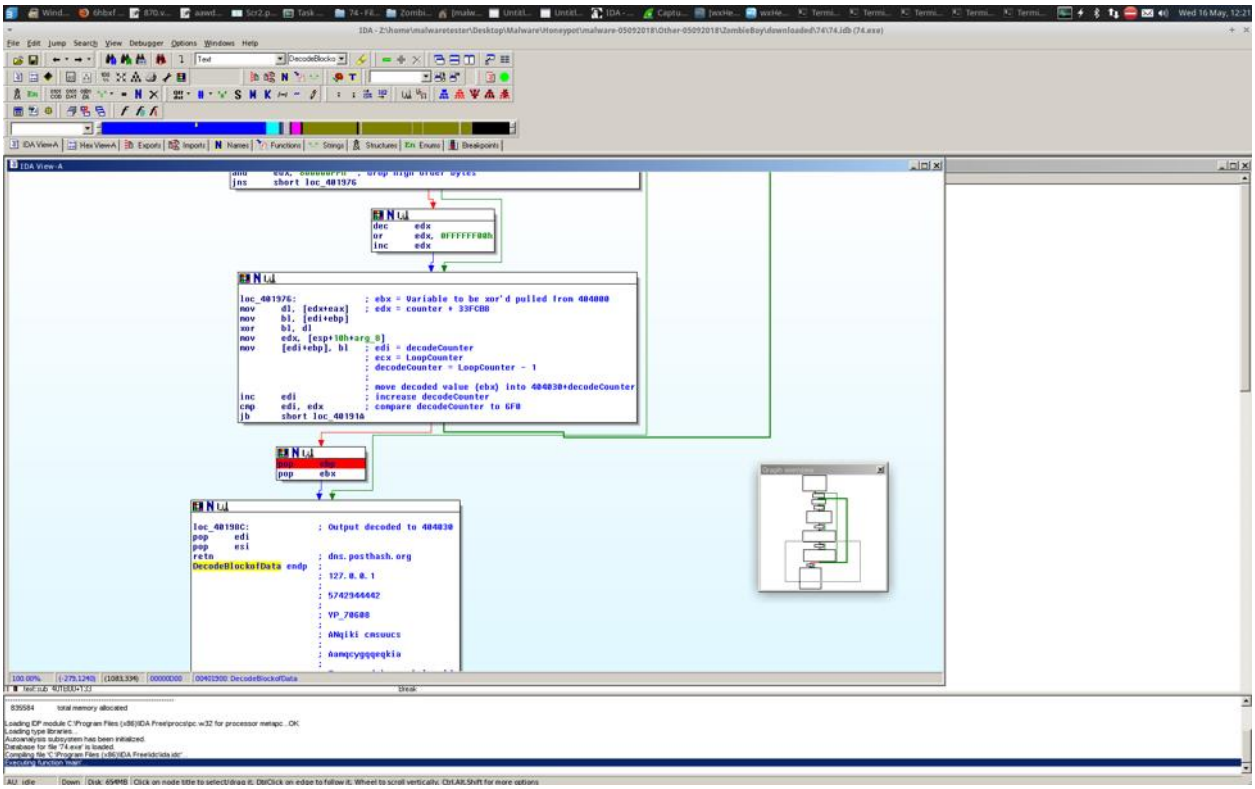
- ۴۲MiUXx۸i۴۹AskDATdAfkUGuBqjCL۷oU۱g۷TsU۳XCJg۹Maac۱mEEd Q۲X۹vAKqu۱pvkFQUuZn۲HEzaa۵UaUkMMfJHU۵N۸UCw
- ۴۹vZGV۸x۳bed۳TiAZmNG۹zHFXytGz۴۵tJZ۳g۸۴rpYtw۷۸J۲UQQaCiH۶ SkozGKHyTV۲Lkd۷GtsMjurZkk۸B۹wKJ۲uCAKdMLQ

۶ مولفه ۷۴.exe

این مولفه به منظور دانلود کردن، decrypt کردن و اجرای Gh۰stRat.dll که به نام NetSyst۹۶.dll بر روی سیستم قربانی قرار می گیرد به کار می رود. علاوه بر این، ۷۴.exe عملیات decrypt کردن یک سری پارامتر به منظور پاس دادن به Netsyst۹۶.dll را نیز بر عهده دارد.

این آرگومان ها به شرح زیر است:

۱. Dns.posthash.org
۲. ۱۲۷.۰.۰.۱
۳. ۵۷۴۲۹۴۴۴۴۲
۴. YP_۷۰۶۰۸
۵. ANqiki cmsuucs
۶. Aamqcygqqeqkia
۷. Fngzxzygdgkywoyvkxlpv ldv
۸. %ProgramFiles%/
۹. Svchost.exe
۱۰. Add
۱۱. Eeie saswuk wso



شکل ۶ – عملیات رمزگشایی پارامترها

هنگامی که ۷۴.exe آرگومان های ذکر شده را رمزگشایی کرد، بررسی می کند که آیا NetSyst۹۶.dll دانلود شده و در مسیر C:\Program Files\AppPatch\mysqld.dll ذخیره شده است یا خیر. این مولفه این کار را با فراخوانی تابع CreateFileA با مقداردهی پارامتر CreationDisposition به عنوان Open_Existing انجام می دهد. اگر mysqld.dll پیدا نشد، این مولفه یک ارتباط با آدرس ca.posthash.org:۴۴۳ برقرار می کند و NetSyst۹۶.dll را دانلود و در مسیر C:\Program Files\AppPatch\mysqld.dll ذخیره می کند.

فایل NetSyst۹۶.dll در تابع قابل صدور به نام های DllFuUpgraddrs و DllFuUpgraddrs۱ دارد. بعد از ذخیره NetSyst۹۶.dll به عنوان mysqld.dll، ۷۴.exe، DllFuUpgraddrs را در NetSyst۹۶.dll جای می دهد (قبل از اینکه آن را فراخوانی کند).

۷ فایل NetSyst۹۶.dll

این فایل توسط مولفه ۷۴.exe فراخوانی می شود. اکثر این فایل کد شده است. پس از رمزگشایی این فایل، رشته های جالب توجهی نظیر Game Over Good Luck By Wind و jingtisanmenxiachuanxiao.vbs در آن یافت شد.

```
Game Over Good Luck By Wind
FunctionMstsc
FunctionMmc
FunctionRegedit
FunctionTaskmgr
FunctionCMD
%s\dllcache\magnify.exe
%s\dllcache\osk.exe
%s\dllcache\sethc.exe
%s\magnify.exe
%s\osk.exe
%s\sethc.exe
DELSHIFTOSK
TermService
\dllcache\termsrvhack.dll
\termsrvhack.dll
SYSTEM\CurrentControlSet\Services\TermService\Parameters
ServiceDll
%SystemRoot%\system32\termsrvhack.dll
SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core
EnableConcurrentSessions
SYSTEM\CurrentControlSet\Control\Terminal Server
fDenyTSConnections
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
KeepRASConnections
SYSTEM\CurrentControlSet\Services\TermService
Start
open
%s%s %s%s
jingtisanmenxiachuanxiao.vbs
```

شکل ۷ – رشته های کشف شده درون فایل NetSyst۹۶.dll

NetSyst۹۶.dll توانایی ضبط اسکرین کاربر، ضبط صدا و حتی ویرایش مقدار clipboard را دارد. همچنین یک تحلیل بر روی رشته های این فایل نشان می دهد که یک KeyLogger نیز توسط این فایل استفاده می شود.

NetSyst۹۶.dll نخست متغیرهای محیطی مسیر (Environment Strings Path) را بدست آورده و برای تولید مسیر از مسیر C:\Program files (x۸۶)\svchost.exe استفاده می کند. سپس با استفاده از CreateToolhelp۳۲Snapshot ،پروسه های در حال اجرا را برای Rundll۳۲.exe جستجو می کند تا ببیند که آیا اولین بار است اجرا شده یا نه.

اولین باری که NetSyst۹۶.dll اجرا می شود، عملیات زیر را به منظور پایدار سازی خود در سیستم انجام می دهد:

- یک کپی از ۷۴.exe در مسیر C:\Program Files(x۸۶)\svchost.exe ایجاد می کند.
- یک سرویس به نام cmsuucs ANqiki با استفاده از ایجاد کلید System/CurrentControlSet/Services/ANqiki cmsuucs ایجاد می کند. موقعی که این سرویس اجرا شد، svchost.exe را اجرا می کند.
- یک کلید رجیستری به نام MARKTIME ایجاد کرده که مشخص کننده اولین باری است که فایل اجرا شده.
- یک snapshot با استفاده از CreateToolhelp۳۲Snapshot ایجاد می کند تا به جستجوی پروسه های در حال اجرا برای svchost.exe بپردازد.
  - اگر پیدا نشد، دوباره آن را اجرا کرده و دوباره به جستجوی svchost.exe می پردازد.
  - اگر یکی پیدا شد، svchost.exe را برای اجرای مجدد ذخیره می کند.
  - اگر بیش از یکی پیدا شد، یک تابع برای ایجاد یک اسکریپت vbs فراخوانی می کند. این اسکریپت svchost.exe های اضافی را پاک می کند.

پس از اجرای موارد بالا، NetSyst۹۶.dll به اتصال به سرور C&C خود می پردازد:

۱- وجود کلید System/CurrentControlSet/Services/ANqiki cmsuucs را بررسی و صحت سنجی می کند.
   a. اگر وجود نداشت، کلید بالا را می سازد.
   b. اگر وجود داشت، به مرحله بعد می رود.
۲- یک رخداد به نام Eeie saswuk wso می سازد.
۳- آدرس ip سرور C۲ را به C۲URL (dns.posthash.org) می فرستد.
۴- WSA (winsock ۲.۰) را اجرا می کند.
۵- به آدرس www.ip۱۲۳.com.cn متصل شده و ip آدرس dns.posthash.org را بدست می آورد.

۶- رخداد را ریست می کند.
۷- به سرور C۲ متصل شده و منتظر دریافت دستورات می ماند.

تا کنون ۳۱ دستور از جانب سرور C۲ که توسط NetSyst۹۶.dll پشتیبانی می شود کشف شده است.

۸ مولفه ۸۴.exe

این سومین مولفه ای است که توسط بدافزار بر روی سیستم قربانی قرار می گیرد و آن طور که به نظر می رسد یک RAT می باشد. البته مواردی نیز وجود دارد که این مورد را نقض می کند. بر خلاف ۷۴.exe، مولفه ۸۴.exe نیاز به دانلود هیچ کتابخانه اضافی ندارد و به جای آن یک کتابخانه کد شده به نام loader.dll را رمزگشایی کرده و درون حافظه خود قرار می دهد.

علاوه بر این، متغیر رشته ای محلی کاربر را به C:\Program Files(x۸۶)\StormII\ تغییر می دهد.

پس از اینکه Loader.dll فراخوانی شد، ۸۴.exe یک سری متغیر به Loader.dll پاس می دهد. این متغیرها تحت یک تابع به نام Update منتقل خواهند شد.

متغیرها:

۱. ChDz۰PYP۸/oOBfMO۰A/۰B۶Y=
۲. ۰
۳. ۶gkIBfkS+qY=
۴. dazsks fsdgsdf
۵. daac gssosjwayw
۶. |_+f+
۷. fc۴۵f۷f۷۱b۳۰bd۶۶۴۶۲۱۳۵d۳۴f۳b۶c۶۶
۸. EQr۸/KY=
۹. C:\Program Files(x۸۶)\StormII
۱۰. Mssta.exe
۱۱. ۰

۱۲. Ccfcdaa

۱۳. Various integers

همه این متغیرها از نوع رشته هستند. ۳ متغیر رمز شده هستند که پس از رمزگشایی مقادیر زیر را خواهند داشت:

۱. [ChDz۰PYP۸/oOBfMO۰A/۰B۶Y=] = "dns[dot]posthash[dot]org"

۲. [۶gkIBfkS+qY=] = "Default"

۳. [EQr۸/KY=] = "mdzz"

۹ مولفه Loader.dll

Loader.dll یک RAT است که قابلیت های جالبی دارد. به عنوان مثال قابلیت جستجوی سرعت نوشتن CPU و همچنین جستجوی سیستم برای بدست آوردن آنتی ویروس های موجود در آن.

این مولفه توسط مولفه ۸۴.exe فراخوانی می شود. اولین کاری که این مولفه می کند، بدست آوردن متغیرهایی توسط تابع Update از مولفه ۸۴.exe است. در این لحظه، Loader.dll اشیا زمان اجرای مهمی را ایجاد می کند:

- یک رخداد با مشخصات Uninheritable, non-signaled, auto-reset به نام Null که آدرس ۰x۸۴ را handle می کند.
- یک نخ برای اجرای یک تابع که DesktopInfo را دستکاری می کند.
- یک ورودی دسکتاپ با handle ۰x۸۴ و پرچم DF_ALLOWOTHERACCOUNTS، که به عنوان دسکتاپ فراخواننده نخ تنظیم می شود.

Loader.dll سپس سیستم را برای یافتن dazsks fsdgsdf در مسیر SYSTEM/CurrentControlSet/Services/Dazsks Fsdgsdf جستجو می کند. که این کار مشخص می کند که آیا بدافزار اولین بار است اجرا شده است یا خیر.

اجرای بار اول:

- Loader.dll یک سرویس به نام Dazsks Fsdgsdf با مسیر C:\Program Files(x۸۶)\StormII\mssta.exe فایل ایجاد می کند.
- Loader.dll تلاش می کند تا سرویس ایجاد شده را اجرا کند. اگر این تلاش موفقیت آمیز بود، به حلقه اصلی می رود در غیر این صورت اجرایش را متوقف می کند.

شکل ۸ – کلیدهای رجیستری ایجاد شده در اجرای اول مولفه loader.dll

اجراهای بعدی:

- Service.exe با آرگومان Dazsks Fsdgsdf اجرا شده تا سرویس ایجاد شده در اجرای اول را اجرا کند.
- به حلقه اصلی می رود.

در حلقه اصلی، Loader.dll موارد زیر را انجام می دهد:

- ایجاد یک رخداد به نام ccfcdaa با مشخصات uninheritable, auto-reset, nonsignaled با یک handle به آدرس ۰x۸C.
- رمزگشایی عبارت ChDz۰PYP۸/oOBfMO۰A/۰B۶Y= که عبارت dns.posthash.org را تولید می کند.
- اجرای شی WinSock.

- ایجاد یک رخداد به نام null با مشخصات uninheritable, unsignaled, manual-reset با یک handle به آدرس ۰x۹۰.
- ایجاد یک درخواست HTTP: Get /?ocid = iefvrt HTTP/۱.۱.
- اتصال به آدرس dns.posthash.org:۵۲۰۰.
- گرفتن اطلاعات در مورد سیستم عامل با استفاده از GetVersionEx.
- بارگذاری ntdll.dll و فراخوانی تابع RtlGetVersionNumbers درون آن.
- ذخیره System\CurrentControlSet\Services\(null) درون رجیستری.
- بدست آوردن نام سوکت.
- بدست آوردن سرعت refresh شدن CPU با استفاده از .\Hardware\Description\System\CentralProcessor
- فراخونی GetVersion برای بدست آوردن مشخصات سیستم.
- فرخوانی GlobalMemoryStatusEx برای بدست آوردن وضعیت حافظه سراسری موجود.
- شمارش تمامی دیسک های سیستم با استفاده از GetDriveTypeA.
- بدست آوردن میزن فضای خالی بر روی هر یک از دیسک ها.
- راه اندازی اولیه کتابخانه COM.
- افزودن زمان فعلی سیستم به سرویس dazsks fsdgsdf با استفاده از تابع marktime.
- بدست آوردن مشخصات سیستمی که در حالت WOW۶۴ در حال اجراست.
- با استفاده از یک لیست بلند بالای نام فایل های آنتی ویروس های چینی و CreateToolHelp۳۲Snapshot، یک snapshot از پروسه های در حال اجرای فعلی تهیه می کند که مشخص کند آنتی ویروسی در حال اجراست یا خیر.
- رمزگشایی عبارت EQr۸/KY= به mdzz.
- ارسال تمامی اطلاعات بدست آمده به سرور C&C به آدرس dns.posthash.org:۵۲۰۰.

۱۰ راه های تشخیص و پاک سازی

بهترین راه برای جلوگیری از ورود بدافزار ZombieBoy به سیستم، به روز رسانی سیستم عامل برای مسدود سازی راه نفوذ اکسپلویت ها است. به طور خاص، نسخه به روز رسانی MS۱۷-۰۱۰ راه های نفوذ بدافزار را مسدود می کند.

در هر صورت، اگر سیستم شما دچار نفوذ این بدافزار شده است، می توانید با استفاده از یک آنتی ویروس به روز شده، سیستم را اسکن نمایید. پس از اسکن نیز راه های زیر را برای پاک سازی تمامی موارد بدافزار انجام دهید:

در پروسه های در حال اجرا هر یک از نام های زیر مشاهده شد، آن را ببندید:

- ۱۲۳.exe
- ۶۴.exe
- ۷۴.exe
- ۸۴.exe
- CPUinfo.exe
- N.exe
- S.exe
- Svchost.exe

البته پروسه svchost.exe در صورتی که فایل اصلی آن در مسیر C:\Windows\System۳۲ نباشد مشکوک خواهد بود.

علاوه بر این، کلیدهای رجیستری زیر را نیز پاک نمایید:

- SYSTEM/CurrentControlSet/Services/Dazsks Fsdgsdf
- SYSTEM/CURRENTCONTROLSET/SERVICES/ANqiki cmsuuc

همچنین تمامی فایل های قرار داده شده توسط بدافزار را نیز پاک نمایید:

- C:\%WindowsDirectory%\sys.exe
- C:\windows\%system%\boy.exe
- C:\windows\IIS\cpuinfo.exe

- All of the ۷۰+ files dropped in IIS
- C:\Program Files(x۸۶)\svchost.exe
- C:\Program Files\AppPatch\mysqld.dll
- C:\Program Files(x۸۶)\StormII\mssta.exe
- C:\Program Files(x۸۶)\StormII*

۱۱ مشخصه فایل های بدافزار

نمونه	MD۵	سایز فایل	IP	مسیر
Zombie Boy[Main Dll]	۸۴۲۱۳۳ddc۲d۵۷fd۰f۷۸۴۹۱b۷ba۳۹a۳۴d	۸۲.۴kb	-	-
۱۲۳.exe	۷۳۲۷ef۰۴۶fe۶۲a۲۶e۵۵۷۱c۳۶b۵c۲c۴۱۷	۷۸۲.۳kb	Downloaded From: ca.posthash[dot]org:۴۴۳	C:\%WindowsDirectory%\sys.exe
[Injector ۱۲۳]	۷۸۵a۷f۶e۱cd۴۰b۵۰ad۷۸۸e۵d۷d۳c۸۴۶۵	۴۳۷.۹kb	-	-
۶۴.exe	۷۹c۶ead۶fa۴f۴addd۷f۲f۰۱۹۷۱۶dd۶ca	۶.۴MB	Mining Server: Minexmr.com Downloaded From	C:\windows\%system%\boy.exe C:\windows\IIS\cpuinfo.exe Necessary files for exploits and WinEggDrop into C:\windows\IIS

			ca.posthash[dot]org:۴۴۳/ sm.posthash[dot]org:۴۴۳/	
۷۴.exe	۳۸d۷d۴f۶a۷۱۲bff۴ab۲۱۲۸۴۸۸۰۲f۵f۹c	۹.۷ kb	C۲ server: dns.posthash[dot]org:۵۲۰۰۹/	C:\Program Files(x۸۶)\svchost.exe SYSTEM/CURRENTCONTROLSET/SERVICES/Anqiki cmsuuc
Netsyst۹۶.dll	۶de۲۱f۲fd۱۱d۶۸b۳۰۵b۵e۱۰d۹۷b۳f۲۷e	۱.۰ MB	Downloaded From ca.posthash[dot]org:۴۴۳/ C۲ server: Dns.posthash[dot]org:۵۲۰۰۹/	C:\Program Files\AppPatch\mysqld.dll,
۸۴.exe	۹۱ebe۲de۷fcb۹۲۲c۷۹۴a۸۹۱ff۸۹۸۷۱۲۴	۳۳۴.۷kb	C۲ Server: dns.posthash[dot]org:۵۲۰۰/	C:\Program Files(x۸۶)\StormII\mssta.exe SYSTEM/CurrentControlSet/Services/Dazsks Fsdgsdf C:\Program Files(x۸۶)\StormII*
Loader.dll	۹a۴۶a۳ae۲c۳۷۶۲۹۶۴c۵cbb۶۳b۶۲d۷dee	۱۳۵.۲kb	C۲ Server: dns.posthash[dot]org:۵۲۰۰/	SYSTEM/CurrentControlSet/Services/(null); Files Queried: Hardware\Description\System\CentralProcessor\ ; SYSTEM/CurrentControlSet/Services/BITS;

۱۲ جمع بندی

ZombieBoy بدافزار جدیدی است که به جای رمز نمودن فایل های کاربر و درخواست باج، از روش جدیدتری یعنی به خدمت گرفتن کامپیوتر قربانی برای ماینینگ پول دیجیال استفاده می کند. همچنین برای نفوذ به سیستم کاربر از اکسپلویت هایی که آسیب پذیری های متعددی در ویندوز را هدف قرار می دهند استفاده می‌کند. این بدافزار هر روز در حال به روز رسانی و افزودن قابلیت های جدیدی به خود است.

۱۳ منابع

- https://securityintelligence.com/news/new-crypto-mining-malware-zombieboy-exploits-multiple-cves-for-maximum-impact/
- https://securityaffairs.co/wordpress/۷۵۰۷۰/malware/zombieboy-monero-miner.html
- https://www.alienvault.com/blogs/labs-research/zombieboy
- https://medium.com/@SwiftSafe/zombieboy-new-crypto-mining-malware-exploits-multiple-cves-e۹a۳۸c۲۹۵۶۷۸
- https://www.howtogeek.com/۲۱۱۶۹۴/cryptocurrency-miners-explained-why-you-dont-want-this-junk-on-your-pc/