

Share

ESET researchers have discovered a new malware campaign misusing stolen digital certificates.

welivesecurity by eset



We spotted this malware campaign when our systems marked several files as suspicious.



Interestingly, the flagged files were digitally signed using a valid D-Link Corporation code-signing certificate. The exact same certificate had been used to sign non-malicious D-Link software; therefore, the certificate was likely stolen.



Having confirmed the file's malicious nature, we notified D-Link, who launched their own investigation into the matter. As a result, the compromised digital certificate was [revoked by D-Link](#) on July 3, 2018.

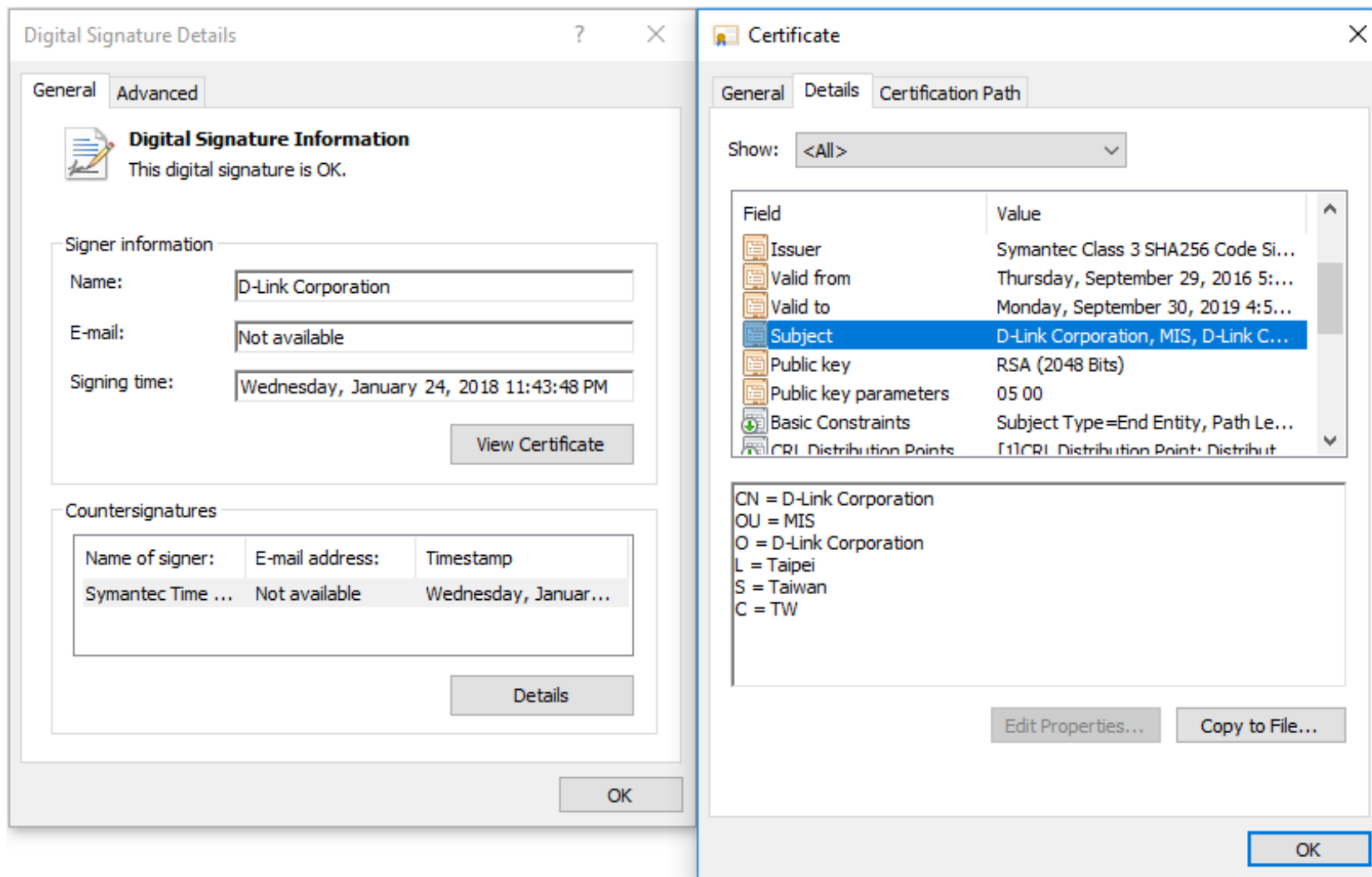


Figure 1. The D-Link Corporation code signing certificate used to sign malware

The malware

Our analysis identified two different malware families that were misusing the stolen certificate

– the Plead malware, a remotely controlled backdoor, and a related password stealer component. Recently, the JPCERT published a thorough [analysis](#) of the Plead backdoor, which, according to Trend Micro, is used by the cyberespionage group [BlackTech](#).

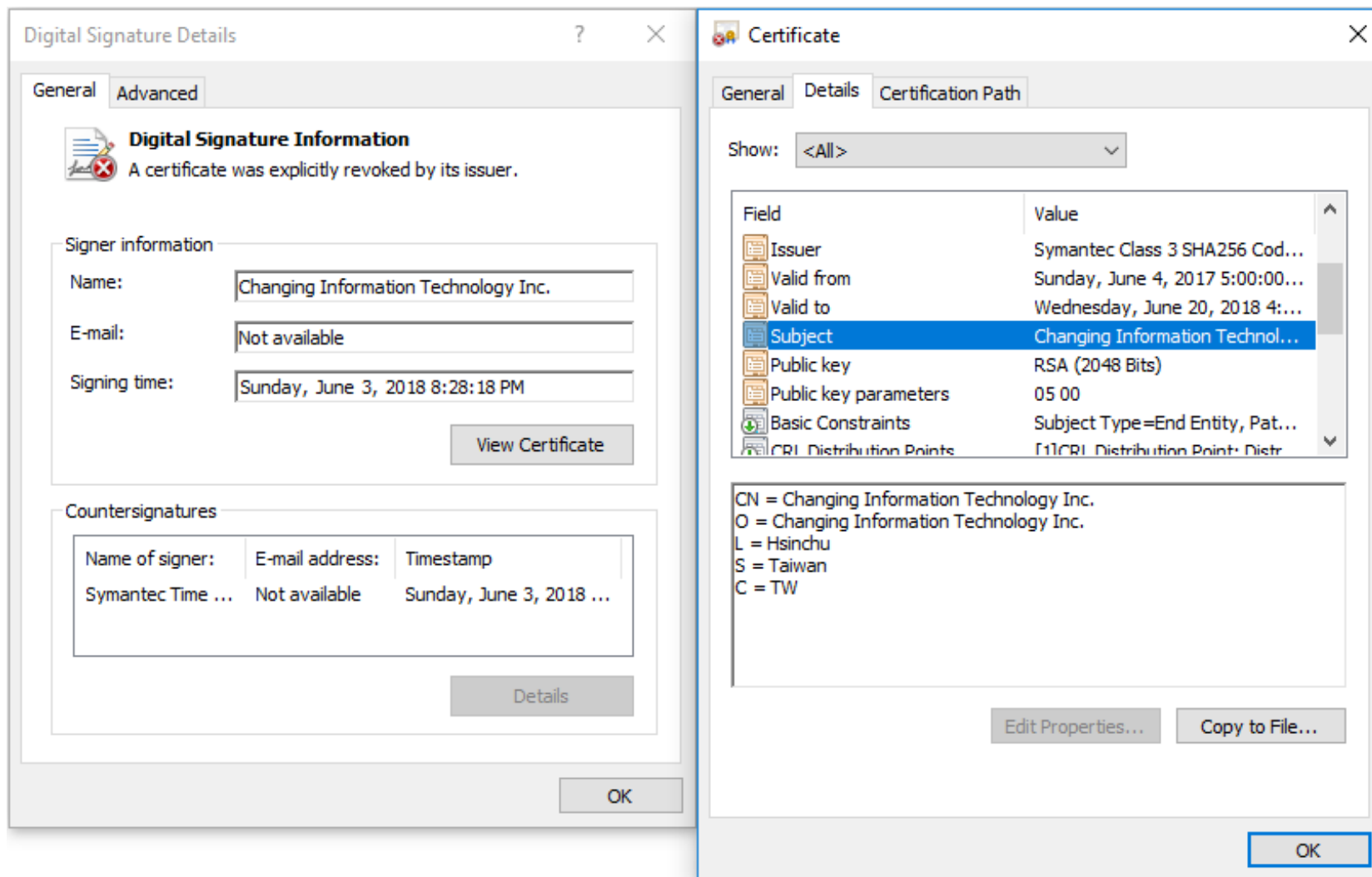


Figure 2. The Changing Information Technology Inc. code signing certificate used to sign malware

Along with the Plead samples signed with the D-Link certificate, ESET researchers have also identified samples signed using a certificate belonging to a Taiwanese security company named Changing Information Technology Inc.

Despite the fact that the Changing Information Technology Inc. certificate was revoked on July 4, 2017, the BlackTech group is still using it to sign their malicious tools.

The ability to compromise several Taiwan-based technology companies and reuse their code-signing certificates in future attacks shows that this group is highly skilled and focused on that region.

The signed Plead malware samples are highly obfuscated with junk code, but the purpose of the malware is similar in all samples: it downloads from a remote server or opens from the local disk a small encrypted binary blob. This binary blob contains encrypted shellcode, which downloads the final Plead backdoor module.

```

.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

```

Figure 3. Obfuscated code of the Plead malware

The password stealer tool is used to collect saved passwords from the following applications:

 Google Chrome

 Microsoft Internet Explorer

 Microsoft Outlook

 Mozilla Firefox

Why steal digital certificates?

Misusing digital certificates is one of the many ways cybercriminals try to mask their malicious intentions – as the stolen certificates let malware appear like legitimate applications, the malware has a greater chance of sneaking past security measures without raising suspicion.

Probably the most infamous malware known to have used several stolen digital certificates is the [Stuxnet](#) worm, discovered in 2010 and the malware behind the very first cyberattack to target critical infrastructure. Stuxnet used digital certificates stolen from RealTek and one from JMicron, two well-known technology companies based in Taiwan.

However, the tactic is not exclusive to high-profile incidents like Stuxnet, as evidenced by this recent discovery.

IoCs

ESET detection names

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

Unsigned samples (SHA-1)

80AE7B26AC04C93AD693A2D816E8742B906CC0E3

62A693F5E4F92CCB5A2821239EFBE5BD792A46CD

B01D8501F1EEAF423AA1C14FCC816FAB81AC8ED8

11A5D1A965A3E1391E840B11705FFC02759618F8

239786038B9619F9C22401B110CF0AF433E0CEAD

Signed samples (SHA-1)

1DB4650A89BC7C810953160C6E41A36547E8CF0B

CA160884AE90CFE6BEC5722FAC5B908BF77D9EEF

9C4F8358462FAFD83DF51459DBE4CD8E5E7F2039

13D064741B801E421E3B53BC5DABFA7031C98DD9

C&C servers

amazon.panasocin[.]com

office.panasocin[.]com

okinawas.ssl443[.]org

Code signing certificates serial numbers

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



Anton Cherepanov 9 Jul 2018 - 12:28PM

Similar Articles



Ammy Admin compromised with malware again; World Cup used as cover



New Telegram-abusing Android RAT discovered in the wild



BackSwap malware finds innovative ways to empty bank accounts



One year later: EternalBlue exploit more popular now than during WannaCryptor outbreak

Discussion

**welive
security**



[Home](#)

[About Us](#)

[Contact Us](#)

[Sitemap](#)

[Our Experts](#)

[ESET](#)

[Research](#)

[How To](#)

[Categories](#)

[RSS Configurator](#)

[News Widget](#)

[Privacy policy](#)

[Legal Information](#)

Copyright © ESET, All Rights Reserved