گزارش تحلیلی بدافزار Chainshot از طریق کرک کلید ۵۱۲ بیتی RSA

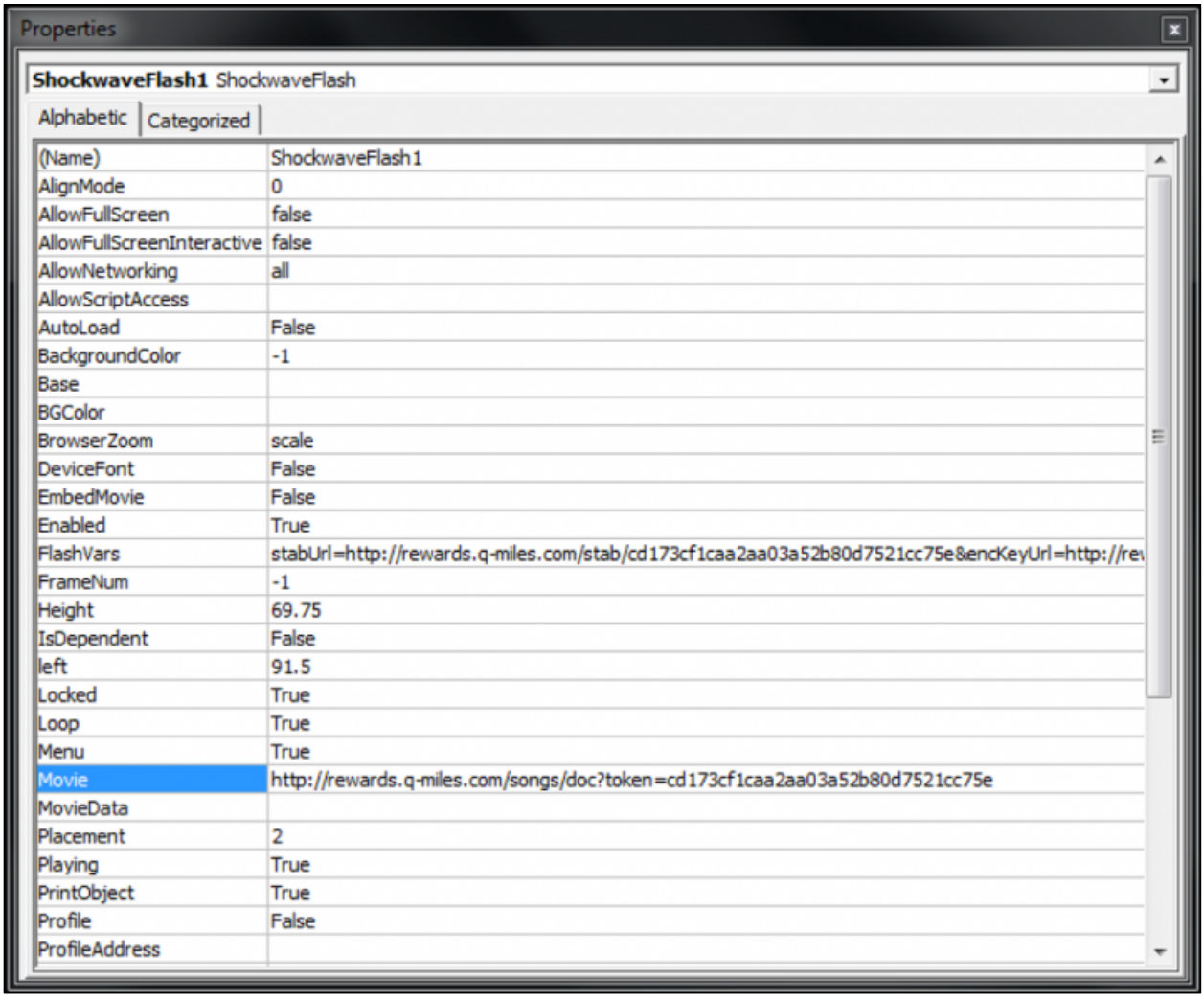
مقدمه

محققین شرکت Palo Alto حمله بدافزاری را کشف کردند که از آسیب پذیری روز صفر Adobe Flash ، که با شناسه "CVE-۲۰۱۸-۵۰۰۲" ثبت شده، استفاده می‌کند و بدافزار جدیدی را به نام "chainshot" را نصب می‌کند. اولین بردار حمله، یک فایل مخرب مایکروسافت اکسل است که در صورت باز شدن، شروع به نصب بدافزار می‌کند. اکسپلویت و پیلودهای شل کد درون بدافزار، مبهم سازی شده‌اند. اکسپلویت تلاش می‌کند با به دست آوردن مجوزهای خواندن-نوشتن-اجرا را به دست بیاورد و پیلود شل کد را اجرا کند. شل کد، یک فایل DLL به نام "FirstStageDropper" را در حافظه ماشین قربانی بارگذاری می‌کند و دو منبع شامل فایل "SecondStageDropper" و یک شل کد ۶۴ بیتی را درحالت کرنل اجرا می‌کند. بدافزار chainshot، اطلاعات فرآیند و کاربر سیستم را به صورت رمز شده به سرور مهاجم ارسال می‌کند. فایل SecondStageDropper.dll به صورت یک دانلود کننده برای پیلود نهایی استفاده می‌کند که اطلاعات متفاوتی را از سیستم قربانی جمع‌آوری می‌کند و آن را به صورت رمز شده را به مهاجم ارسال می‌کند.

این محققین موفق شدند با کرک کلید ۵۱۲ بیتی RSA استفاده شده برای رمزگذاری در این حمله، به پیلودها و اکسپلویت این بدافزار دست پیدا کنند. در ادامه این گزارش، ابتدا نحوه اجرای حمله توضیح داده می‌شود تا علت نیاز به کلید ۵۱۲ بیتی RSA درک شود و سپس نحوه کرک کلید ۵۱۲ بیتی و کشف بدافزار بیان می‌شود.

تشریح روش حمله :

این اکسپلویت از یک سند آفیس برای دانلود و اجرای اکسپلویت آسیب پذیری روز صفر Adobe Flash روی کامپیوترهای قربانی استفاده می‌کند. سند اکسل، حاوی اطلاعات یک شی کوچک Sockwave Flash ActiveX است که ویژگی‌هایی آن شبیه به ویژگی‌های نشان داده شده در تصویر ۱ است :



شکل ۱. ویژگیهای شی Shockwave Flash ActiveX

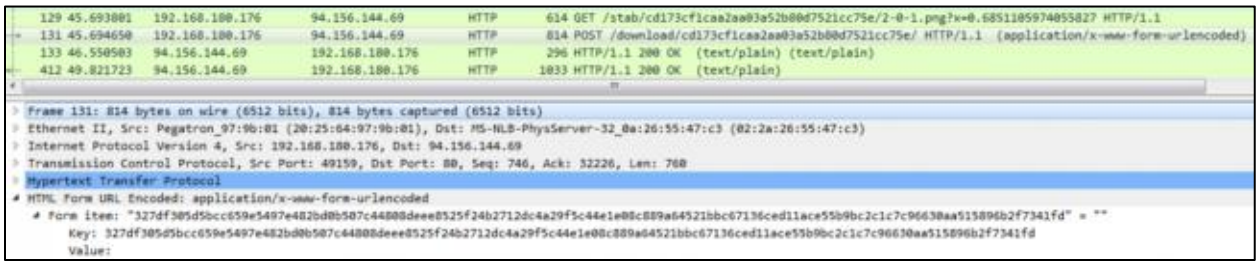
ویژگی "Movie" شامل آدرس یک برنامه Flash است که به صورت متن آشکار قابل دانلود و اجرا است. ویژگی "FlashVars"، یک رشته طولانی شامل چهار آدرس است که به برنامه Flash دانلود شده ارسال می‌شود. برنامه Flash مذکور، یک دانلود کننده مبهم شده است که در حافظه پردازه، یک زوج کلید ۵۱۲ بیتی RSA را به صورت تصادفی تولید می‌کند. کلید خصوصی تولید شده در حافظه باقی می‌ماند و پیمانه کلید عمومی (n) به سرور مهاجم ارسال می‌شود. در سمت سرور، از پیمانه n و توان هاردکد شده e (۰X۱۰۰۰۱) برای رمزگذاری کلید ۱۲۸ بیتی AES، که قبلا برای رمزگذاری اکسپلویت و پیلود شل کد به کار گرفته شده، استفاده می‌شود. اکسپلویت رمز شده یا پیلود توسط برنامه Flash دانلود می‌شود و از کلید خصوصی درون حافظه پردازه روی سیستم قربانی، برای رمزگشایی کلید AES و سپس اکسپلویت یا پیلود استفاده می‌شود.

تشریح روش کشف بدافزار :

به این دلیل که پیمانه کلید عمومی به سرور مهاجم ارسال می‌شود، می‌توان آن را با ضبط بسته های شبکه به دست آورد. با داشتن این مقدار و توان هارد کد شده e، کلید عمومی به دست می‌آید و از آنجایی که طبق استانداردهای امروزی، ماژول‌های ۵۱۲ بیتی

RSA، ناامن محسوب می‌شوند، می‌توان کلید خصوصی را به دست آورد. به این منظور، پیمانه n به دو عدد اول بزرگ p و q تجزیه می‌شود. این مساله با استفاده از سرویس‌های ابری آمازون، در چند ساعت قابل حل است.

با فرض اینکه پیمانه کلید عمومی با درخواست HTTP، شبیه تصویر ۲، به مهاجم ارسال شود :



شکل ۲. درخواست HTTP برای دریافت پیلود شل کد با پیمانه n در فرم هگزادسیمال

بعد از پاک کردن دو بایت اول که در این مورد برای بازیابی نسخه ۳۲ بیتی پیلود شل کد استفاده شده، فرم هگزادسیمال پیمانه به صورت زیر خواهد بود:

```
0x7df305d5bcc659e5497e482bd0b507c44808deee8525f24b2712dc4a29f5c44e1e08c889a64521bbc67136ce
d11ace55b9bc2c1c7c96630aa515896b2f7341fd
```

شکل ۳ . پیمانه n به فرم هگزادسیمال

پس از تجزیه، دو عدد اول p و q در فرم دهدهی به صورت زیر خواهد بود:

p

```
0x7df305d5bcc659e5497e482bd0b507c44808deee8525f24b2712dc4a29f5c44e1e08c889a64521bbc67136ce
d11ace55b9bc2c1c7c96630aa515896b2f7341fd
```

شکل ۴. عدد اول p

q

```
0x7df305d5bcc659e5497e482bd0b507c44808deee8525f24b2712dc4a29f5c44e1e08c889a64521bbc67136ce
d11ace55b9bc2c1c7c96630aa515896b2f7341fd
```

شکل ۵. عدد اول q

با داشتن p و q، کلید خصوصی محاسبه می‌شود. کلید خصوصی با فرمت PEM در تصویر ۶ نشان داده شده است :

```
1  -----BEGIN RSA PRIVATE KEY-----
2  MIIBOgIBAAJAffMF1bzGWeVJfkgr0LUHxEgI3u6FJfJLJxLcSin1xE4eCMiJpkUh
3  u8ZxNs7RGs5VubwsHHyWYwqlFYlrL3NB/QIDAQABAkBog3SxE1AJItIkn2D0dHR4
4  dUofLBCDF5czWlxAkqcleG6im1BptrNWdJyC5102H/bMA9rhgQEDHx42hfyQiyTh
5  AiEA+mWGmrUOSLL3TXGrPCJcrTsR3m5XHzPrh9vPinSNpPUCIQCAxI/z9Jf10ufN
6  PLE2JeDnGRULDPn9oCAqwsU0DWxD6QIhAPdiyRseWI9w6a5E6IXP+TpZSu00nLTC
7  Sih+/kxvnOXlAiBZMc7VGVQ5f0H5tFS8QTisW39sDC0ONeCSPiADkliwIQIhAMDu
8  3Dkj2yt7zz04/H7KUV9WH+rdrhUmoGhA5UL2PzfP
9  -----END RSA PRIVATE KEY-----
```

شکل ۶. کلید خصوصی

با کمک کلید خصوصی به دست آمده، کلید ۱۲۸ بیتی AES، رمزگشایی می‌شود. دستور رمزگشایی با OpenSSL در تصویر ۷ نشان داده شده است :

```
openssl rsautl -decrypt -in enc_aes.bin -out dec_aes.bin -inkey private_key.pem
```

شکل ۷. دستور OpenSSL برای رمزگشایی کلید ۱۲۸ بیتی AES

کلید AES رمز شده‌ای که توسط شرکت Icebrg از فایل باینری رمز شده استخراج شده، در تصویر ۵ آمده است. این کلید از آفست ۰x۴ شروع می‌شود و طول آن، ۰x۴۰ بایت است.

```
0x5BC64C5DC7EC96750CCB466935ED2183FE90212CB1BF6305F0B79B4B9D9261A4AC8A3E06F3E07D4037A40F4E2
21BB12E05B4DE2682B31617F177712BD12B501A
```

شکل ۸. کلید AES رمز شده

کلید AES رمزگشایی شده، در تصویر ۹ آمده است.

```
0xE4DF3353FD6D213E7400EEDA8B164FC0
```

شکل ۹. کلید AES رمزگشایی شده

فایل دانلود کننده Flash، برای رمزگشایی از یک بردار اولیه (IV) سفارشی برای الگوریتم AES استفاده می‌کند که در آفست ۰x۴۴ قرار دارد و طول آن، ۱۶ بایت است :

```
0xE4DF3353FD6D213E7400EEDA8B164FC0
```

شکل ۱۰. بردار اولیه استفاده شده در الگوریتم AES

دستور OpenSSL، برای رمزگشایی نهایی، در تصویر ۱۱ آمده است:

```
openssl enc -nosalt -aes-128-cbc -d -in payload.bin -out decrypted_payload -K
E4DF3353FD6D213E7400EEDA8B164FC0 -iv CC6FC77B877584121AEBCBFD4C23B67C
```

شکل ۱۱. دستور OpenSSL برای رمزگشایی پیلود شل کد

با مشاهده مقدار ۰x۷۸۹C در دو بایت ابتدایی، می‌توان به این مطلب پی برد که پیلود شل کد رمزگشایی شده، با zlib فشرده سازی شده است که می‌توان آن را با Offzip از حالت فشرده خارج کرد. برای رمزگشایی اکسپلویت Flash که با فشرده سازی هم نشده، می‌توان از فرآیندی شبیه به فرآیند توضیح داده شده استفاده کرد.

روش مقابله با بدافزار chainshot :

محققین شرکت Palo Alto، به روشهای زیر از مشتریان خود در برابر این تهدید محافظت می‌کنند:

- استفاده از سیستم‌های تحلیل تهدید برای شناسایی اسناد مخرب، اکسپلویت و دانلود کننده Flash و همه نمونه‌های chainshot
- استفاده از سرویس‌های مقابله با تهدید برای دنبال کردن نمونه‌هایی با اکسپلویت CVE-۲۰۱۸-۵۰۰۲ و تگهای بدافزار chainshot
- استفاده از آنتی ویروس برای کشف و بلاک کردن اسناد اکسل با اکسپلویت Flash

جمع بندی

در این گزارش، بدافزاری تشریح شد که از اکسپلویت Adobe Flash (شناسه CVE-۲۰۱۸-۵۰۰۲)، به عنوان دانلود کننده برای هدف قرار دادن قربانیان استفاده می‌کند. کشف این بدافزار به دلیل استفاده از رمزنگاری نا امن ۵۱۲ بیتی RSA امکان پذیر بوده است. این بدافزار اطلاعات رمزشده کاربر را به سرور مهاجم ارسال می‌کند و تلاش می‌کند پیلود نهایی را دانلود کند.

پیوست

شاخص های سازش

اکسپلویت Adobe Flash (CVE-۲۰۱۸-۵۰۰۲)

۳e۸cc۲b۳۰ece۹adc۹٦b۰a۹f٦۲٦aefa٤a۸۸۰۱۷b۲f٦b۹۱٦۱٤٦a۳bbd۰f۹۹ce۱e٤۹۷

نمونه های Chainshot

پیلودهای شل کد ۳۲ بیتی

d۷۵de۸f۷a۱۳۲e۰eb۹۲۲d٤b۵۷f۱ce۸db٤۷dfcae٤٤۷۷۸۱۷d۹f۷۳۷۷٦۲e٤۸٦۲۸۳۷۹۵

۲d۷cb۵ff٤a٤٤۹fa۲۸٤۷۲۱f۸۳e۳۵۲۰۹۸c۲fdea۱۲۵f۷۵٦۳۲۲c۹۰a٤۰ad۳ebc۵e٤۰d

FirstStageDropper.dll

a۲٦۰d۲۲۲dfc۹٤b۹۱a۰۹٤۸۵٦٤۷c۲۱acfa٤a۲٦٤٦۹۵۲۸ec٤b۱b٤۹٤٦۹db۳b۲۸۳eb۹a

a۰۹۲۷۳b٤cc۰۸c۳۹afe۰c۹٦٤f۱٤cef۹۸e۵۳۲ae۵۳۰eb٦۰b۹۳aec٦٦۹۷۳۱c۱۸۵ea۲۳

SecondStageDropper.dll

٤۳f۷ae۵۸e۸e۵٤۷۱۹۱۷۱۷۸٤۳۰f۳٤۲۵۰٦۱d۳۳۳b۷۳٦۹۷٤f٤b۲۷۸٤ca۵٤۳e۳۰۹۳۲۰٤b

۳٤۸۵c۹b۷۹dfd۳e۰۰aef۹۳٤۷۳۲٦b۹ccfee۵۸۸۰۱۸a٦۰۸f۸۹ecd٦۵۹۷da۵۵۲e۳۸۷۲f

مرجع:

https://researchcenter.paloaltonetworks.com/۲۰۱۸/۰۹/unit۴۲-slicing-dicing-cve-۲۰۱۸-۵۰۰۲-/payloads-new-chainshot-malware