АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Сертификаты D-Link и Changing Information Technologies использовались для подписи вредоносного ПО

10 июля 2018 года

ESET обнаружила новую киберкампанию, в которой используются украденные сертификаты для подписи кода. Цифровые сертификаты D-Link Corporation и Changing Information Technologies украдены высококвалифицированной кибершпионской группой, ориентированной на Восточную Азию.

Мы зафиксировали вредоносную кампанию, когда наши системы отметили несколько файлов как подозрительные. Интересно, что отмеченные файлы имели цифровую подпись с действительным сертификатом компании D-Link Corporation. Тот же сертификат использовался для подписи легитимного ПО D-Link; скорее всего, этот сертификат был украден.

Подтвердив вредоносность файла, мы сообщили о проблеме в D-Link, которая начала собственное расследование. В результате 3 июля компания отозвала скомпрометированный цифровой сертификат.

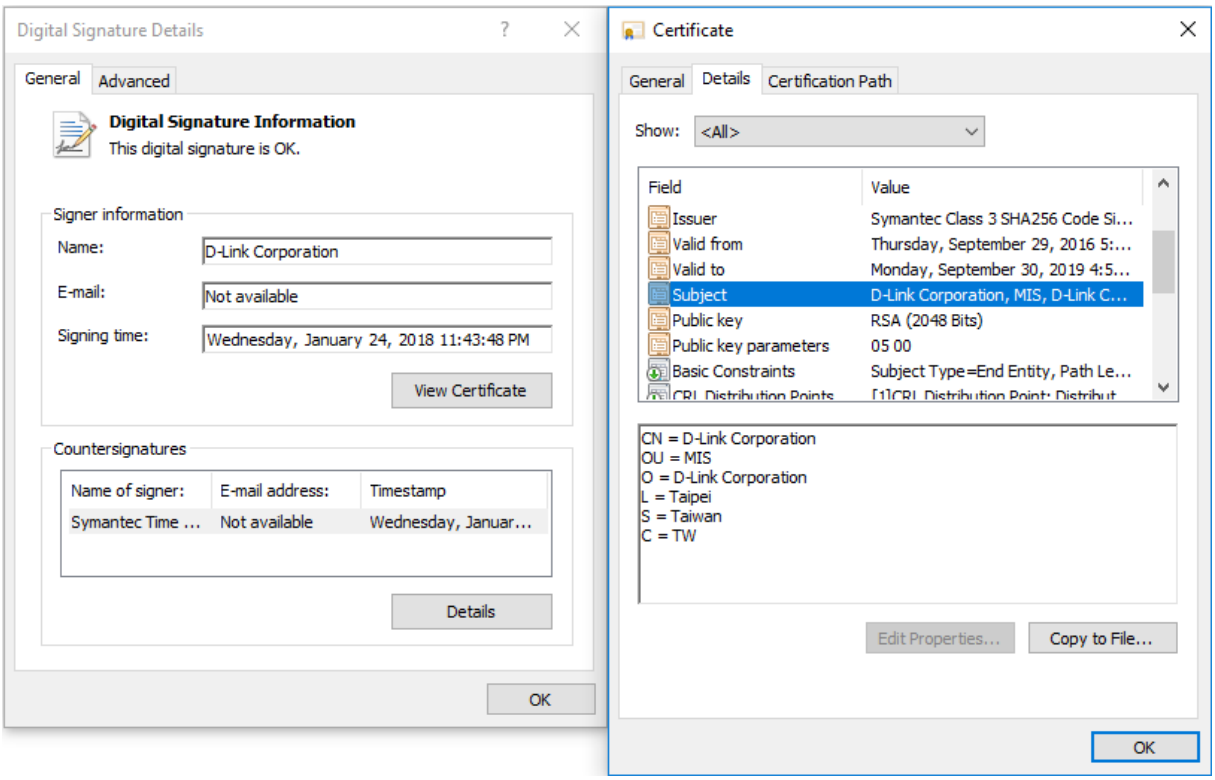

Рисунок 1. Цифровой сертификат D-Link используется для подписи вредоносного ПО

Вредоносное ПО

В ходе исследования мы нашли два семейства вредоносных программ, использующих украденные сертификаты – бэкдор для удаленного управления целевым устройством и связанный с ним компонент для кражи паролей. Недавно JPCERT опубликовал детальный анализ бэкдора Plead; по мнению Trend Micro, он используется кибершпионской группой BlackTech.

Помимо образцов Plead с цифровой подписью D-Link, мы идентифицировали образцы, подписанные сертификатом тайваньской ИБ-компании Changing Information Technology Inc.

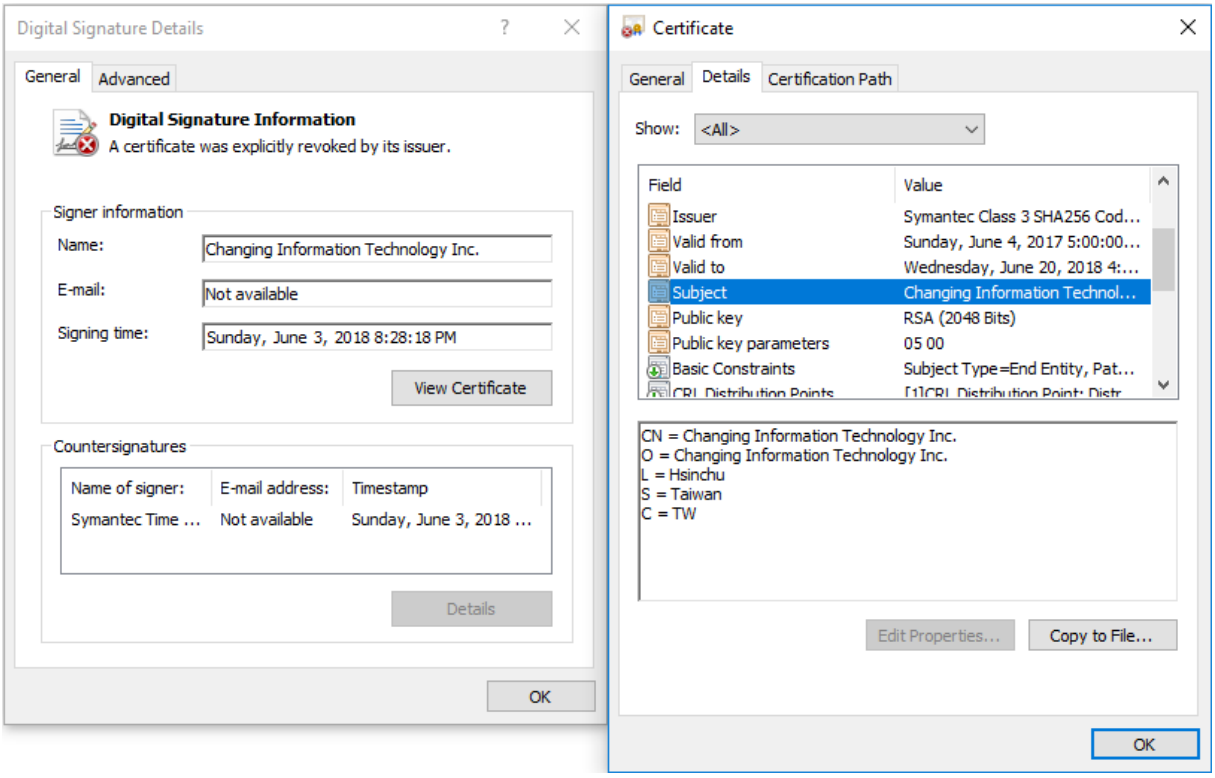

Рисунок 2. Цифровой сертификат Changing Information Technology Inc. используется для подписи вредоносного ПО

Сертификат Changing Information Technology Inc. отозван 4 июля 2017 года, однако группа BlackTech все еще использует его для подписи своих вредоносных инструментов.

Возможность компрометации нескольких тайваньских технологических компаний и повторное использование их сертификатов в новых атаках демонстрирует высокую квалификацию кибергруппы и ее интерес к данному региону.

Подписанные образцы Plead сильно обфусцированы с помощью мусорного кода, но назначение вредоносного ПО едино во всех образцах – загрузить с удаленного сервера или открыть с локального диска небольшой зашифрованный двоичный блоб. Он содержит зашифрованный шелл-код, загружающий финальный модуль бэкдора Plead.

```
.text:00401C8B     call    dummy_func_1
.text:00401C90     push    40h ; '@'           ; _DWORD
.text:00401C92     push    1000h               ; _DWORD
.text:00401C97     push    500000h             ; _DWORD
.text:00401C9C     push    edi                 ; _DWORD
.text:00401C9D     call    kernel32_GetCurrentProcess
.text:00401CA3     push    eax                 ; _DWORD
.text:00401CA4     call    kernel32_VirtualAllocEx
.text:00401CAA     mov     edi, eax
.text:00401CAC     test    edi, edi
.text:00401CAE     jz      loc_401D9B
.text:00401CB4     call    dummy_func_1
.text:00401CB9     push    esi                 ; Format
.text:00401CBA     call    ebx ; printf
.text:00401CBC     pop     ecx
.text:00401CBD     call    dummy_func_1
.text:00401CC2     call    dummy_func_3
.text:00401CC7     call    dummy_func_1
.text:00401CCC     push    esi                 ; Format
.text:00401CCD     mov     [ebp+lpString2], edi
.text:00401CD0     call    ebx ; printf
.text:00401CD2     call    dummy_func_1
.text:00401CD7     call    dummy_func_1
.text:00401CDC     call    dummy_func_2
.text:00401CE1     call    dummy_func_1
.text:00401CE6     call    dummy_func_1
.text:00401CEB     call    dummy_func_2
.text:00401CF0     call    dummy_func_3
.text:00401CF5     push    [ebp+var_4]         ; Size
.text:00401CF8     push    [ebp+Src]           ; Src
.text:00401CFB     push    edi                 ; Dst
.text:00401CFC     call    memcpy
```

Рисунок 3. Обфусцированный код бэкдора Plead

Инструмент для кражи паролей используется для сбора сохраненных паролей в следующих приложениях:

— Google Chrome
— Microsoft Internet Explorer
— Microsoft Outlook
— Mozilla Firefox

Зачем красть цифровые сертификаты?

Использование украденных цифровых сертификатов – один из способов маскировки. Сертификаты помогают вредоносным программам выглядеть как легитимные и, значит, обходить защиту, не вызывая подозрений.

Вероятно, самое известное вредоносное ПО, использовавшее несколько «чужих» сертификатов – Stuxnet, обнаруженное в 2010 году и известное как первое кибероружие, ориентированное на критическую инфраструктуру. Stuxnet использовал цифровые сертификаты, украденные у RealTek и JMicron, известных технологических компаний из Тайваня.

Тем не менее, эта тактика не является исключительной для таких масштабных инцидентов, как Stuxnet, о чем свидетельствует и последнее открытие.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации:

Детектирование продуктами ESET:

```
Win32/PSW.Agent.OES trojan
Win32/Plead.L trojan
Win32/Plead.S trojan
Win32/Plead.T trojan
Win32/Plead.U trojan
Win32/Plead.V trojan
Win32/Plead.X trojan
Win32/Plead.Y trojan
Win32/Plead.Z trojan
```

Неподписанные образцы (SHA-1):

```
80AE7B26AC04C93AD693A2D816E8742B906CC0E3
62A693F5E4F92CCB5A2821239EFBE5BD792A46CD
B01D8501F1EEAF423AA1C14FCC816FAB81AC8ED8
11A5D1A965A3E1391E840B11705FFC02759618F8
239786038B9619F9C22401B110CF0AF433E0CEAD
```

Подписанные образцы (SHA-1):

```
1DB4650A89BC7C810953160C6E41A36547E8CF0B
CA160884AE90CFE6BEC5722FAC5B908BF77D9EEF
9C4F8358462FAFD83DF51459DBE4CD8E5E7F2039
13D064741B801E421E3B53BC5DABFA7031C98DD9
```

C&C-серверы:

```
amazon.panasocin[.]com
office.panasocin[.]com
okinawas.ssl443[.]org
```

Серийные номера сертификатов для подписи кода:

```
D-Link Corporation:
13:03:03:E4:57:0c:27:29:09:E2:65:Dd:B8:59:De:Ef
Changing Information Technology Inc.:
73:65:ED:E7:F8:FB:B1:47:67:02:D2:93:08:39:6F:51
1E:50:CC:3D:D3:9B:4A:CC:5E:83:98:CC:D0:DD:53:EA
```