

安全威胁每周警讯

2020/03/23 ~ 2020/03/29

本周威胁指数



亚信安全 网络安全监控中心

TOP 10 前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	PE_RAMNIT.DEN	File infector	★	↑	该文件感染程序执行删除的文件。结果，被删除文件的恶意例程会显示在受影响的系统上。
2	Trojan.ALS.BURSTED.AA	Trojan	★	↓	用于 AutoCAD 使用的脚本语言，用于在 AutoCAD 启动时加载的脚本。
3	WORM_WCRY.F	Worm	★★★	↓	挖矿病毒，通过其他恶意软件感染。
4	ALS_DUXFAS.K	Trojan	★	→	该木马可能会与恶意软件包捆绑在一起作为恶意软件组件。
5	Ransom_WCRY.THAOBFJ	Worm	★★★★	↓	勒索病毒，通过其他恶意软件感染。
6	LNK_DORKBOT.SM1	Trojan	★	↑	木马病毒，它可能是使用者手动安装的
7	HTML_RAMNIT.SM	Trojan	★★★	↑	此特洛伊木马执行已删除的文件。在受影响的系统上显示已删除文件的恶意例程
8	TROJ_EQUATED.J	Trojan	★★	↑	此特洛伊木马可能与恶意软件包捆绑在一起作为恶意软件组件。它作为被其他恶意软件丢弃的文件或用户在访问恶意站点时在不知不觉中下载的文件到达系统。它可以由用户手动安装。
9	Worm.Win32.OTORUN.NKLSFG	Worm	★★	↑	蠕虫病毒，通过其他恶意软件感染。
10	Coinminer_TOOLXMR.E-WIN32	Coinminer	★★	→	挖矿病毒，可能是和其他病毒一并下载，需要运行在一些特殊的参数环境中

病毒通告

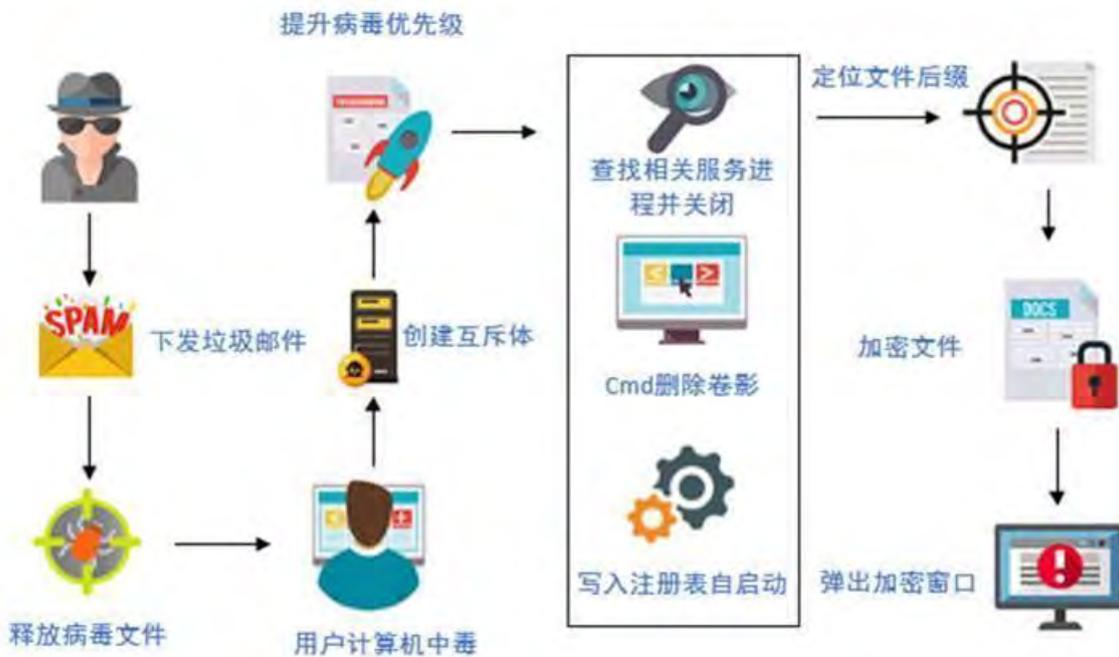
2020年3月27日

海盗王勒索病毒通告

事件描述

近日，亚信安全截获新型海盗王勒索病毒，该病毒的勒索界面中有海盗图标，因此得名。经过分析，我们发现该病毒为 CRYSIS 勒索家族的最新变种文件，其通过垃圾邮件附件传播，加密磁盘中的文件，加密后的文件扩展名为 `id-XXXXXX.wang_team888@aol.com.ROGER`，亚信安全将其命名为 [Ransom.Win32.CRYSIS.SM](#)。

加密流程



详细分析

病毒首先会向寄存器写入特定扩展名，后面将会对这些扩展名文件进行加密：


```

Address  UNICODE dump
0089FAE8 Global\synchronize_E27793A.....
0089FB68 .....
0089FBE8 .....
0089FC68 .....
0089FCE8 .....
0089FD68 .....
0089FDE8 .....
0089FE68 .....
0089FEE8 .....
0089FF68 .....
0089FFE8 .....
008A0068 .....
008A00E8 .....

0018FD84 0089F898 UNICODE "Global\synchronize_"
0018FD88 00000041
0018FD8C 00000000
0018FD90 00882F68 ASCII "E27793."
0018FD94 00320045
0018FD98 00370037
0018FD9C 00330039
0018FDA0 00890000
0018FDA4 0089FAE8 UNICODE "Global\synchronize_E27793A"
0018FDA8 00000006
0018FDAC 0018FDC4
0018FDB0 00408303 RETURN to 海盗王.00408303 from 海盗王.00408303
0018FDB4 00000001
0018FDB8 000000A0
  
```

然后开始枚举系统中是否含有以下进程，若有以下进程，则将其终止，并停止所有数据库相关的进程服务，为后面加密数据库做准备：

- 1c8.exe
- 1cv7.exe
- outlook.exe
- postgres.exe
- mysqld.exe
- sqlservrexe
- Sqlwriter
- Mssqlserver
- Sqlserveradhelper
- mysqld-nt.exe
- FirebirdGuardianDefaultInstance
- FirebirdServerDefaultInstance

```

Hex dump  UNICODE
31 00 63 00 1c8.exe;
31 00 63 00 1cv77.ex
65 00 38 00 e;outloo
60 00 2E 00 k.exe;po
73 00 74 00 stgres.e
78 00 65 00 xe;mysql
64 00 2D 00 d-nt.exe
38 00 6D 00 ;mysqld.
65 00 76 00 exe;sqls
65 00 72 00 ervr.exe
3B 00 00 00 ;.....
00 00 00 00

0018FC38 00288C00
0018FC3C 00000000
0018FC40 00000000
0018FC44 0018FC5C
0018FC48 004068BE 海盗王.004068BE
0018FC4C 00280000 ASCII "宝宽q9"
0018FC50 00000000
0018FC54 0029F888
0018FC58 002C0268 UNICODE "1c8.exe;1cv77.exe;outlook.exe;postgres.exe;
0018FC5C 0018FC88
0018FC60 00405AC3 海盗王.00405AC3
0018FC64 0029F888
0018FC68 00000100
  
```

```

address  Hex dump  UNICODE
00309738 46 00 69 00 Firebird
00309748 47 00 75 00 Guardian
00309758 44 00 65 00 DefaultI
00309768 6E 00 73 00 nstance;
00309778 46 00 69 00 Firebird
00309788 53 00 65 00 ServerDe
00309798 66 00 61 00 FaultIns
003097A8 74 00 61 00 tance;sq
003097B8 6C 00 77 00 lwriter;
003097C8 6D 00 73 00 mssqlser
003097D8 76 00 65 00 ver;sqls
003097E8 65 00 72 00 erveradh
003097F0 5F 00 68 00 tance;sq

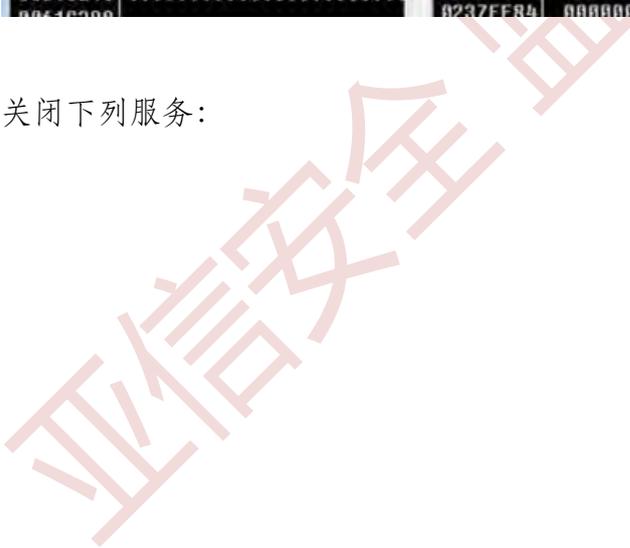
024DFF68 0041798C 海盗王.0041798C
024DFF6C 0040E080 海盗王.0040E080
024DFF70 00309630 Arg1 = 00309630
024DFF74 00000000 Arg2 = 00000000
024DFF78 00309630 UNICODE "1c8.exe;1cv77.exe;outlook.exe;postgres
024DFF7C 00000000
024DFF80 00000000
024DFF84 00309738 UNICODE "FirebirdGuardianDefaultInstance;fireb
024DFF88 024DFF94
024DFF8C 774233CA
024DFF90 00000000
024DFF94 024DFFD4
024DFF98 77A99E02
024DFF9C 00000000
  
```

```

FirebirdGuardianDefaultInstance;FirebirdServerDefaultInstance;sq
lwriter;mssqlserver;sqlserveradhelper;.....
00000000 Arg2 = 00000000
0018FDC0 00300268 UNICODE "1c8.exe;1cv77.exe;outlook.exe;postgres.exe;mysqld-
0018FDC4 00000000
0018FDC8 00000000 uc2_32_776230EB
0018FDCC 00300268 UNICODE "FirebirdGuardianDefaultInstance;FirebirdServerDefa
0018FDD0 0018FF88
0018FDD4 00400B2C RETURN to 海盗王.<ModuleEntryPoint>+15C from 海盗王.00400B18
0018FDD8 00000000
  
```


The screenshot displays a debugger's assembly view and registers window. The assembly code on the left shows instructions such as `add esp, 0x10`, `mov [local.3], eax`, and `call 海盗王.004018A0`. The registers window on the right shows the state of various registers, with EAX containing `002E7620` and EIP containing `004067C0`. Below the assembly view, a hex dump shows the content of a file, with the UNICODE column displaying `boot.ini` and `bootfont.bin;ntldr;ntdetect.com;io.sys;`.

病毒关闭下列服务：



Address	UNICODE dump
00538E16醜S截S .!.¥.....■.醜S鄭S .!.■.....■.鄆S郤S .!.■..
00538E96■.鄆S參S .!.A.....■.遯S途S .!.■.....■.兀...逆S迦S .!.■
00538F16■.达S迈S .!.A.....■.■.辦S辈S .!.■.....■.兀...Windows
00538F96	Update.wuauseru.Windows Search.WSearch.Security Center.wscsvc.W
00539016	indows Management Instrumentation.Winmgmt.WinHTTP Web Proxy Auto
00539096	-Discovery Service.WinHttpAutoProxySvc.Windows Defender.WinDefen
00539116	d.Windows Error Reporting Service.WerSvc.Diagnostic Service Host
00539196	.WdiServiceHost.UMware 物理磁盘助手服务.UMware Physical Disk Hel
00539216	ice.UMware Tools.UMTools.UMware Alias Manager and Ticket Service
00539296	.UGAuthService.Desktop Window Manager Session Manager.UxSms.Dist
00539316	ributed Link Tracking Client.TrkWks.Themes.Themes.Superfetch.Sys
00539396	Main.SSDP Discovery.SSDPSRU.Print Spooler.Shell Hardware
00539416	Detection.ShellHWDetection.System Event Notification Service.SE
00539496	NS.Task Scheduler.Schedule.Security Accounts Manager.SamSs.Remot
00539516	e Procedure Call (RPC).RpcSs.RPC Endpoint Mapper.RpcEptMapper.Us
00539596	er Profile Service.ProfSvc.Power.Power.Plug and Play.PlugPlay.Pro
00539616	gram Compatibility Assistant Service.PcaSvc.Network Store Inter
00539696	face Service.nsi.Network Location Awareness.MlaSvc.Network List
00539716	Service.netprofm.Network Connections.Netman.Distributed Transact
00539796	ion Coordinator.MSDTC.Windows Firewall.MpsSvc.TCP/IP NetBIOS Hel
00539816	per.lmhosts.Workstation.LanmanWorkstation.Server.LanmanServer.IP
00539896	Helper.iphlpvc.Group Policy Client.gpsvc.Windows Font Cache Se
00539916	rvice.FontCache.COM+ Event System.EventSystem.Windows Event Log.
00539996	eventlog.Diagnostic Policy Service.DPS.DNS Client.Dnscache.DHCP
00539A16	Client.Dhcp.DCOM Server Process Launcher.DcomLaunch.Offline File
00539A96	s.CscService.Cryptographic Services.CryptSvc.Background Intellig
00539B16	ent Transfer Service.BITS.Base Filtering Engine.BFE.Windows Audi
00539B96	o.AudioSrv.Windows Audio Endpoint Builder.AudioEndpointBuilder.A

调用系统函数，遍历磁盘 A~Z:

```

v10 = (char *)get_user_file((int)&unk_40E508, (int)&unk_40E080, 128, 2u); // 获取用户文件夹
v2 = sub_406780();
v9 = sub_406850(8 * v2);
v8 = 0;
v15 = dirve() & 0xFFFFFFF; // 调用遍历磁盘函数
for ( i = 0; i < 32; ++i )
{
    if ( v15 & (1 << i) )
    {
        v11 = *(_WORD *)&v10[2 * i];
        v12 = 58;
        v13 = 0;
        v3 = traverse((int)&v11, a1, 1, a2); // 遍历磁盘数据
        *(_DWORD *)&v9 + 4 * v8 = v3;
        if ( v3 )
            ++v8;
        v4 = traverse((int)&v11, a1, 0, a2);
        *(_DWORD *)&v9 + 4 * v8 = v4;
        if ( v4 )
            ++v8;
    }
}

```

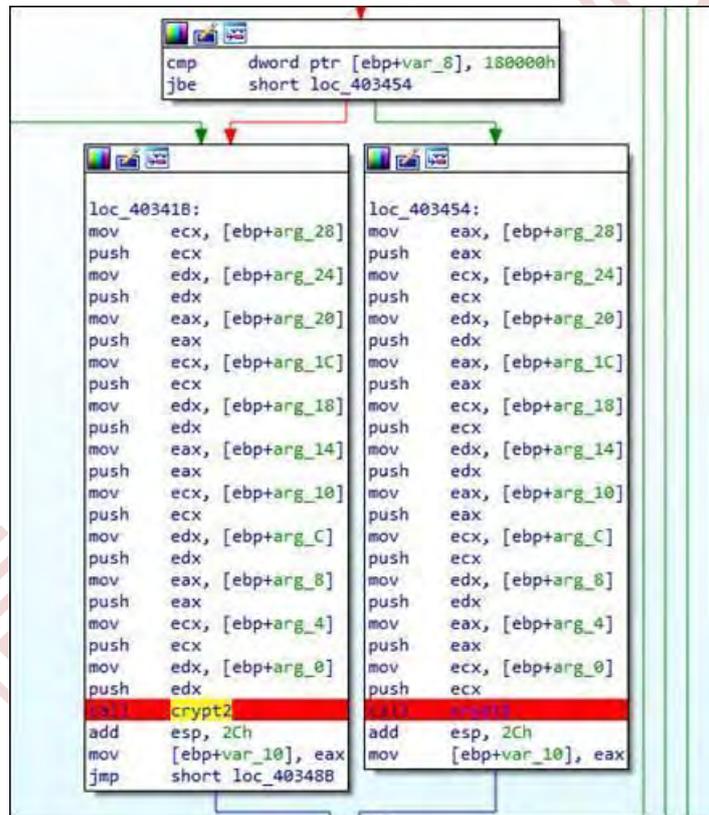
```

0018FD9C 004097D6 CALL to GetLogicalDrives from 海盗王.004097D1
0018FDA0 00000000
0018FDA4 0018FDC8
0018FDA8 00000000
0018FDAC 002A2E08
0018FDB0 002A1BC0 UNICODE "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
0018FDB4 00000003
    
```

加密分析:

病毒首先判断文件大小, 以文件大小来进行加密, 调用的是基于 AES 的高级分组加密算法

Rijndael:

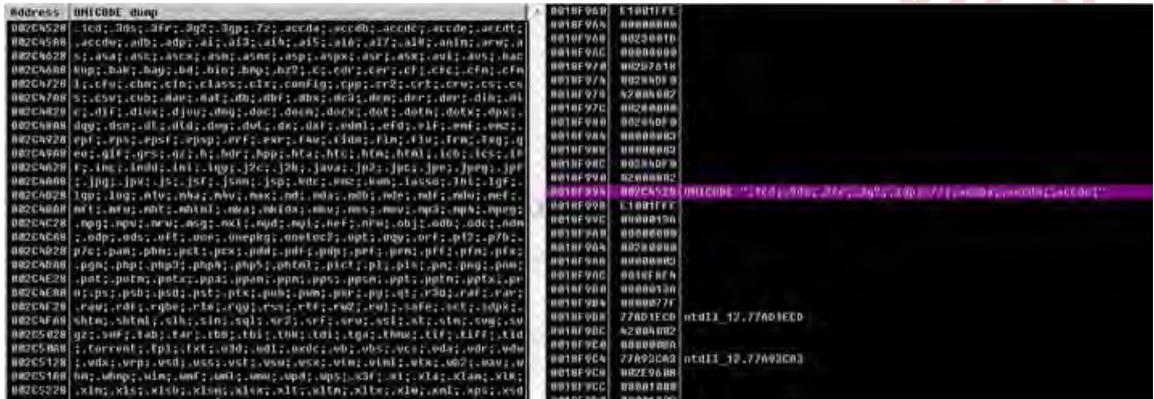


```

if ( u4 == 1 )
{
while ( 1 )
{
v14 = v16[7];
v16[8] = dword_40D488[v17] ^ Rijndael_Te1[v14 >> 24] & 0xFF ^ Rijndael_Te0[(unsigned __int6)v14] & 0xFF00 ^ Rijndael_Te3[(unsigned __int6)v14 >> 8] & 0xFF;
v16[9] = v16[8] ^ v16[3];
v16[10] = v16[9] ^ v16[2];
result = v16[10] ^ v16[3];
v16[11] = result;
if ( ++v17 == 7 )
break;
v15 = v16[11];
v16[12] = Rijndael_Te1[(unsigned __int6)v15] & 0xFF ^ Rijndael_Te0[(unsigned __int6)v15 >> 8] & 0xFF00 ^ Rijndael_Te3[(v15 >> 16) & 0xFF] & 0xFF0000 ^
v16[13] = v16[12] ^ v16[5];
v16[14] = v16[13] ^ v16[4];
v16[15] = v16[14] ^ v16[7];
v16 += 8;
}
}

```

病毒会枚举加密后缀:



加密后文件后缀为 [id-XXXXXX.wang team888@aol.com.ROGER](#):

02C9FF34	03030048	Unicode "C:\\$Recycle.Bin\S-1-5-21-53883564-2239540567-35130"
02C9FF38	00007FFF	
02C9FF3C	00418204	Unicode "ssbss"
02C9FF40	0035EFD0	Unicode "C:\\$Recycle.Bin\S-1-5-21-53883564-2239540567-35130"
02C9FF44	002D8CC0	Unicode ".id"
02C9FF48	00000004	
02C9FF4C	002C5348	
02C9FF50	002C1C98	Unicode ".[wang_team888@aol.com]"
02C9FF54	002D7A98	Unicode ".ROGER"
02C9FF58	00000000	
02C9FF5C	002D9128	ASCII "E27793"
02C9FF60	00000000	
02C9FF64	0035F05A	Unicode ".zip"
02C9FF68	03030048	Unicode "C:\\$Recycle.Bin\S-1-5-21-53883564-2239540567-35130"
02C9FF6C	002D8CA8	

加密国家和地区黑名单:

```

005181A0 ... 鵠泐 en-US.ar-SA.pt-BR.zh-TW.zh-CN.zh-HK.cs-CZ.da-DK.el-GR.
00518220 -ES.fi-FI.fr-FR.de-DE.he-IL.hu-HU.it-IT.ja-JP.ko-KR.nl-NL.nb-NO.
005182A0 p1-PL.pt-PT.ru-RU.sv-SE.tr-TR.bg-BG.hr-HR.et-EE.lv-LV.lt-LT.ro-R
00518320 0.sr-Latn-CS.sk-SK.sl-SI.th-TH.uk-UA.fy-NL.qps-ploc.qps-plocm..
005183A0 鵠泐 鵠泐
  
```

病毒最后调用 releaseMutex，释放互斥变量：

0040B018	EnterCriticalSection	KERNEL32
0040B01C	ReleaseMutex	KERNEL32
0040B020	CloseHandle	KERNEL32

该病毒勒索界面：



解决方案

- ✓ 不要点击来源不明的邮件以及附件；
- ✓ 不要点击来源不明的邮件中包含的链接；
- ✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
- ✓ 打开系统自动更新，并检测更新进行安装；
- ✓ 尽量关闭不必要的文件共享；
- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案

- ✓ 亚信安全病毒码版本 15.765.60，云病毒码版本 15.765.71，全球码版本 15.767.00 已经可以检测，请用户及时升级病毒码版本。

IOC

文件名	SHA-1	亚信安全检测名
海盗王.exe	F92F7E91F9160626953711380140D2C04865E62D	Ransom.Win32.CRYSIS.SM

亚信安全 监控中心 提供

