2017 年 9 月 18 日，星期一

CCleanup：大量设备面临风险

作者：Edmund Brumaghin、Ross Gibb、Warren Mercer、Matthew Molyett 和 Craig Williams

*9 月 18 日更新：*根据相关报告，CCleaner Cloud 版本 1.07.3191 也受到影响
*9 月 19 日更新：*Morphisec 和思科在不同的实际应用情况下发现此问题，并分别向 Avast 报告。
*9 月 19 日更新：*对域生成算法 (DGA) 域的解析方式存在一些困惑。

CCBkdr 使用的回退命令和控制方案包括：
1. 生成每月域名（2017 年全部被 Talos 所控制）
2. 请求该域的 AAA 记录。
3. 将真实目的 IP 地址的 16 位编码到第一个 AAA 记录中，并将另 16 位编码到第二个 AAA 记录中
4. 然后，计算并连接到真实的目的 IP 地址。
要控制这些连接，Talos 必须创建两个 IP 地址，这样才能将其送入应用中并解析为 Sinkhole IP 地址。
我们随机生成一个 32 位数据。将其中 16 位与目的地址的 16 位组合，创建第一个 AAA 记录。其余的随机 16 位与目的地址的其余 16 位组合，创建第二个 AAA 记录。
然后，我们将得到的两个 AAA 记录 IP 地址分配给 DNS 配置。
除了确定可通过组合所选地址来创建目的地址外，我们未对所选地址执行其他分析。

*9 月 20 日更新：*有关 C2 和负载的后续研究，请访问：
http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

引言

要将恶意软件分发到目标组织中，供应链攻击是非常有效的方式。这是因为在供应链攻击中，攻击者利用了制造商或供应商与客户之间的信任关系。攻击者可以出于多种不同原因，滥用这种信任关系来攻击组织和个人。2017 年早些时候投放到网上的 Nyetya 蠕虫就反映了这类攻击的强大影响力。最初的感染媒介往往可以保持相当长的时间不被发现，正如 Nyetya 的情况一样。幸运的是，借助 AMP 等工具，我们可以获得更高的可视性，这往往可以帮助我们有效找到始作俑者。

在 Talos 最近发现的一个案例中，攻击者利用软件供应商用来分发合法软件包的下载服务器，向不知情的受害者传送恶意软件。在一段时间内，Avast 分发的具有合法签名的 CCleaner 5.33 版本除了安装 CCleaner 之外，还包含一个多阶段恶意软件负载。根据 CCleaner 发布的数据，截至 2016 年 11 月，其总下载量超过 20 亿，从用户增长率来看，每周新增用户达到 500 万。考虑到被感染的计算机网络可能造成的潜在危害，即使受到影响的版本只占如此小的比例，我们仍然决定迅速采取行动。2017 年 9 月 13 日，思科 Talos 在第一时间将发现通知 Avast，以便他们启动相应的响应活动。接下来的部分将介绍有关此攻击的具体细节。

技术详情

CCleaner 是一款供用户对系统执行日常维护的应用。其功能包括清理临时文件，分析系统以确定性能优化方法，以及提供简化的方法来管理已安装的应用。

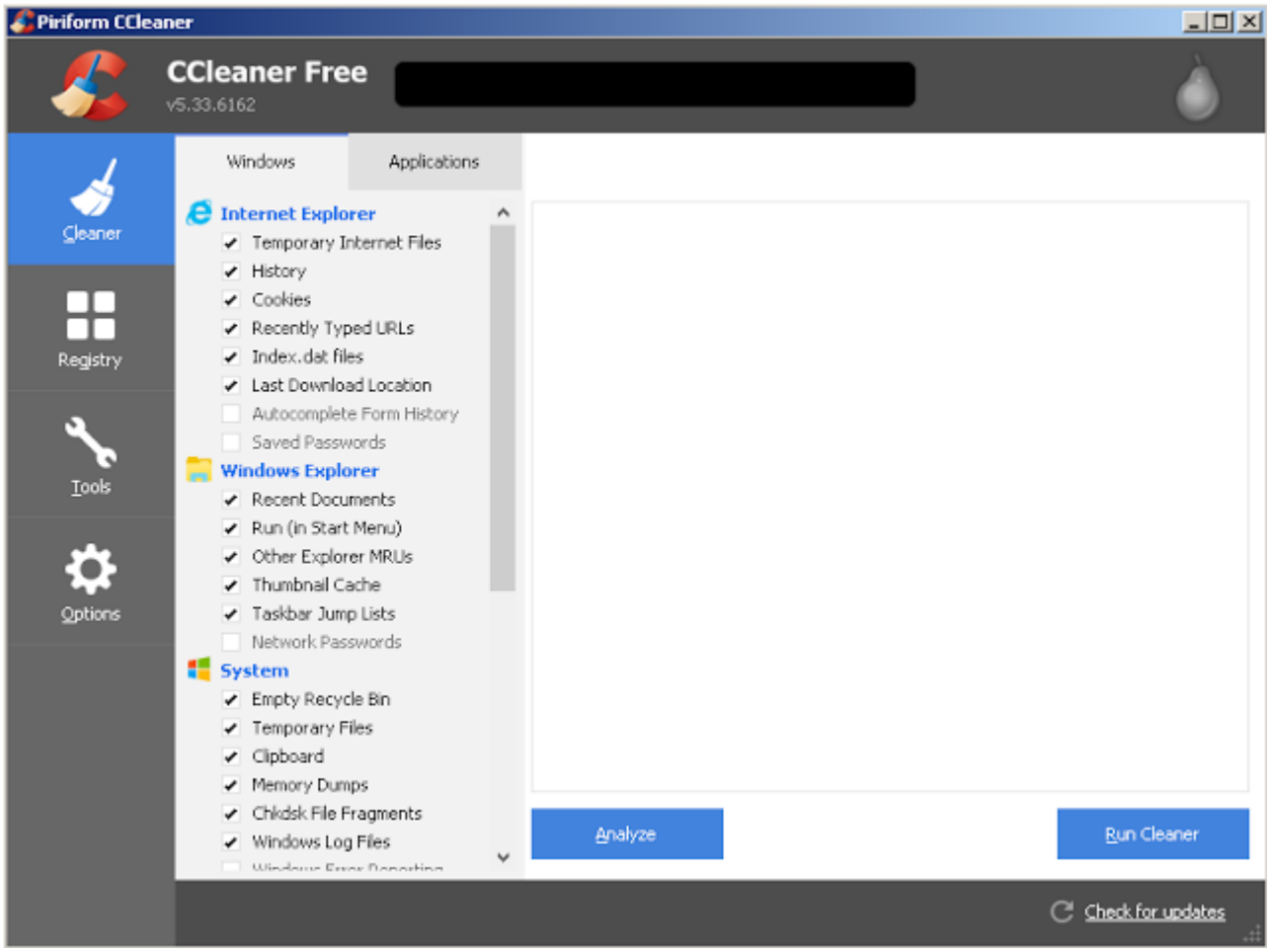

图 1：CCleaner 5.33 的屏幕截图

2017 年 9 月 13 日，思科 Talos 在对新的漏洞攻击检测技术进行客户 Beta 测试时，发现有一个特定的可执行文件触发了思科高级恶意软件保护 (AMP) 系统。经过仔细检查后，我们确定存在问题的可执行文件是 CCleaner v5.33 的安装程序，它由合法的 CCleaner 下载服务器传送到终端。Talos 开始进行初步分析，希望能确定导致 AMP 系统标记 CCleaner 的原因。我们发现，尽管下载的可执行安装文件使用颁发给 Piriform 的有效数字签名进行签名，但 CCleaner 并非该下载中包含的唯一应用。在安装 CCleaner 5.33 的过程中，安装文件中包含的 32 位 CCleaner 二进制文件还包含具有域生成算法 (DGA) 以及硬编码命令和控制 (C2) 功能的恶意负载。我们确认，直到 2017 年 9 月 11 日，此恶意版本的 CCleaner 仍直接挂载于 CCleaner 的下载服务器上。

查阅 CCleaner 下载站点上的“版本历史记录”页面后，可以得知受影响的版本 (5.33) 发布于 2017 年 8 月 15 日。2017 年 9 月 12 日，版本 5.34 发布。因此，这两个日期之间分发的就是包含恶意负载的版本 (5.33)。此版本使用由 Symantec 颁发给 Piriform Ltd 的有效证书进行签名，有效期截至 2018 年 10 月 10 日。Piriform 是 CCleaner 软件应用的原创开发公司，最近被 Avast 收购。

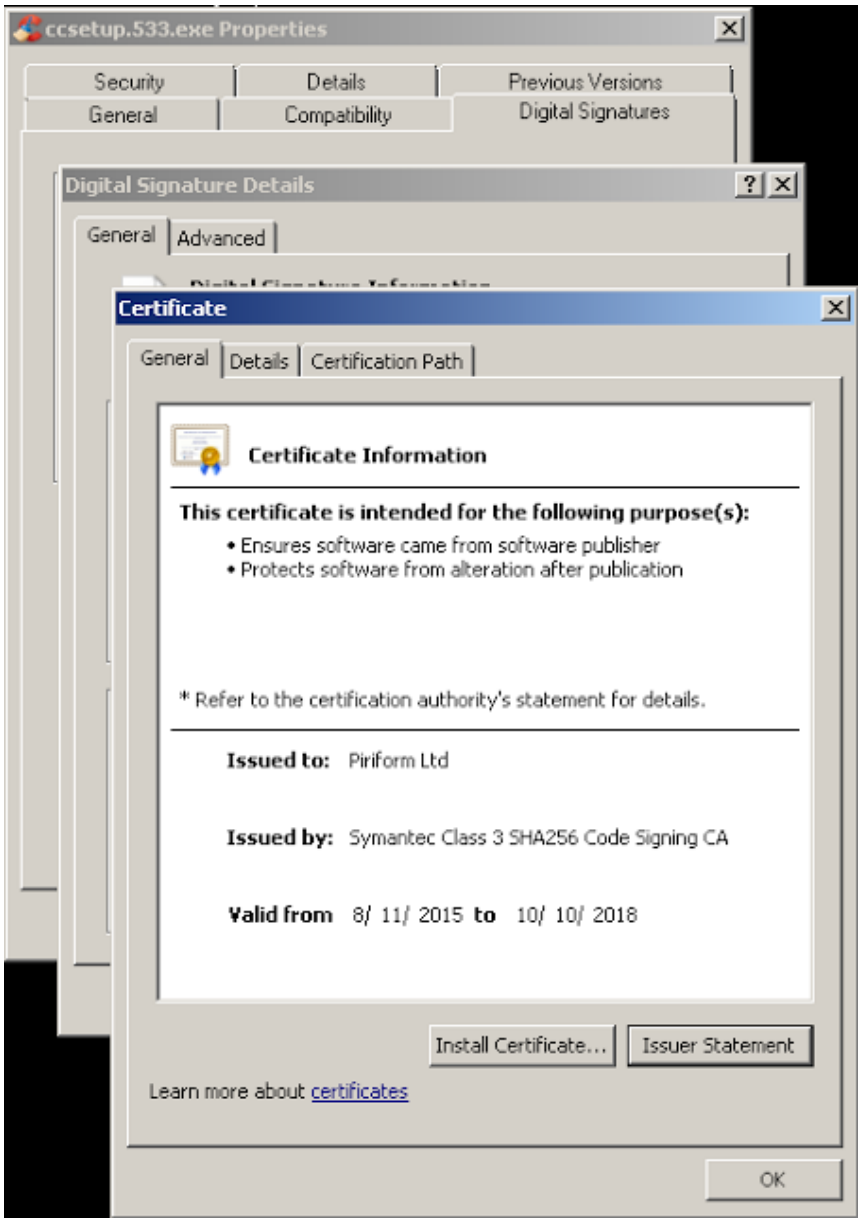

图 2：CCleaner 5.33 的数字签名

随后，我们发现了与此威胁关联的第二个样本。这第二个样本也使用有效数字证书进行签名，但是签名时间戳比初始样本的签名时间大约晚 15 分钟。

恶意 CCleaner 二进制文件中存在有效的数字签名可能表示存在更大的问题，进而导致开发或签名过程的环节被侵入。在理想情况下，该证书应该撤销，并且不再受到信任。在生成新证书时，必须注意确保攻击者在相关环境中没有可借以感染新证书的立足之地。只有事件响应过程可以提供关于此问题影响范围的详细信息，以及最佳的应对方法。

有趣的是，在 Talos 分析的 CCleaner 二进制文件中发现了以下编译构件：

S:\workspace\ccleaner\branches\v5.33\bin\CCleaner\Release\CCleaner.pdb

鉴于此编译构件的存在，以及使用颁发给软件开发商的有效证书对二进制文件进行数字签名这一事实，我们推测可能存在以下情况：外部攻击者侵入开发或内部版本环境的某个部分，并利用这种访问将恶意软件插入组织发布和托管的 CCleaner 版本中；有权访问组织内部的开发或内部版本环境的内部人员有意插入恶意代码，或者帐户（或类似凭证）被侵入，致使攻击者得以插入恶意代码。

还必须注意，虽然以前的 CCleaner 安装程序版本目前在下载服务器上仍然可用，但包含恶意负载的版本已经删除并且不再可用。

恶意软件的安装和运行

在合法的 CCleaner v5.33 安装程序所包含的 32 位 CCleaner v5.33 二进制文件内，“__scrt_get_dyn_tls_init_callback”遭到修改，用于调用位于 CC_InfectionBase(0x0040102C) 的代码。此举的目的是为了在继续正常的 CCleaner 运行之前，将 CCleaner 二进制文件内的代码执行流重定向至恶意代码。调用的代码负责解密包含两个阶段恶意负载的数据，其中一个负载是 PIC（位置无关代码）PE 加载程序，还有一个是可以有效用作恶意软件负载的 DLL 文件。恶意软件创作者试图通过确保将 IMAGE_DOS_HEADER 清零来降低恶意 DLL 的检测率，这表明此攻击者意欲逃避正常的检测手段。

之后，二进制文件使用 HeapCreate(HEAP_CREATE_ENABLE_EXECUTE,0,0) 创建一个可执行的堆，然后为此新堆分配空间，解密后的数据内容（其中包含恶意软件）正是被复制到此堆中。二进制文件在将数据复制到堆中时，会擦除源数据。然后，它会调用 PE 加载程序，让 PE 加载程序开始运行。一旦感染过程开始，二进制文件就会擦除先前包含 PE 加载程序和 DLL 文件的内存区域，释放先前分配的内存，销毁堆，并继续正常的 CCleaner 运行。

PE 加载程序利用与位置无关的编码方式在内存中查找 DLL 文件，然后将 DLL 映射到可执行内存中，调用 DLLEntryPoint 以便开始执行加载的 DLL，而 CCleaner 二进制文件则继续如常运行。一旦发生这种情况，恶意软件就会按照下一部分概述的过程开始全面执行。

CBkrdr.dll

DLL 文件 (CBkdr.dll) 遭到修改，攻击者试图借此避开检测并将 IMAGE_DOS_HEADER 清零。DLLEntryPoint 将创建一个执行线程，以便将控制返回到加载程序。此线程负责调用 CCBkdr_GetShellcodeFromC2AndCall。它还会设置一个面向返回的编程 (ROP) 链，用于释放与 DLL 关联的内存并退出线程。

CCBkrdr_GetShellcodeFromC2AndCall

此函数负责完成 Talos 在分析此恶意软件时观察到的大部分恶意操作。首先，它会记录受感染系统上的当前系统时间。然后，它会延迟 601 秒之后再继续运行，这可能是为了逃避那些被配置为在一段预定义时间内执行样本或决定是否在调试器中执行恶意软件的自动分析系统。为了实现此延迟功能，恶意软件调用了一个函数，该函数使用设置为 601 秒的 delay_in_seconds 超时尝试 ping 224.0.0.0。然后，它会通过检查确定当前的系统时间，看看 600 秒是否已过去。如果不满足这一条件，恶意软件将终止执行，而 CCleaner 二进制文件则继续正常运行。在恶意软件无法执行 IcmpCreateFile 的情况下，它会回退至使用 Sleep() 来实现相同的延迟功能。恶意软件还将当前系统时间与存储在以下注册表位置的值进行比较：

HKLM\SOFTWARE\Piriform\Agomo:TCID

如果存储在 TCID 值较晚，恶意软件也将终止执行。

```
00EC2543 2BC FF D6              call    esi ; time
00EC2545 2BC 8B F8              mov     edi, eax
00EC2547 2BC C7 04 24 59 02 00+mov     [esp+2B8h+delay], 601 ; delay
00EC254E 2BC E8 84 FF FF FF     call    DelayForSeconds
00EC2553 2BC 53                 push    ebx             ; Time
00EC2554 2C0 FF D6              call    esi ; time
00EC2556 2C0 2B C7              sub     eax, edi
00EC2558 2C0 59                 pop     ecx
00EC2559 2BC 3D 58 02 00 00     cmp     eax, 600
00EC255E 2BC 59                 pop     ecx
00EC255F 2B8 72 1B              jb      short BailOut
```

图 3：延迟例程

然后，恶意软件通过检查来确定系统上正在运行的用户所分配到的权限。如果运行恶意进程的当前用户不是管理员，恶意软件将终止执行。

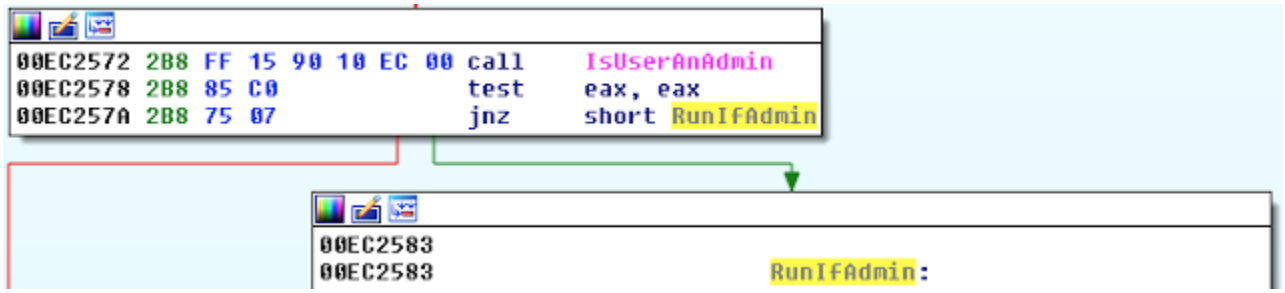

图 4：权限检查

如果执行恶意软件的用户具有受感染系统的管理权限，恶意软件就会为该进程启用 SeDebugPrivilege。然后，恶意软件会读取存储在以下注册表位置的“InstallID”值

HKLM\SOFTWARE\Piriform\Agomo:MUID

如果此值不存在，恶意软件会使用 ' “((rand()*rand() ^ GetTickCount())”创建该值。

一旦上述活动执行完毕，恶意软件就会开始分析系统并收集系统信息，这些信息稍后会被传输到 C2 服务器。系统信息存储在以下数据结构中：

```
00000000 CCBkdr_System_Information struc
00000000 InstallID       dd
00000004 NtMajorVersion  db
00000005 NtMinorVersion  db
00000006 IsWow64Process  db
00000007 unk_zero        db
00000008 ComputerName    db 64
00000048 ComputerNameDnsDomain db 64
00000088 IpAddresses     dd 6
000000A0 Records         CCBkdr_Record 254 ; Installed processes according to
000000A0                                   ;
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
000000A0                                   ; Running processes
```

图 5：CCBkdr_System_Information 数据结构

收集完系统信息后，恶意软件会对其进行加密，然后使用修改后的 Base64 进行编码。随后，恶意软件将按下一部分所述建立命令和控制 (C2) 信道。

命令和控制 (C2)

在分析此恶意软件时，Talos 发现其恶意代码中似乎存在一个与 C2 功能相关的软件错误。Talos 所分析的样本会读取一个使用 DGA 计算出来的 IP 地址，它位于以下注册表位置但目前全然无所作为：

HKLM\SOFTWARE\Piriform\Agomo:NID

目前还不清楚此 IP 地址的用途是什么，因为恶意软件在随后的运行过程中似乎并没有使用它。在任何情况下，一旦前面提到的系统信息收集完毕并准备好传输到 C2 服务器，恶意软件就会尝试使用 HTTPS POST 请求将其传输到 216[.]126[.]225[.]148。HTTPS 通信使用硬编码的 HTTP 主机报头，报头被设置为 speccy[.]piriform[.]com，这是 Piriform 为监控硬件而创建的合法平台。这一点加大了动态分析的难度，因为这个域看起来是合法的，甚至有可能是预期的传输目的（根据受害者的基础设施而定）。由于服务器当前返回的自签名 SSL 证书是颁发给主机报头字段中定义的子域的，因此该请求在使用 HTTPS 时还忽略了所有安全错误。如果没有从 C2 服务器收到任何响应，恶意软件就会故障恢复为使用本文“域生成算法”部分所述的域生成算法 (DGA)。

一旦恶意软件确定可用的 C2 服务器，就会发送包含系统配置文件信息的编码数据，并将 C2 IP 地址存储到以下注册表位置：

HKLM\SOFTWARE\Piriform\Agomo:NID

然后，恶意软件将当前系统时间加上两天后得出的值存储到以下注册表位置：

HKLM\SOFTWARE\Piriform\Agomo:TCID

然后，对从 C2 服务器收到的数据进行验证，确认收到的数据符合 CCBkdr_ShellCode_Payload 结构的正确格式。示例如下所示：

```
00000000 CCBkdr_ShellCode_Payload struc
00000000 Size                dd
00000004 EncryptedInstallID dd
00000008 EncodedEncryptedDataBuffer db *
```

图 6：CCBkdr_ShellCode_Payload 数据结构

接下来，恶意软件确认 EncryptedInstallID 的值与先前传输到 C2 服务器的值匹配，然后为最终的 shellcode 负载分配内存。在此之后，使用修改后的 Base64 对负载进行解码并将结果存储到新分配的内存区域中，再对负载进行解密，并以 LoadLibraryA 和 GetProcAddress 的地址为参数调用负载。执行完负载后，释放内存，并将下面的注册表值设置为当前系统时间加七天：

HKLM\SOFTWARE\Piriform\Agomo:TCID

接收缓冲区则被清零后释放。CCBkdr_ShellCode_Payload 结构也被释放，恶意软件继续进行正常的 CCleaner 运行。此恶意软件的运行概况如下图所示：

图 7：恶意软件运行流程图

域生成算法

在发生上一部分所述的情况，即主 C2 服务器没有返回对 HTTP POST 请求的响应时，恶意软件将故障恢复为使用 DGA 算法。此恶意软件使用的算法基于时间，可以使用年和月的值进行计算。DGA 域的列表如下图所示：

Year-Month	DGA Domain
2017-02	ab6d54340c1a[.]com
2017-03	aba9a949bc1d[.]com
2017-04	ab2da3d400c20[.]com
2017-05	ab3520430c23[.]com
2017-06	ab1c403220c27[.]com
2017-07	ab1abad1d0c2a[.]com
2017-08	ab8cee60c2d[.]com
2017-09	ab1145b758c30[.]com
2017-10	ab890e964c34[.]com
2017-11	ab3d685a0c37[.]com
2017-12	ab70a139cc3a[.]com

图 8：生成 12 个月的 DGA 域

恶意软件将对 DGA 算法生成的每个域启动 DNS 查找。如果 DNS 查找未返回 IP 地址，此过程将继续。恶意软件将对活跃的 DGA 域执行 DNS 查询，并期望从管理该 DGA 域的命名空间的域名服务器返回两个 IP 地址。然后，恶意软件将对返回的 IP 地址值执行一系列位运算来计算辅助 C2 服务器，并通过组合这些值确定要用于后续 C2 运行的 C2 服务器实际回退地址。此过程如下图所示：

图 9：C2 流程图

思科 Talos 在分析过程中发现这些 DGA 域尚未注册，因此我们注册了这些域并将其作为 Sinkhole 域，以防攻击者将其用于恶意用途。

潜在影响

鉴于可能受到影响的系统数量非常多，此攻击造成的影响可能十分严重。根据 CCleaner 发布的数据，截至 2016 年 11 月，其全球下载量超过 20 亿，从报道的用户增长率来看，每周新增用户达到 500 万。

图 10：CCleaner 消费者的人口统计数据

即使这些系统中只有一小部分受到感染，攻击者也可以将这一小部分系统用于任意数量的恶意用途。受到影响的系统需要恢复到 2017 年 8 月 15 日之前的状态或重新安装。而且，用户还应该更新到最新的 CCleaner 可用版本以避免感染。在撰写本文时，最新的版本为 5.34 版。值得注意的是，根据 CCleaner 下载页面来看，CCleaner 的免费版本不提供自动更新，所以使用免费版本的受影响用户需要手动进行更新。

通过分析与此攻击相关的基于 DNS 的遥感勘测数据，Talos 确定有大量系统发出 DNS 请求，试图解析与上述 DGA 域关联的域。由于这些域从未注册过，所以我们可以得出这些系统受到此恶意软件影响的合理结论。虽然与此 DGA 关联的大多数域几乎没有（甚至完全没有）与其关联的请求流量，但是与 8 月和 9 月这两个月（此时间可以与这种威胁的活跃时间关联起来）相关的域却显示出更高的活跃度。

分析思科 Umbrella 观察到的 2017 年 7 月（CCleaner 5.33 发布之前）与 DNS 相关的活跃度后，我们发现用于解析与此恶意软件关联的 DGA 域 IP 地址的 DNS 请求非常少：

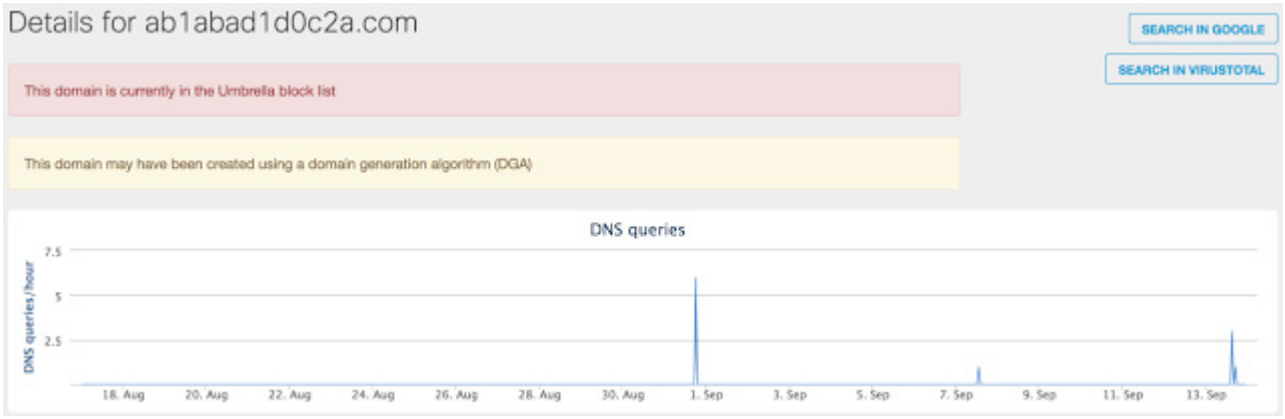

图 11：2017 年 7 月 DGA 域的 DNS 活跃度

正如本文前文所述，包含此恶意软件的 CCleaner 版本发布于 2017 年 8 月 15 日。下图显示，与 2017 年 8 月所用 DGA 域关联的 DNS 活跃度显著提高：

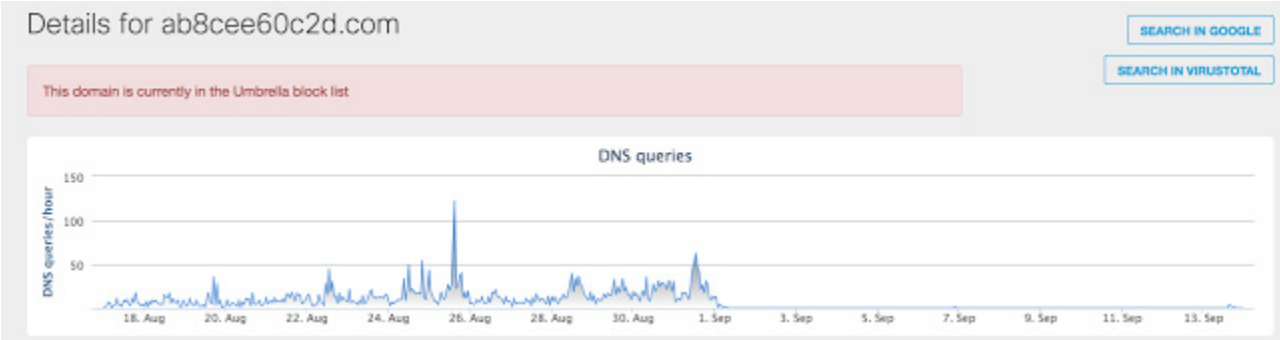

图 12：2017 年 8 月 DGA 域的 DNS 活跃度

同样，与 2017 年 9 月关联的 DGA 域在试图解析与其关联的 IP 地址方面也反映出极高活跃度，如下图所示：

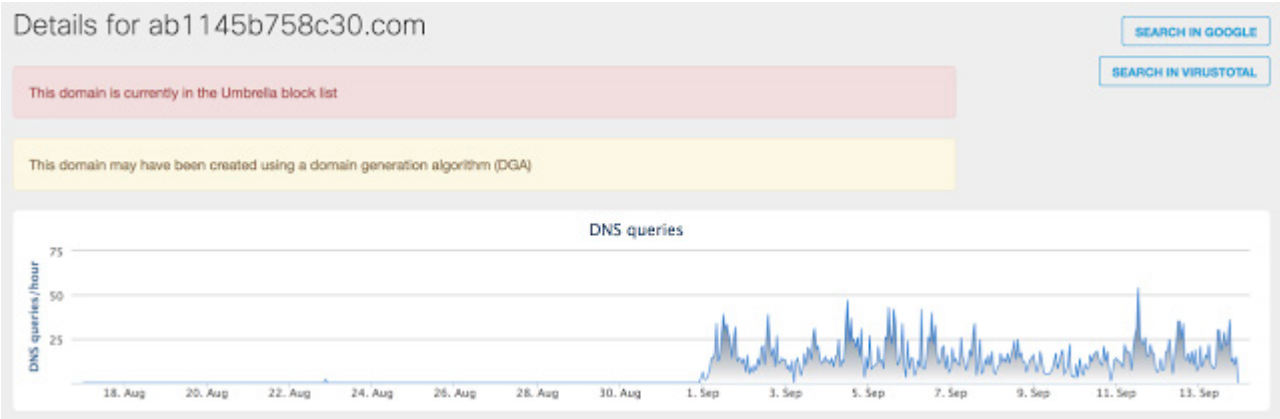

图 13：2017 年 9 月 DGA 域的 DNS 活跃度

请注意，2017 年 9 月 1 日，DNS 活跃度似乎从此前在 8 月使用的 DGA 域转移到 9 月使用的一个域，这种情况与本文“域生成算法”部分所述的基于时间的 DGA 算法相符。与 Avast 联系后，我们注意到他们关闭了服务器，因此服务器对已经感染的系统不再可用。结果，针对恶意软件所用故障恢复 DGA 域的请求量显著增加。

图 14：服务器关闭后的流量激增

还有一点值得注意的是，在本文撰写时，此威胁的防病毒检测率仍然非常低（本文撰写时的检测率为 1/64）。

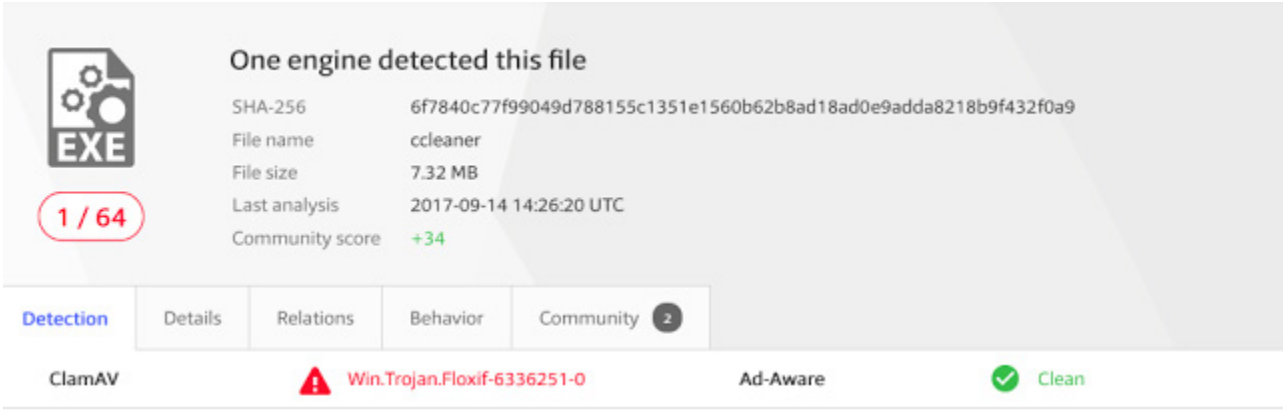

图 14：CCleaner 二进制文件的 VirusTotal 检测率

作为思科应对此威胁的一项对策，思科 Talos 公布了全面的防护信息，列出可为客户提供保护的各种产品。有关此防护的详细信息，请参阅本文“防护”部分。

结论

这是一个反映攻击者不择手段试图向全球范围内的组织和个人分发恶意软件的典型例子。利用软件供应商与其软件用户之间的信任关系，攻击者就可以因为用户对用于分发更新的文件和 Web 服务器的固有信任而得到好处。在许多组织中，较之被视为不可信来源的数据所适用的审查级别，来自常用软件供应商的数据极少会接受相同级别的审查。攻击者的行为表明，他们意欲利用这种信任，不被察觉地分发恶意软件。思科 Talos 会继续监控威胁形势的各个方面，确保快速发现攻击者用于攻击全球组织和个人的各种新手段和翻新手法。

防护

已发布用于检测此威胁的以下 ClamAV 签名：6336251 和 6336252。

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	✔
CloudLock	不适用
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

CWS 或 WSA Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella，我们的安全互联网网关 (SIG)，可阻止用户连接恶意域、IP 和 URL（无论用户是否位于公司网络上）。

感染指标 (IOC)

文件散列值

6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9
1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff
36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0bfdb2e9

DGA 域

ab6d54340c1a[.]com
aba9a949bc1d[.]com
ab2da3d400c20[.]com
ab3520430c23[.]com
ab1c403220c27[.]com
ab1abad1d0c2a[.]com
ab8cee60c2d[.]com
ab1145b758c30[.]com
ab890e964c34[.]com
ab3d685a0c37[.]com
ab70a139cc3a[.]com

IP 地址

216[.]126[.]225[.]148

发布者：EDMUND BRUMAGHIN；发布时间：3:51