

# 样本分析报告

文件名称：letsvpn-3.7.1.exe

SHA256：2ee52db4edf06e527dd7bf1f30a2b6ba52353fac8f8ca78647c9f1668b013ffd

文件大小：14.67 MB

文件类型：PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

分析环境： Win10(1903 64bit, Office2016)

微步判定： 安全



目录

- 1 行为检测 -----
- 2 引擎检测 -----
- 3 静态分析 -----
- 4 动态分析 -----





安全

# letsvpn-3.7.1.exe

首次提交: 2024/06/17      末次提交: 2024/06/26      末次分析: 2024/06/26 11:07:04

文件大小: 14.67 MB      文件类型: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting...  
引擎检出: 1 / 27      分析环境: Win10(1903 64bit,Office2016)

HASH  
SHA256: 2ee52db4edf06e527dd7bf1f30a2b6ba52353fac8f8ca78647c9f1668b013ffd  
MD5: ac770f1cb8e8190fabcd1dac18aeca371  
SHA1: 38f1a1d34f00ac31bfceb60d739ecfc464d87b71

## 行为检测

MITRE ATT&CK™ 矩阵 (技术) 检测到 11 条技术指标。 [查看完整结果](#)

Win10(1903 64bit,Office2016)

### 高危行为 (4)

全部展开

#### 系统环境探测

枚举系统的服务，可能被恶意程序用于检测是否运行在虚拟环境中

Win10(1903 64bit,Office2016)



#### 系统敏感操作

可疑的父进程创建了脚本进程

Win10(1903 64bit,Office2016)



在用户目录下创建可执行文件

Win10(1903 64bit,Office2016)



更改防火墙设置

Win10(1903 64bit,Office2016)



### 可疑行为 (21)

全部展开

#### 反检测技术

查询系统硬盘大小，某些恶意程序会根据硬盘大小来判定是否运行在虚拟机中

Win10(1903 64bit,Office2016)



检查适配器地址，可用于检测虚拟网络接口

Win10(1903 64bit,Office2016)



#### 反逆向工程

尝试严重拖慢分析任务的进度

Win10(1903 64bit,Office2016)



检测内核调试器是否在调试进程

Win10(1903 64bit,Office2016)



创建PAGE\_GUARD属性的内存页，通常用于反逆向和反调试

Win10(1903 64bit,Office2016)



#### 系统环境探测

疑似获取机器信息和检测时间

Win10(1903 64bit,Office2016)



扫描Windows任务栏，（常用于注入explorer）

Win10(1903 64bit,Office2016)



#### 持久化

创建快捷方式

Win10(1903 64bit,Office2016)



#### 信息搜集

安装消息钩子

Win10(1903 64bit,Office2016)



获取按键信息

Win10(1903 64bit,Office2016)



#### 网络相关

HTTP流量具有可疑的特征，可能包含恶意的流量

Win10(1903 64bit,Office2016)



一般行为	感知时区，常用于躲避恶意软件分析系统	Win10(1903 64bit,Office2016)	▼
	请求访问系统服务	Win10(1903 64bit,Office2016)	▼
	样本从自身读取所需要的信息	Win10(1903 64bit,Office2016)	▼
	创建驱动文件	Win10(1903 64bit,Office2016)	▼
	将文件属性设置为删除	Win10(1903 64bit,Office2016)	▼
	利用Windows操作系统的空闲时间计算系统持续运行时间	Win10(1903 64bit,Office2016)	▼
系统敏感操作	创建一个或多个可疑进程	Win10(1903 64bit,Office2016)	▼
	使用windows实用程序代替windows的基础功能	Win10(1903 64bit,Office2016)	▼
	绕过PowerShell执行策略	Win10(1903 64bit,Office2016)	▼
	检查系统上的唯一标识符是否具有可疑的权限	Win10(1903 64bit,Office2016)	▼
! 通用行为 (17)			全部展开
静态文件特征	在文件内存中发现IP地址或url	Win10(1903 64bit,Office2016)	▼
	安装程序	Win10(1903 64bit,Office2016)	▼
系统环境探测	查询Windows的产品ID	Win10(1903 64bit,Office2016)	▼
	包含查询计算机时区的功能	Win10(1903 64bit,Office2016)	▼
	读取计算机名称	Win10(1903 64bit,Office2016)	▼
	查询系统用户名	Win10(1903 64bit,Office2016)	▼
	获取系统信息	Win10(1903 64bit,Office2016)	▼
	查询计算机名	Win10(1903 64bit,Office2016)	▼
	收集操作系统硬件相关的指纹信息（MachineGuid，DigitalProductId，SystemBiosDate）	Win10(1903 64bit,Office2016)	▼
网络相关	发起了HTTP请求	Win10(1903 64bit,Office2016)	▼
一般行为	创建日志文件	Win10(1903 64bit,Office2016)	▼
	在临时目录中创建文件	Win10(1903 64bit,Office2016)	▼
	读取系统的信任设置	Win10(1903 64bit,Office2016)	▼
	枚举文件和目录	Win10(1903 64bit,Office2016)	▼
	向系统软件管理程序注册了卸载方法	Win10(1903 64bit,Office2016)	▼

在文件系统中创建脚本文件

Win10(1903 64bit,Office2016)

在文件系统中创建可执行文件

Win10(1903 64bit,Office2016)

多引擎检测

检出率：1 / 27

最近检测时间：2024-06-26 10:37:52

引擎	检出	引擎	检出
ESET	! MSIL/LetsVPN.A potentially unwante...	微软 (MSE)	无检出
卡巴斯基 (Kaspersky)	无检出	小红伞 (Avira)	无检出
IKARUS	无检出	大蜘蛛 (Dr.Web)	无检出
Avast	无检出	AVG	无检出
GDATA	无检出	K7	无检出
安天 (Antiy)	无检出	江民 (JiangMin)	无检出
360 (Qihoo 360)	无检出	Baidu	无检出
NANO	无检出	Trustlook	无检出
瑞星 (Rising)	无检出	熊猫 (Panda)	无检出
Sophos	无检出	ClamAV	无检出
WebShell专杀	无检出	Baidu-China	无检出
MicroAPT	无检出	OneAV	无检出
OneStatic	无检出	MicroNonPE	无检出
OneAV-PWSH	无检出		

收起全部

静态分析

基础信息

文件名称	2ee52db4edf06e527dd7bf1f30a2b6ba52353fac8f8ca78647c9f1668b013ffd
文件格式	EXE:x86
文件类型(Magic)	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
文件大小	14.67MB
SHA256	2ee52db4edf06e527dd7bf1f30a2b6ba52353fac8f8ca78647c9f1668b013ffd
SHA1	38f1a1d34f00ac31bfceb60d739ecfc464d87b71
MD5	ac770f1cb8e8190fabc1dac18aeca371
CRC32	8CDE32AA
SSDEEP	393216:le2m5Tvm98UwJ5LDYkzGaJfOdFy65fCT33RaKZ7:oxTILsCGaiyNxak
TLSH	T1D4F63349AC83FC97C4A78E31D6F1C7F486BAD7278901CE7164A8A725EE713F43829911
AuthentiHash	D9243FCAAF7F925FD4D1E9C7C0E05F0920EB5A7E3854BF495B31297044DF96C6

peHashNG	a358933b8b03f35aa6d62f9d138e75bbe584de91021a06e880d603cf49afbe7
RichHash	dbbea5de38bb665ba46f5da13ef89ab8
impfuzzy	48:JBeZv2GaOlzYArO8AltKz+eOxHALlIa/5LRFzn7+P9KQJ45EQI/KAEowrSv0WbXy:n+v3aVz0H1Wx94pKsU
ImpHash	b34f154ec913d2d2c435cbd644e91687
ICON_SHA256	09deeb5ea41ab3a24325c1f8620cb8c2c67ad67bfad0377554bef47352988001
ICON_DHash	d0e0f86cf4dcddcc
Tags	exe,lang_english,installer,codesign,signed,valid_signature,encrypt_algorithm

元数据

ExifTool	
FileType	Win32 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2018:01:30 11:57:48+08:00
ImageFileCharacteristics	No relocs, Executable, No line numbers, No symbols, 32-bit
PEType	PE32
LinkerVersion	6.0
CodeSize	26624
InitializedDataSize	186368
UninitializedDataSize	2048
EntryPoint	0x338f
OSVersion	4.0
ImageVersion	6.0
SubsystemVersion	4.0
Subsystem	Windows GUI

TrID	
47.3% (.EXE)	Win32 Executable MS Visual C++ (generic) (31206/45/13)
15.9% (.EXE)	Win64 Executable (generic) (10523/12/4)
9.9% (.DLL)	Win32 Dynamic Link Library (generic) (6578/25/2)
7.6% (.EXE)	Win16 NE executable (generic) (5038/12/1)
6.8% (.EXE)	Win32 Executable (generic) (4505/5/1)

DIE	
链接器	Microsoft Linker(6.0)
编译器	Microsoft Visual C/C++(13.10.4035)[C]
工具	Visual Studio()
安装程序	Nullsoft Scriptable Install System(3.03)[zlib,solid]
字节序	LE
模式	32
程序类型	GUI
文件类型	PE32
熵	7.99695318725892
语言	C/C++
操作系统	Windows(95)[I386, 32位, GUI]

格式深度分析

文档分析

PE头信息

平台	Intel 386 or later processors and compatible processors
----	---

子系统	Windows graphical user interface (GUI) subsystem
编译时间戳	2018-01-30 11:57:48
入口点(OEP)	0x338f
入口所在段	.text
镜像基地址	0x400000
节区数量	5
LinkerVersion	6

签名信息

签名验证	Signed	
签名时间	14:03 2024/5/10	
签名者	LetsGo Network Incorporated	展开
	Sectigo Public Code Signing CA R36	展开
	Sectigo Public Code Signing Root R46	展开
	Sectigo (AAA)	展开
会签者	DigiCert Timestamp 2023	展开
	DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA	展开
	DigiCert Trusted Root G4	展开
	DigiCert	展开

导入表(7)

DLL	DLL描述	函数数量	
KERNEL32.dll	-	65	展开
USER32.dll	-	65	展开
GDI32.dll	-	8	展开
SHELL32.dll	-	6	展开
ADVAPI32.dll	-	13	展开

查看全部

PE节区(5)

节名	虚拟地址	虚拟大小	物理地址	物理大小	节权限	熵值	节哈希
.text	0x00001000	0x00006627	0x00000400	0x00006800	R-E	6.452235553722483	8c030dfed318c62753a7b0d60218279b
.rdata	0x00008000	0x0000149a	0x00006c00	0x00001600	R--	5.007075185851696	966a3835fd2d9407261ae78460c26dcc
.data	0x0000a000	0x0002aff8	0x00008200	0x00000600	RW-	4.03532418489749	939516377e7577b622eb1ffdc4b5rlh4a

PE资源(23)

资源名	资源类型	资源大小	偏移地址	语言	子语言
RT_ICON	data	0x0000616b	0x000674c0	LANG_ENGLISH	SUBLANG_ENGLISH_US

RT_ICON	data	0x000025a8	0x0006d630	LANG_ENGLISH	SUBLANG_ENGLISH_US
RT_ICON	data	0x000010a8	0x0006fbd8	LANG_ENGLISH	SUBLANG_ENGLISH_US
RT_ICON	data	0x000008a8	0x00070c80	LANG_ENGLISH	SUBLANG_ENGLISH_

文件内容

字符串

Unicode ASCII

Software\Microsoft\Windows\CurrentVersion  
RichEdit  
Control Panel\Desktop\ResourceLocale  
#+3;CScs  
\\Microsoft\Internet Explorer\Quick Launch  
RichEdit20M

URLs

http://ocsp.digicert.com  
http://ocsp.comodoca.com  
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#  
http://ocsp.sectigo.com  
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0  
https://sectigo.com/CPS0

沙箱动态检测

Win10(1903 64bit,Office2016)

运行截图

无运行截图

网络行为

指纹	域名	DNS	HTTP	TCP	Hosts	HTTPS	UDP	SMTP	ICMP	IRC	Dead-Hosts
5	6	6	1	6	5	0	0	0	0	0	0

指纹 : 5

协议	地址	指纹类型	指纹哈希	详情
HTTP	目的 IP 52.76.166.240:80	clientHeaderHash	3e9c8269ef72de5c62f1fa3440974639	request_uri_path,request_uri_query,request_uri_query_parameter,host,upgrade,connection,sec_websocket_version,sec_websocket_key
HTTP	目的 IP 52.76.166.240:80	hfingerHash	80594d0966277bc14fe0e315dcbc4d78	1.9 2 1.1  1.7 0.9 GE 1 ho,up,co,e4dd8fa1,7234ece6,or co:Up
TLS	目的 IP 4.152.45.219:443	JA3	6e253bca1914df137ef73d14bcb57cc0	771,49161-49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0
TLS	源 IP 4.152.45.219:443	JA3S	a9e3ed16ee3208291487c8d2aa2ad924	771,49200,0-65281-11



协议	地址	指纹类型	指纹哈希	详情
TLS	源 IP 4.152.45.219:443	JA3S	364ff14b04ef93c3b4cfa429d729c0d9	771,49200,65281

域名 : 6

域名	微步判定	情报内容	当前解析IP
in.appcenter.ms	安全	白名单	4.152.45.219
ocsp.sectigo.com	安全	白名单	172.64.149.23
ws-ap1.pusher.com	安全	白名单	52.76.166.240
www.baidu.com	安全	白名单 icp	110.242.68.4
www.google.com	安全	白名单	157.240.17.35

< 1 / 2 > 每页显示 5条 ▾

DNS : 6

域名	请求	应答
ocsp.sectigo.com	A	CNAME → ocsp.comodoca.com.cdn.cloudflare.net A → 172.64.149.23 104.18.38.233
ws-ap1.pusher.com	A	CNAME → socket-ap1-ingress-1471706552.ap-southeast-1.elb.amazonaws.com A → 52.76.166.240 54.251.147.3 18.136.43.97
in.appcenter.ms	A	CNAME → in-prod-pme-eastus2-ingestion-66ddb56a.trafficmanager.net in1-gw2-01-3d6c3051.eastus2.cloudapp.azure.com A → 4.152.45.219
www.yandex.com	A	CNAME → yandex.com A → 5.255.255.50 77.88.55.88 5.255.255.5 77.88.55.70
www.baidu.com	A	CNAME → www.a.shifen.com A → 110.242.68.4 110.242.68.3

< 1 / 2 > 每页显示 5条 ▾

HTTP : 1






Timeshift	进程	响应头	URL	目标地址	内容
128ms	(3784) LetsPRO.exe	GET   101	http://ws-ap1.pusher.com:80/app/4fc436ef...sion=1.1.2	52.76.166.240:80	0 B ↑ empty 0 B ↓ empty

TCP : 6

Timeshift	进程	目标地址	微步判定	情报内容	流量
130ms	(3784) LetsP...	 5.255.255.50:443	安全	<span>白名单</span> <span>搜索引擎爬虫</span>	0 B ↑ 0 B ↓
130ms	(3784) LetsP...	 110.242.68.4:443	未知	<span>网关</span>	0 B ↑ 0 B ↓
131ms	(3784) LetsP...	 52.76.166.240:80	未知	<span>亚马逊云主机</span> <span>IDC服务器</span>	269 B ↑ 404 B ↓
131ms	(3784) LetsP...	 4.152.45.219:443	未知	-	297 B ↑ 3.36 KB ↓
131ms	(3784) LetsP...	 4.152.45.219:443	未知	-	203 B ↑ 137 B ↓

< 1 / 2 > 每页显示 5条 ▾

Hosts : 5

IP地址	微步判定	情报内容	地理信息	ASN	使用场景
110.242.68.4	未知	<span>网关</span>	 China Hebei Bao ding City	4837(CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN)	-
157.240.17.35	未知	<span>CDN服务器</span>	 Switzerland Zurich	32934(FACEBOOK, US)	-
4.152.45.219	未知	-	 United States Virginia Virginia Beach	3356(LEVEL3, US)	-
52.76.166.240	未知	<span>亚马逊云主机</span> <span>IDC服务器</span>	 Singapore Singapore	16509(AMAZON-02, US)	Cloud Provider
5.255.255.50	安全	<span>白名单</span> <span>搜索引擎爬虫</span>	 Russia Moscow	13238(YANDEX, RU)	-

📁 释放文件 (38)

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定	操作
<b>AddWindowsSecurityExclusion.ps1(318 B)</b> 文件类型：ASCII text, with CRLF line terminators 文件路径：C:\Program Files (x86)\letsvpn\AddWindowsSecurityExclusion.ps1 SHA256：a9901397d39c0fc74adfdb95dd5f95c3a14def3f9d58ef44ab45fc74a56d46df	(6576) letsvpn-3.7.1.exe	0/27	-	安全	📄
<b>LetsPRO.exe(241.48 KB)</b> 文件类型：PE32 executable (GUI) Intel 80386, for MS Windows 文件路径：C:\Program Files (x86)\letsvpn\LetsPRO.exe SHA256：44899d913eb45db2654880c5f096fe5d24245d24c6f765320b97be432da5ad81	(6576) letsvpn-3.7.1.exe	0/27	-	安全	📄
<b>Update.exe(1.82 MB)</b> 文件类型：PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows 文件路径：C:\Program Files (x86)\letsvpn\Update.exe SHA256：0d069ea8705a717fca60e15d71ac5ed67daca175e4e8459de10bf75f2a692b38	(6576) letsvpn-3.7.1.exe	0/27	-	安全	📄

释放样本	进程	多引擎检出	威胁类型/木马家族	微步判定	操作
<div>CommunityToolkit.Mvvm.dll(110.48 KB)</div> <div>文件类型：PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows</div> <div>文件路径：C:\Program Files (x86)\letsvpn\app-3.7.1\CommunityToolkit.Mvvm.dll</div> <div>SHA256：900878978ecdc72d2383b27bfdb3a174a13d7a3718005801dd469d71ea887c18</div>	(6576) letsvpn-3.7.1.exe	0/27	-	安全	<a href="#">↓</a>
<div>DeltaCompressionDotNet.MsDelta.dll(16.48 KB)</div> <div>文件类型：PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows</div> <div>文件路径：C:\Program Files (x86)\letsvpn\app-3.7.1\DeltaCompressionDotNet.MsDelta.dll</div> <div>SHA256：e562a936512e469628ba1ece2ab95c2112a67d848c38278e4aed77ec47a449c3</div>	(6576) letsvpn-3.7.1.exe	0/27	-	安全	<a href="#">↓</a>