发现了 64 位版本的 HAVEX

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	64-bit Version of HAVEX Spotted		
原文作者	Jay Yaneza	**原文发布日期**	2014 年 12 月 29 日
作者简介	Jay Yaneza 是趋势科技公司的高级技术经理、应用程序开发人员、系统/网络/数据库管理员，尤其专注于各种趋势科技产品的部署、配置和故障排除。https://www.linkedin.com/pub/jay-yaneza/7/33a/547		
原文发布单位	趋势科技公司		
原文出处	http://blog.trendmicro.com/trendlabs-security-intelligence/64-bit-version-of-havex-spotted/#more-64874		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版		

	权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

发现了 64 位版本的 HAVEX

Jay Yaneza

2014 年 12 月 29 日

远程访问工具 HAVEX 被发现在 ICS(工业控制系统)攻击活动中起着重要作用 ,此后，它成为安全业界关注的焦点。在检测 HAVEX(不同厂商分别将其命名为 Dragonfly、Energetic Bear 和 rouching Yeti ）时，我们发现了一些有趣的事情。

此前，大多数关键系统最有可能是 Windows XP，所以研究人员认为 Dragonfly（蜻蜓）行动只适用于 32 位版本的系统。此事件之后，Windows XP 系统逐渐退出舞台。反之，我们发现了 Windows 7 系统的两个有趣感染。

第一款 64 位 HAVEX

通过分析（参见图 1），我们发现了一个称为 TMPpovider023.dll 的文件，将其命名为 BKDR64_HAVEX.A ，它能够在文件系统中创建若干文件。应当指出的是，TMPprovider0<2-digit version number>.dll 是 HAVEX 的已知信标和组件，能够与 C&C 服务器交互，以便执行下载行为或接收相关的执行命令。

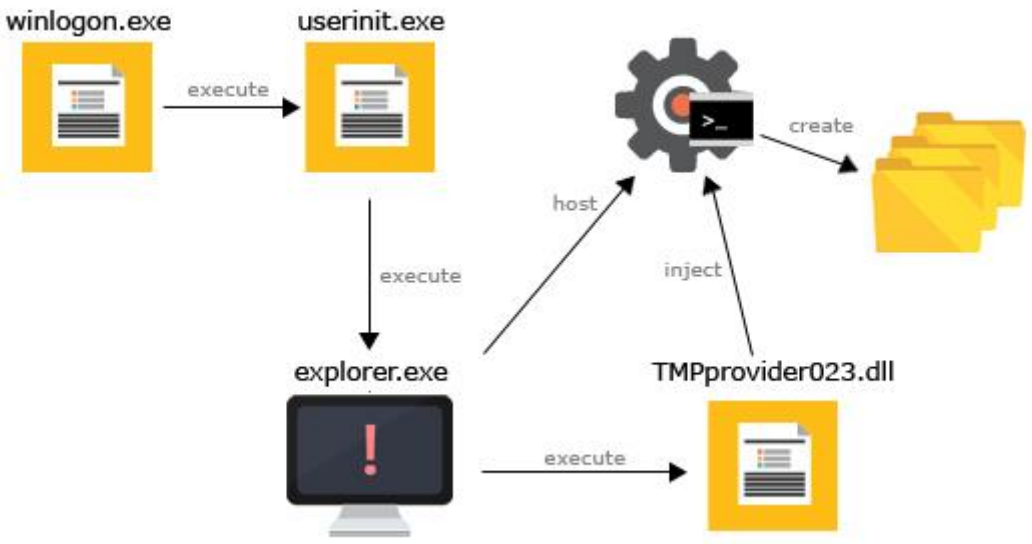

图 1：文件安装链

我们发现了 BKDR_HAVEX 的 3 个有趣的信标。

- 文件 TMPProvider023.dll，其中的数字表示该 HAVEX RAT 的版本号（v023 ）。

- 名为 34CD.tmp.dll 的投放文件，我们将其命名为 BKDR_HAVEX.SM。此时，该文件被安装的趋势科技产品重复检测和隔离。后来发现这是 HAVEX 的版本 29 或 v029。
- 从主机发起或到主机的 C&C 通信。

图 2：投放的文件被命名为 BKDR_HAVEX.SM

深入分析第一款 64 位 HAVEX

为了更好地理解这两个文件（TMPProvider023.dll 和 34CD.tmp.dll）如何运作，我们需要确定与感染链有关的其他文件。我们发现了另外两个投放文件。

第一个文件是 734.tmp.dll，我们将其命名为 BKDR_HAVEX.C，它负责创建注册表值和项，由“主”HAVEX 文件查询：

HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\Options

b = <data>

与较新的 HAVEX 版本（> =038 版本）相比，该版本需要另一个加载器，如下所示。

图 3：投放文件 734.tmp.dll

第二个文件是 4F2.tmp.dll，我们将其命名为 BKDR_HAVEX.C，该文件更加有趣。技术上说，两个版本的 HAVEX RAT 驻留在同一台机器中，现在的问题是：v029 能否“向后兼容”v023。

4F2.tmp.dll 清除下列的文件系统：

文件	注册表
%TEMP%*.yls%TEMP%*.xmd%TEMP%\qln.dbx	HKCU\Software\Mirosoft\Internet Explorer\InternetRegistry\Options

```
sub_10001054((int)&v3, L"TEMP");
v5 = 0;
v0 = sub_100092A0((int)&v3, (int)&v2);
LOBYTE(v5) = 1;
sub_1000119C((int)&v4, v0, L"\\qln.dbx");
...
sub_10001054((int)&v4, L"TEMP");
v13 = 0;
sub_100092A0((int)&v4, (int)&v7);
LOBYTE(v13) = 2;
sub_10002678((int)&v4, 1, 0);
sub_10001054((int)&v9, L".xmd");
...
sub_10001054((int)&TEMP, L"TEMP");
v26 = 1;
sub_100092A0((int)&TEMP, (int)&v17);
LOBYTE(v26) = 3;
sub_10002678((int)&TEMP, 1, 0);
v2 = sub_1000119C((int)&v7, (int)&v17, L"\\*");
LOBYTE(v26) = 4;
sub_1000119C((int)&v18, v2, L".yls");
...
```

```
sub_10001054((int)&v7, &word_10034358);
v13 = 0;
sub_10001054((int)&v6, L"Software\\Microsoft\\Internet Explorer\\InternetRegistry\\Options");
LOBYTE(v13) = 1;
sub_100094D0((int)&v11, HKEY_CURRENT_USER, (int)&v6, 0xF003Fu, (int)&v7);
sub_10002678((int)&v6, 1, 0);
LOBYTE(v13) = 4;
sub_10002678((int)&v7, 1, 0);
sub_10001054((int)&v8, &word_10034358);
LOBYTE(v13) = 5;
v0 = lpValueName;
if ( v10 < 8 )
  v0 = (const WCHAR *)&lpValueName;
v1 = RegDeleteValueW(hKey, v0);
```

图 4：表示删除文件（上）和注册表项（下）的伪代码

我们发现了 v023（以前是一个 64 位的文件）如何升级为 32 位的 v029 HAVEX RAT。这使我们想到了一个感染中相互关联的 4 个文件，如下所示。

文件名	SHA1	编译日期	架构
%TEMP%\TMPprovider023.dll	997C0EDC9E8E67FA0C0BC88D6FDEA512DD8F7277	2012-10-03	AMD64
%TEMP%\34CD.tmp.dll	CF5755D167077C1F8DEEDDEAFEBEA0982BEED718	2013-04-30	I386
%TEMP%\734.tmp.dll	BFDDB455643675B1943D4E33805D6FD6884D592F	2013-08-16	I386
%TEMP%\4F2.tmp.dll	8B634C47087CF3F268AB7EBFB6F7FBCFE77D1007	2013-06-27	I386

TMPprovider023.dll（v023）的编译时间早于其他 3 个文件，这表明在该感染中，64 位文件早于 32 位文件进行编译。事实上，32 位模块的独立执行导致了文件 TMPprovider029.dll 的生成，这绝对是 HAVEX RAT 的 v029 版本。

网络分析

端点上出现了两个不同的 HTTP POST 请求。

对于 32 位的“主”v029 HAVEX 文件 34cd.tmp.dll，C&C 查询字符串的格式类似于：

- hxxp://<C&C location>/path/to/php-script/php-php?id=<victim_ID>&v1=<HAVEX_version>&v2=<OS_version>&q=<command>

另一方面，64 位“主”v023 HAVEX 文件 TMPprovider023.dll 的查询字符串则不同：

- hxxp://<C&C location>/path/to/php-script/php-script.php?id=[20 numeric characters][10 numeric characters][6 alphanumeric characters]-[2 numeric characters]-[3 digit number]-[9 numeric characters]

字符串中总是出现最后两个组合（[3 位数]-[9 个数字字符]）。该 3 位数字组合最有可能是恶意软件的版本号，而其余 9 位数可能代表行动 ID。

该 ID 是随机生成的，并且写入以下注册表项中：

- HKCU\Software\Microsoft\Internet Explorer\InternetRegistry\fertger={malware ID}

在这个特殊的感染中，v023 HAVEX 文件使用的 C&C 服务器与 v029 HAVEX 文件的相同。这就说明，HAVEX 各版本（至少 v023 和 029 之间）的基础设施可能共享。

目前，我们已经发现了至少 4 个 IP 地址与 C&C 服务器进行通信，其中两个都会升级 HAVEX RAT 的 C＆C 模块的版本。

另一个感染：HAVEX 二进制文件试图伪造数字签名

在第二个感染中，文件 NSDS.dll 被投放在％APPDATA％中，引发了 BKDR_HAVEX.SM 感染，而且 BKDR_HAVEX.SM 具有数字签名。在过去几年中，恶意软件签名有所增加，恶意软件编写者通常寻求允许文件签名的方法，使恶意文件看起来合法。

这个特殊组件的 4 个文件模仿 IBM 签名的文件，不过，很明显可以看出数字证书是自签名的。

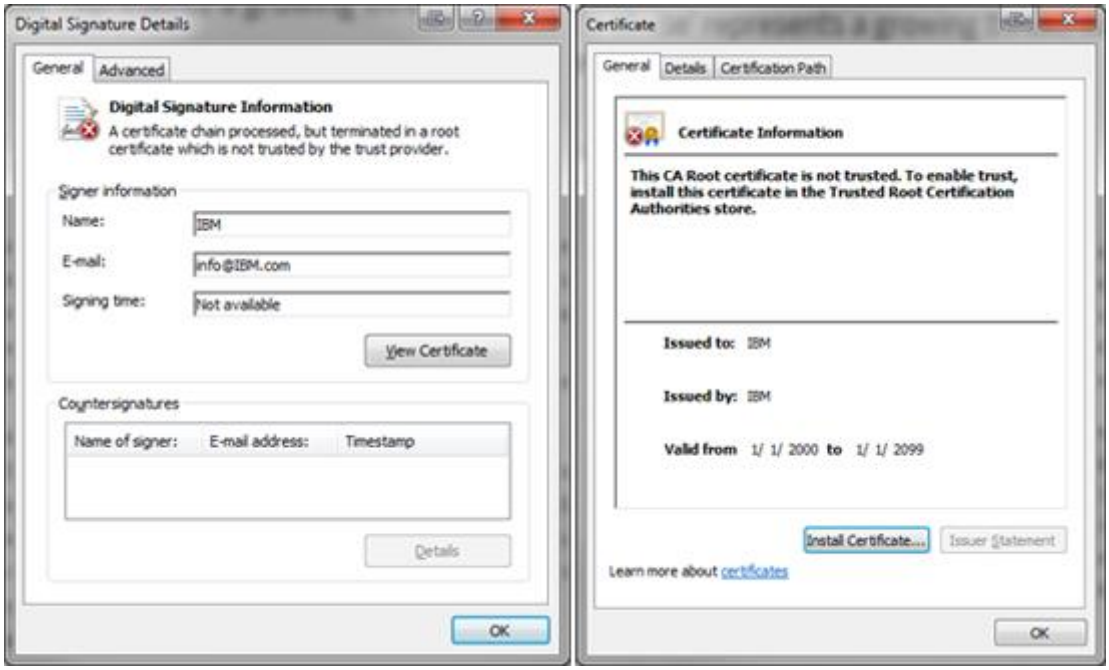

图 5：伪造的由 IBM "签名" 的数字证书

正确签名的文件应该附上受信的证书颁发机构，以验证颁发的数字证书，但这些文件并没有。虽然我们尚无法确定哪个软件包包含这些文件，但是我们发现了另外 3 个具有类似数字签名的文件。所有这些文件都被命名为 BKDR_HAVEX.SM。

文件哈希	文件大小	编译日期
*bb59cc5e0040ede227332e7da1942264cd75ec4c	133,152 字节	2013-03-21
80caa936528ceefcb614ae175bda2a27609a5dd3	133,152 字节	2013-04-08
49b109d94602195fe5705a9b5f7b5ddd59477015	133,152 字节	2013-04-23
361c0a4f8213693e974b6ae55bf0ad16c74adf61	133,152 字节	2013-06-11

*最近感染中发现的文件

恶意软件的重用

虽然 HAVEX RAT 已经被多次使用了，曾用于攻击 ICS/ SCADA 甚至制药公司，但是没有什么能够阻止它被不断地重复使用。ICS 运营商必须注意，HAVEX 二进制文件的结构类似于常见的 Windows 恶意软件。随着 64 位 Windows 7 系统的感染，其相似度也更高了。因此，验证安装在端点上的软件并经常监控 HTTP 流量是很重要的。

趋势科技阻断并检测了以上所有的信标。欲了解 ICS 环境的更多威胁信息，请参考趋势科技的两篇报告：《究竟是谁在攻击你的 ICS 设备？》和《没有喊狼来了的 SCADA》。

相关文件的哈希值：

- 997C0EDC9E8E67FA0C0BC88D6FDEA512DD8F7277
- CF5755D167077C1F8DEEDDEAFEBEA0982BEED718
- BFDDB455643675B1943D4E33805D6FD6884D592F
- 8B634C47087CF3F268AB7EBFB6F7FBCFE77D1007
- bb59cc5e0040ede227332e7da1942264cd75ec4c